Proposer Information Package (PIP)

Real-time Adversarial Intelligence

and Decision-making

(RAID)

BAA 04-16

March 1, 2004

# A TABLE OF CONTENTS

# B PIP ROADMAP

## B.1 PROBLEM STATEMENT (SECTION C)

- Provide predictive, anticipative analysis of enemy future actions while making effective assumptions and suggestions for friendly actions
- Identify enemy's attempts to conceal its assets and actions and to deceive the friendly forces
- Monitor the unfolding operation and continuously confirm, disconfirm and update the products of predictive analysis
- Enable the predictive analysis support in a transparent fashion that does not impose additional workload on the commander and staff

## B.2 PROGRAM STRUCTURE (SECTION D)

- Two (2) technology-intensive components to be developed: adversarial reasoning module and deception reasoning module
- One (1) systems-level integrator
- One (1) experimentation and evaluation team
- Three (3) successive 12-month phases focused on specific capability thrusts

## B.3 TECHNICAL OBJECTIVES (SECTION E)

- Prove that adversarial reasoning can be automated and can generate high quality predictions of enemy actions
- Prove that automated reasoning can be robust and effective in the presence of concealment, deception, and the impact of doctrinal and cultural biases
- Integrate the predictive analysis tools into a warfighter's C2 and intelligence support system

## B.4 PROPOSAL MANAGEMENT (SECTION F)

- Briefing to Industry at the Executive Conference Center, 3601 Wilson Blvd Suite 600, Arlington VA on 17 March 2004
- Proposals due to DARPA 3PM ET 21 April 2004

## B.5 PROPOSAL EVALUATION (SECTION G)

- First: Technical Depth and Feasibility
- Second: Consistency with RAID Program Concepts
- Third: Cost Realism and Value of Proposed Work to the Government
- Fourth: Personnel and Corporate Capabilities and Experience

# C PROBLEM STATEMENT

*"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."*

*Sun Tzu*

## C.1 THE MILITARY CHALLENGE

The Real-time Adversarial Intelligence and Decision-making (RAID) program focuses on the challenge of anticipating enemy actions in a military operation. In a number of recent publications, US military leaders call for the development of techniques and tools to address this critical challenge.

In the US Air Force community, the term, *predictive battlespace awareness,* refers to future techniques and technologies that would help the commander and staff to characterize and predict likely enemy courses of action, to relate the history of the enemy's performance to its current and future actions, and to associate these predictions with opportunities for friendly actions and effects [1]. *Numbers in square brackets refer to the listing in Section J – REFERENCES.*

A related term, *predictive analysis,* is beginning to be used in the US Army community to denote a process and tools for predicting future enemy actions [2]

Today's practices of military intelligence and decision-making do include a number of processes specifically aimed at predicting enemy actions. Thus, the Intelligence Preparation of the Battlefield [3] is a systematic process of assessing the likely actions of the enemy and the ways in which environment affects the potential actions of enemy and friendly forces. When a specific friendly course of action is being planned and analyzed, the planning staff executes a wargame [4] in which the participants use the action-reaction-counteraction technique in order to visualize in time and space how the enemy may react or counteract the friendly actions. When the operation is executed, the commander and staff make the necessary changes to the original plans while continually visualizing the possible future actions and reactions of the enemy.

Currently, these processes and wargames are largely manual as well as mental, and do not involve any significant use of technical means (although attempts have been made, e.g., [5]. The effectiveness and accuracy of the processes can be heavily impacted by the difficult conditions (exhaustion, stress, sleep deprivation, etc.) under which the staff performs them, by the relative scarcity of the requisite skills, and by the interpersonal dynamics. Even when computerized wargaming is used (albeit rarely in field conditions), it relies either on human guidance of the simulated enemy units or on simple reactive behaviors of such simulated units; in neither case is there a computerized prediction of *intelligent and forward-looking* enemy actions.

Thus, the challenge of predicting enemy actions involves the development of computational means to reason about the future enemy actions in a way that combines: the enemy's intelligent plans to achieve his objectives by effective use of his strengths and opportunities; the enemy's perception of friendly strengths, weaknesses and intents; the enemy's tactics, doctrine, training, moral, cultural and other biases and preferences; the impact of terrain, environment (including non-combatant population), weather, time and space available; the influence of personnel attrition, ammunition and other consumable supplies, logistics, communications, sensors and other elements of a military operation; and the complex interplay and mutual dependency of friendly and enemy actions, reactions and counteractions that unfold during the execution of the operation. In this document we use the term *adversarial reasoning* to refer to the process of making inferences over the totality of the above factors.

We also use the term *deception reasoning* to refer to another important aspect of predicting enemy actions: the fact that military operations are historically, crucially dependent on the ability to use various forms of concealment and deception for friendly purposes while detecting and counteracting the enemy's concealment and deception. Therefore, adversarial reasoning must include deception reasoning.

## C.2 THE PROBLEM DOMAIN

Although many types of military operations can greatly benefit from the capabilities we outlined above, the RAID program will attack the challenge of developing such capabilities by focusing on a well-circumscribed, intentionally narrow but still very challenging domain: tactical combat of largely dismounted infantry (supported by armored and air platforms) against a guerilla-like enemy force in urbanized terrain.

Consider briefly the following scenario. A company-sized blue (friendly) force executes a mission: seize and control several key intersections in a city. The blue force is supported by several armored vehicles and by close air support. Opposing them is the red (enemy) force organized in multiple teams of 3-7 fighters each experienced in urban warfare, familiar with each building in the city and enjoying the sympathy of some members of the local population. The red force is equipped with automatic rifles and machine guns that are effective against the dismounted blue personnel; with rocket propelled grenade launchers that can threaten armored vehicles; and with man-portable air defense missiles that are of concern to blue air platforms. The red force intends to delay the blue force and to inflict extensive casualties. Each building can become a strong point and may have to be cleared methodically, room by room. Each street crossing is a complex task. Each corner is a potential ambush point. Blending with the local population and using sympathizers for intelligence gathering, the red force employs ambushes, counterattacks, and infiltration and exfiltration techniques to create a very complex, non-linear, discontinuous battlefield. The area of operations is on the order of 5x5 kilometers and the operation is expected to take about 8 hours.

This scenario, in multiple variations, will be used in RAID experiments (Section D.2). Operations in urbanized terrain [6, 7, 8, 9, 10] exacerbate the challenges inherent in adversarial reasoning. The highly three-dimensional nature of the environment presents a high density of features that can offer an array of threats and opportunities for both friendly and enemy forces and requires one to think about an extremely broad range of potential enemy movements, positions and actions. The enemy and friendly forces can be situated in extreme proximity to each other and even intermeshed in a complex pattern, e.g., the basement of a building may be occupied by enemy force, the first floor by the friendly and the second floor again by the enemy.

Urbanized terrain tends to disperse the forces and give even the smallest tactical unit, enemy or friendly, a significant degree of freedom while complicating synchronization and opportunities to form a holistic view of the battlespace and its evolution. Maneuver can be highly distributed and nonlinear. Actions of the combatants can rapidly modify the terrain in many important ways: a breach in a wall creates a new mobility corridor; a barricade can transform a previously passable street into a major obstacle; a collapsed building transforms the landscape. Forces have a rich range of options for concealment, for stealthy movements, for infiltration and exfiltration. Resupply and casualty evacuation (by air or ground) are complicated by the high risk of ambush.

Of particular importance is the presence of non-combatants. Dismounted enemy personnel, often in civilian clothes, are difficult to distinguish from non-combatants. The fire of friendly troops is constrained by concerns regarding collateral damage while the enemy often disregards the potential for casualties among non-combatants and even exploits the restraint of the friendly troops. The enemy may use and manipulate non-combatants in order to obtain supplies, intelligence and communications, to conceal and infiltrate his troops, and to distract and deceive the friendly personnel.

## C.3 A POTENTIAL OPERATIONAL CONCEPT

RAID capabilities are likely to find application in a number of different settings. One possible concept is depicted in Fig.1.

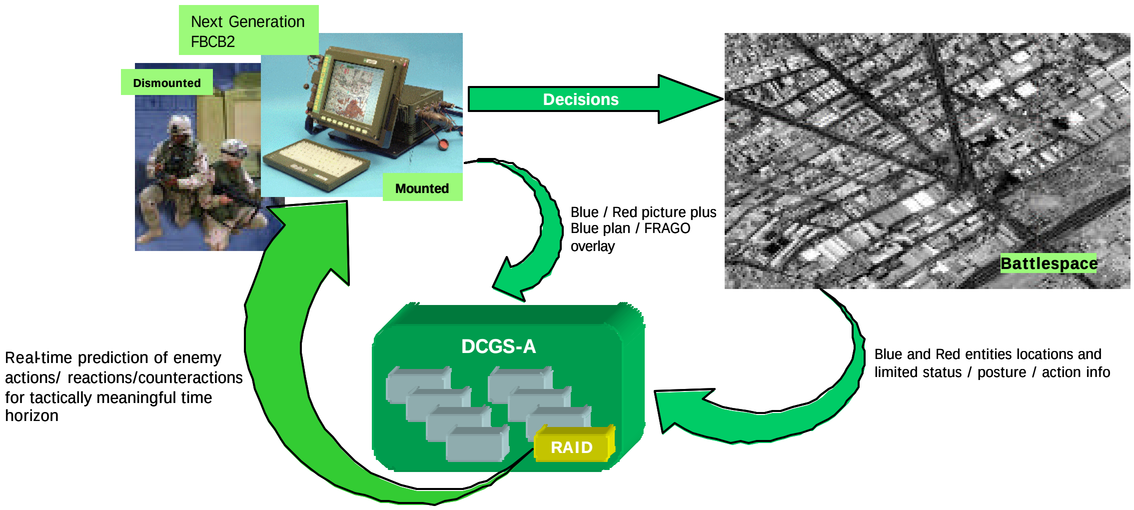


Figure 1. A Possible CONOPS

*Here RAID is envisioned as a potential tool within the future Distributed Common Ground System-Army (DCGS-A) with the predictions being made available to the commander on his Commanders Digital Assistant (CDA) or the next generation Force XXI Battle Command, Brigade-and-Below (FBCB2) command and control console.*

Here, as a military operation is being executed, the information from the battlespace, such as location, strengths and postures of enemy and friendly troops, is rapidly delivered to a future military intelligence system, such as DCGS-A or ASAS-L. With today's rapid proliferation of blue force tracking devices, unmanned ground sensors and sensors onboard unmanned aerial vehicles, one envisions that latency of such information would be measured in minutes. The sensor data would have undergone a fusion process that may identify locations of some of the enemy units, as well as, some attributes, such as type, size, posture, etc. It is understood, however, that the fog of war would remain thick – in spite of the proliferation of sensors and improved fusion techniques, the battlespace information, especially the enemy information, would remain incomplete and potentially deceptive.

This information arrives to a RAID module, an application within the DCGS-A suite of applications. Continually monitoring the changes in the battlespace state as the information unfolds, RAID periodically or on request generates predictions of enemy actions and represents them in a user-friendly, rapidly comprehensible format. If staff availability permits, the RAID products may be previewed and even filtered by a staff member, e.g., a battalion S2. This preview, however, does not need to be a strict requirement, especially at lower echelons. RAID predictions are then delivered to the user, such as a company commander via a system like FBCB2 [11] available on computer displays in combat vehicles or on PDA-like devices for dismounted personnel.

Each set of RAID products includes several possible alternative enemy courses of action, worked out in requisite detail, ranked in the order of likelihood, and presented as graphic overlays with brief textual notes and with an explanation of assumptions about the friendly course of action. The scope and details of the products are tailored for each individual user, his current situation and area of responsibility. RAID products are unobtrusive to the user. The user may elect not to see them at all, or to see them occasionally on request; he may use them extensively or ignore them entirely.

If time and situation permits, the user, at his discretion, may input to RAID additional information, such as his updated intent and friendly scheme of maneuver for the upcoming phase of the operation or his estimates of enemy intent. RAID uses this additional information, when available, to fine-tune its predictions. In the absence of such input, RAID makes do with its own assumptions and estimates. In no case does RAID become an additional burden on the user's time and attention.

# D PROGRAM STRUCTURE

## D.1 SYSTEM CONCEPT

This BAA is structured around the development of several key components and interfaces of the RAID system. As depicted in Fig.2, the developmental RAID system will consist of several technology components exercised against a largely existing testbed. It must be emphasized that the developmental RAID system, especially in the first two phases of the program, has somewhat different inputs and outputs than a deployable RAID system. Thus, Figures 1 and 2 are not identical. As the RAID program moves into the transition phase, the developmental system will be modified and adapted to its target transition environment.

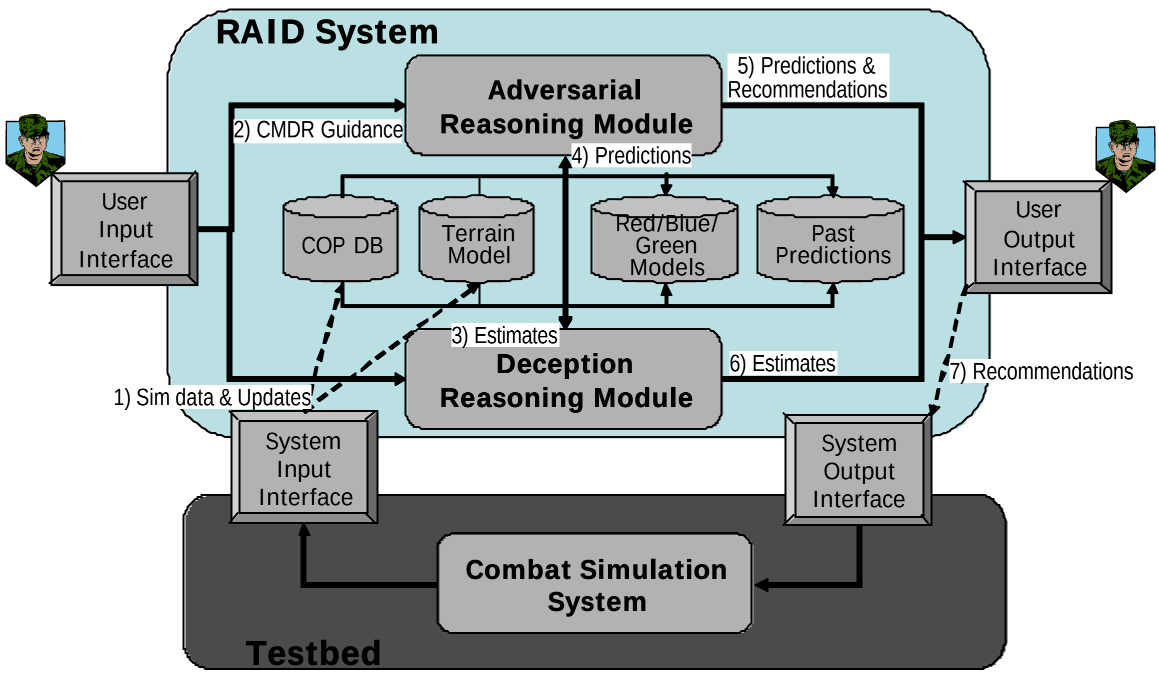


Figure 2. Key Components

### D.1.1 Components

Refer to Fig. 2.

**The Adversarial Reasoning Module (ARM)** is responsible for generating predictions of enemy actions. A more detailed discussion of this module is given in Section E.1.

The Deception Reasoning Module (DRM) is responsible for identifying probable enemy deceptions, decoys, feints, etc., concealed enemy assets, movements and actions. A more detailed discussion of this module is given in Section E.2.

**The Terrain Model** contains a detailed description of the urbanized terrain, including: elevation data for the base terrain (excluding man-made structures); soil and vegetation data (e.g., rubble, wooded, concrete), a representation of each building including at least the geometry of its footprint, height, number of floors, type of construction, type and density of internal subdivisions and stairways; possibly presence and approximate geometry of basements and subterranean cavities and passages (sewers, etc.). This model is dynamically updated because the actions of combatants do change the terrain. For the purposes of a deployable RAID system, it is envisioned that such digital, feature-based information will become available to warfighters in the near future, particularly from UAV-based three-dimensional near real-time mapping systems. For the purposes of the developmental RAID system, this information will reflect the terrain and structures modeled in the Combat Simulation System.

**The Common Operating Picture database (COP DB)** contains the description of the most recently available status of each blue (friendly) and (known) red (enemy) unit of force, including (when available): unit identifier, unit type and strength, unit's command and support relations to other units, posture (e.g., entrenched, on the move), parameters of the posture (e.g., direction of the movement), supplies on hand, casualties, occasionally intent (e.g., capture building X, block intersection Y), data latency, degree of data certainty. Clearly, for red units much of this information will be available only sparsely and with much uncertainty. Given the tactical focus of RAID, a unit is typically as small as a fire team or squad, and on occasion even an individual combatant, e.g., a lone sniper. A subset of such information is available for non-combatants (green). Weather and lighting conditions are also represented here. The COP DB also maintains snapshots of the COP information from several earlier time points, so that the ARM and DRM can see the history of the battle. For the purposes of a deployable RAID system, one envisions such information becoming available with low latency from the emerging automated Level 1 and Level 2 fusion systems that exploit information from rapidly proliferating BFT, UGS and UAV sensor systems. For the purposes of the developmental RAID system, this information will reflect the simulation data available within the Combat Simulation System.

**The Red Blue Green Models** contain a formal representation of parameters, capabilities and behaviors of red, blue and green (non-combatant) entities, including: number and type of personnel and weapons in units of different types; range, accuracy and effects of weapons as function of circumstances of employment; unit's rate of movements as a function of circumstances; time required to accomplish different classes of actions; parameters related to sensing, communication and supply capabilities of units; commonly used tactics (patterns of actions); doctrinal and cultural preferences toward actions or tactics. These models remain largely static while RAID operates on-line; however, some of the parameters could be modified by the ARM or DRM based on observations.

**The Past Predictions** is a store of products generated by the ARM and DRM at earlier time points. These can be used by the ARM and DRM to control their respective reasoning processes and to adjust parameters in the Red Blue Green Models.

**The RAID User Input Interface** is an interface that allows the user of RAID (e.g., a company commander) to enter, at his discretion, certain high-level guidance that enables RAID to produce more accurate predictions, including: high-level objectives and priorities of the red force; characterization of the intent and style of the red command; intent and scheme of maneuver of the blue force; user's estimates of the red forces other than (or different from) those contained in the COP DB; terrain features other than those in Terrain Model. This interface is also responsible for transforming the user inputs from the original input format (which is to be user-oriented from both cognitive and doctrinal perspectives) to the formats required by the COP DB, Terrain Model, ARM and DRM. In the first two phases of the RAID program, this interface is to be built in a manner that minimizes its development costs and optimizes its utility for RAID experiments. As such, this interface could be built, for example, using the potentially extant UI facilities of the Combat Simulation System. However, in the third phase of the program, this interface will have to be rebuilt within the target transition environment, for example as a UI application within the future generation of the FBCB2 system and future DCGS-A and ASAS-L systems.

**The RAID User Output Interface** is a user interface that allows the user of RAID (e.g., a company commander) to view, explore, manage, edit, export and forward to other systems or products the outputs generated by the ARM and DRM, i.e., predictions of red actions, assumptions / recommendations for blue actions, identification of suspected concealed red units or red movements and other actions, red deceptions and decoys. This interface also allows the user to select some or all of the RAID recommendations for blue actions and to submit these actions for execution to the Combat Simulation System via the RAID System Output Interface. In the first two phases of the RAID program, this interface is to be built in a manner that minimizes its development costs and optimizes its utility for RAID experiments. As such, this interface could be built, for example, using the potentially extant UI facilities of the Combat Simulation System. However, in the third phase of the program, this interface will have to be rebuilt within the target transition environment, for example as a UI application within the future generation of the FBCB2 system and future DCGS-A and ASAS-L systems.

**The Combat Simulation System** is to be an existing simulation system (yet to be selected within this BAA process). Some examples of potential candidates are: OneSAF (OTB), JSAF, and others. The RAID System Integrator is expected to identify and propose a system most suitable for the purposes of RAID. Description of the planned experiments (later in this document) offers insights into the required capabilities of the Combat Simulation Model. Modifications to the existing system's interfaces and entity behaviors may be required. In particular, the Combat Simulation System must be available to the component developers for their in-house experiments; must be available in an unclassified version; must operate with human cells commanding the simulated entities as well as with software systems commanding the entities; must offer a significant degree of credible semi-automated behavior of the entities; must provide facilities for modeling dismounted infantry and multiple non-combatants in urbanized terrain.

**The RAID System Output Interface** transforms the blue actions arriving from the RAID User Output Interface into the format required by the Combat Simulation System. It is possible that the transformation will have to address semantic gaps between the two systems, and will require a degree of inference to fill these gaps.

**The RAID System Input Interface** periodically extracts the information required by the COP DB and Terrain Model from the Combat Simulation System, and sends it in the requisite formats. It is possible that the transformation will have to address semantic gaps between the two systems, and will require a degree of inference to fill these gaps.

### D.1.2 Information Flows

Refer to Fig. 2.

Flow 1. Data required to populate and continually update the COP DB and Terrain Model. See discussion of the COP DB and Terrain Model components.

Flow 2. This is the RAID user's high-level guidance that enables RAID to produce more accurate predictions. See discussion of the RAID User Input Interface component.

Flow 3. This is the DRM's estimates or assumptions about the true state of the battlespace. These are in effect changes to the COP DB and are similar in content to Flow 1.

Flow 4. This is the ARM's predictions of red actions and recommendations for blue actions based on the assumptions provided by the DRM. Similar in content to Flow 5.

Flow 5. The ARM's predictions of red actions and recommendations for blue actions. See discussion of the ARM component.

Flow 6. The DRM estimates of concealed units and actions of the red, decoys and deceptions. See discussion of the DRM component.

Flow 7. Blue actions recommended by the ARM on the basis of its predictions of red actions and approved by the commander. A subset of Flow 5.

## D.2 MANAGEMENT CONCEPT

### D.2.1 Program Elements

This solicitation requests efforts in four related areas.

**Adversarial Reasoning**: design and build the Adversarial Reasoning Module, the Terrain Model, the COP DB, the Red Blue Green Models; continue to develop and enhance these components as the program progresses through its phases; support the program's series of increasingly realistic experiments; share the content of the Terrain Model, the COP DB, the Red Blue Green Models with the Deception Reasoning Module via the interfaces constructed by the System Integrator; perform the efforts in close coordination with the System Integrator and according to the system specifications developed by the System Integrator; and provide ARM software to the other ARM performer for the purposes of acting as an automated red commander in in-house experiments. It is expected that there will be up to two (2) awards in this area. However, in the event of two awards for this area, only one will be carried to Phase III.

**Deception Reasoning**: design and build the Deception Reasoning Module; continue to develop and enhance this component as the program progresses through its phases; support the program's series of increasingly realistic experiments; utilize the content of the Terrain Model, the COP DB, the Red Blue Green Models via the interfaces constructed by the System Integrator; and perform the efforts in close coordination with the System Integrator and according to the system specifications developed by the System Integrator. It is expected that there will be up to two (2) awards in this area. In the event of two or more awards for this area, only one will be carried to Phase III.

**System Integration**: design and build the overall architecture, interfaces, representations and formats of the RAID system, components and testbed, including but not limited to RAID User Input Interface, RAID System Input Interface, RAID User Output Interface, RAID System Output Interface, Past Predictions DB; enable sharing of data and models between the ARM and DRM; modify, as necessary, the interfaces and entity behaviors of the Combat Simulation System; replace notional parameters and models with validated and realistic ones in connection with system-wide experiments; implement elements of the experimental scenario and terrain as designed by the Experimentation and Evaluation performer; provide hardware, software and facilities for experiments; design and build interfaces required for integration of RAID capability into target transition environment; and act as the prime contractor and manage the efforts of the Adversarial Reasoning and the Deception Reasoning area performers. It is expected that there will be only one (1) award in this area.

**Experimentation and Evaluation**: design experiments, design wargame scenarios, define system- and component-level metrics, design instrumentation to obtain data, provide and train human players, manage and execute experiments, collect and analyze data; provide subject matter expertise to the RAID technology developers; liaison with potential users of RAID and transition partners; and maintain organizational and contractual independence from performers in other areas of the program in order to provide objective experimental evaluation of RAID performance but coordinate closely with the System Integrator. It is expected that there will be only one (1) award in this area.

Teaming is encouraged. An organization can propose to more than one area, with a separate proposal for each area.

### D.2.2 Program Phases

The RAID program will be conducted in three 12-month phases. Funding for later phases is entirely contingent upon meeting system-level performance goals established for earlier phases. System-level performance goals appear in Section E.

1) **Phase I – Anticipation:** Develop mechanisms to compute adversarial, anticipative, move-countermove actions. For planning purposes, assume Phase I extends from October 1, 2004 through October 1, 2005.
2) **Phase II – Detection:** Develop ability to see through fog or war and recognize deceptions. For planning purposes, assume Phase II extends from October 1, 2005 through October 1, 2006.
3) **Phase III - Transition:** Develop fieldable products which can integrate with existing C2 and ISR systems. For planning purposes, assume Phase III extends from October 1, 2006 through October 1, 2007.

The specific objectives and content of each phase are best described by the experiments which will be used to exercise RAID capabilities.

### D.2.3 Program Experiments and Metrics by Phases

The development of RAID will be driven by a rigorous schedule of increasingly difficult and realistic experiments. Each phase of the program will include two series of experiments. Outcomes of the experiments will have a decisive influence on continuing funding of the program or its individual efforts. For planning purposes, assume the following schedule of experiments: Phase I – 8 and 11 months after contract; Phase II - 18 and 23 months after contract, Phase III - 30 and 35 months after contract. To assess RAID progress at the end of each phase DARPA will use quantitative metrics and experimental conditions summarized in Table 1 and discussed in detail below.

In addition to these program-wide experiments, RAID contractors will design and perform in-house experiments to assess the progress made toward the program goals in development of the contractor's respective component. RAID contractors will propose specific component-level assessment metrics to be used in such component-specific experiments.

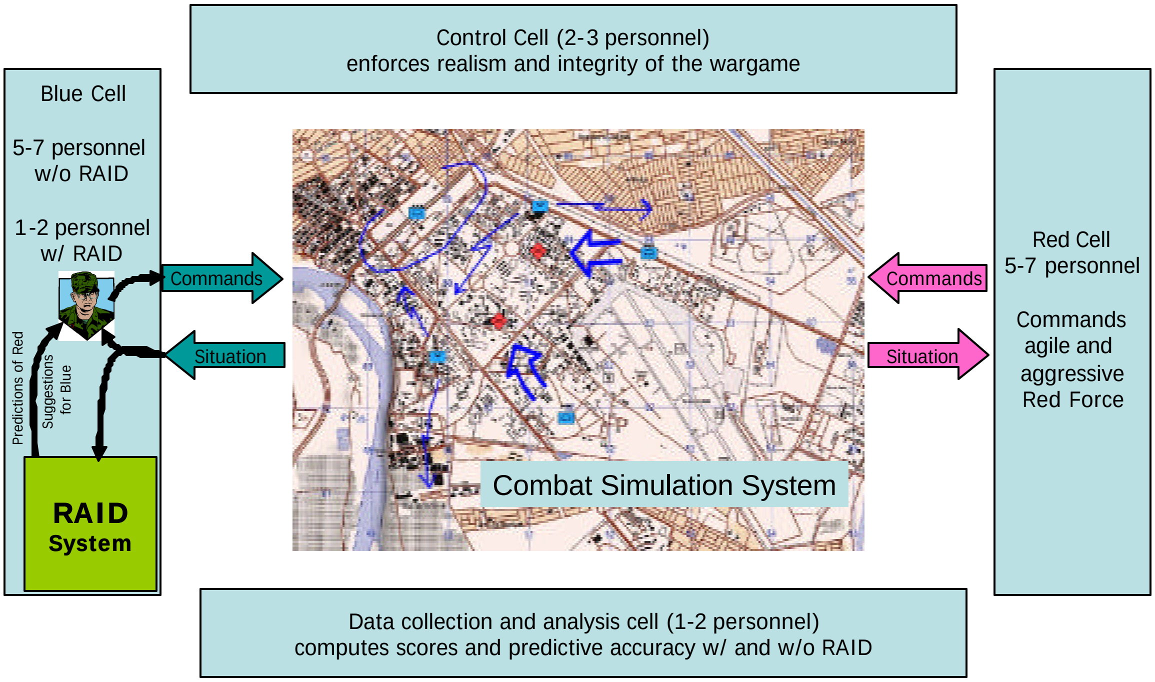


Figure 3. Experimental Approach

### *D.2.3.1 Phase I Experiments and Metrics*

The purpose of these wargaming experiments is to explore the ability of RAID to make effective estimates of enemy actions and assumptions about friendly counteractions (move-countermove reasoning), as compared to a human staff. In the experiments, RAID performs the following functions: read red/blue situation from the Combat Simulation System; accept guidance from the blue commander (priorities, key objectives, etc.); on demand, estimate most effective actions of red and assumed actions of blue for the next 30 minutes of wargame time; complete every new estimate in less than 300 seconds; present the estimate to blue commander as overlay graphics; if desired by blue commander, submit blue actions to the Combat Simulation System for execution by blue simulated entities.

The experiments will consists of approximately 10 benchmark games (without RAID) and 10 test games (with RAID). Control of red entities will be performed by the red cell of 5-7 experienced human wargamers. Control of blue entities in the 10 benchmarking games will be performed by a blue cell of 5-7 human wargamers. Control of blue entities in the 10 test games will be by a blue cell of only 1-2 human wargamers supported by RAID. Each game lasts about 2 hours (preceded by an orientation and planning session) and simulates 1 hour of real-world actions (i.e., 2 times slower than real time).

The formulation of the Phase 1 experiments involves numerous significant simplifications. The scenario is to be built around the blue force's mission to capture several geographic objectives in an urban environment. The blue objectives and priorities (specified by the relative values of terrain elements, enemy and friendly casualties, time delay) are known and fixed, entered by the blue commander. The red force includes up to 20 teams of fixed composition, each of 3 fighters; these are well-trained irregular forces with small arms, anti-tank weapons. The blue force is company-sized with a few armored vehicles with anti-personnel and wall-breaching weapons. The blue force is represented as a flat set of fire teams each consisting of 4-6 personnel and commanded directly by a single command node. The intelligence collection capabilities of both forces are presumed such that they have full-state information on location and status of all assets. They also possess idealized instant, reliable communications. Casualties are presumed to be instantly evacuated. Supplies are instantly replenished. Groups of civilians are randomly positioned and move randomly around the terrain. The red and blue fire teams are restricted to executing a meaningful but small repertoire of actions, such as: move at two different speeds (aggressive and cautious) in the streets; breach a building; clear a building; move horizontally and vertically in a building; prepare a firing position; direct fire.

In all series of experiments, overall complexity of the problem is varied by adjusting number and granularity of red/blue units, and restrictions on the set of available actions and weapon types. It is estimated that the complexity measure (the size of the search space) of the Phase I problem will exceed 10**8,000. In all experiments, the computing power available to the primary components of RAID, i.e., the ARM and DRM, is restricted to a single processor of about 2.5 GHz.

The terrain representation includes several hundreds of buildings, each building is defined by its footprint, height, number of floors, ease of breaching the external and internal walls; aggregated measure of trafficability in horizontal and vertical directions, aggregated measure of cover and concealment within the building. Specific layout of internal walls, rooms and stairways is not considered.

Success of the blue force is measured by the rate of progress toward the mission accomplishment (e.g., advancing to or clearing the specified objective); red personnel destroyed; avoidance of friendly losses and collateral casualties. Success of the red force is measured by delaying the blue force and causing blue casualties.

In accordance with DARPA policy, the RAID program must meet a specified goal (also called “gate”) at the conclusion of each project phase in order to obtain funding for the next phase. Detailed definition of the metrics, design of experiments, methodologies for data collection and processing are to be determined by the Experimentation and Evaluation performer. In the experiments of Phase I, the goal is to demonstrate in a statistically significant manner that the small blue cell supported by RAID (i.e., the test wargames) can be at least as successful as the larger all-human blue cell (i.e., the benchmark wargames).

| | Phase I | Phase II | Phase III |
|---|---|---|---|
| **Thrust** | Action-reaction-counteraction | Concealment and deception | Breadth, robustness, transition |
| **Experiment Design** | 10 benchmark, 10 test games, compare scores | Add: compare accuracy of predictive estimates | In CPX-like setup, integrated with FCBC2, CDA and DCGS-A |
| **OPFOR** | Up to 20 teams of 3 fighters each w/ small arms, RPGs | Up to 30 teams of 3-7. Add sniper rifles, MGs, MANPADS | 200 fighters, dynamically formed teams. Add mortars, rockets |
| **BLUFOR** | Company-sized force w/ several armored vehicles | Add air support (helicopters) | Add CAS, joint close support fires, air mobility |
| **Terrain Representation** | Buildings and floors, aggregated internals | Add breached openings in bldgs; basements, internal passages | Add underground corridors of mobility, overpass, fences, walls, urban clutter |
| **Intel Capabilities** | Full state known to both sides | Observations by troops | Add UGS and UAV sensors |
| **Organization** | Flat organization of fixed small teams with single command node | Company w/ three fixed platoons | Dynamic reorganization and reattachment |
| **Communications** | Implicit idealized instant broadcast | Comms and info processing delays | Differentiated nets with realistic delays and sporadic loss |
| **Casualty Mgmt** | Implicit immediate evacuation | Treatment, delayed evacuation | Add explicit medevac actions |
| **Logistics** | Implicit continuous resupply | Run out of ammo, delays in resupply | Explicit resupply actions |
| **Civilians** | Random presence and reactions | Civilians help red resupply, intel | Blue actions to manage civilians |
| **Concealment, Deception** | Feint movements and attacks | Concealment, stealthy moves | Decoys, civilians do diversions |
| **Timing** | Game 2 hours, slower than real | Each game lasts 2 hrs, real time | Game lasts 4-6 hrs, real time |
| **Lookahead into future** | At least 30 min | At least 60 min | At least 5 hours |
| **Problem Complexity** | over 10**8,000 | over 10**20,000 | over 10*50,000 |
| **Solution speed** | Within 300 sec | Within 120 sec | Within 30 sec |
| **Key Gate** | RAID-assisted small staff scores as high as large unassisted | RAID-assisted small staff scores as high as large unassisted | RAID-assisted small staff scores as high as large unassisted |

*Table 1. Experimentation Plan and Metrics*

### *D.2.3.2 Phase II Experiments and Metrics*

These series of experiments are to demonstrate the ability of RAID to identify enemy concealment and deception. The structure of the experiments includes an additional element: periodically (every 15 minutes) the staff (in the benchmark wargames) produces a predictive estimate of enemy actions. In the test wargames the same is performed by RAID. Both most dangerous and most likely predictions are made. The term most dangerous refers to a red course of actions that results in the red's greatest achievement of its goals in spite of the blue force's best efforts. However, for a variety of reasons that may include enemy's doctrine, culture, command style and limitations, etc., the most dangerous red course of action is often not the one most likely to be adopted by the red. The blue commander normally considers both the most dangerous red course of action (in order to take precautionary measures if necessary) and the most likely one (to prepare blue actions).

Then both series of predictions are compared to the actual unfolding of the wargames. The predictions made in the benchmark wargames (without RAID) and the prediction made in the test wargames (with RAID) are then compared to the actual unfolding of the wargames and a metrics that reflect "closeness of prediction" (to be developed by the experimentation performer) are computed. In this way, the accuracy of

RAID's predictive analysis is compared to that of humans. Each wargame lasts 2 hours, in real time.

In this way, the accuracy of RAID's predictive analysis is compared to that of humans. Each wargame lasts 2 hours, in real time.

The scenario is built around the blue force's mission to clear and secure a specified area within a specified time period. The red force is to defeat the blue by imposing an excessive time delay and unacceptable level of casualties. Unlike in Phase I, user's management of blue objectives and priorities is complicated by changing them in the course of the operation. The red force involves up to 30 teams of 3-7 fighters; their arsenal is broadened by addition of sniper rifles, heavy machine guns, and MANPADS. They maintain well-prepared positions. The key approaches are mined, and the mines are covered by ambushing fire. The blue force acquires a more complicated structure: it is now organized in 3 platoons, each divided into squads and fire teams, and several helicopters add to their fire support. The terrain representation is enriched by adding openings and passages (natural or generated by breaching) through buildings, basements, greater variety of construction types.

The problem's simplification is much less drastic than in Phase I. These experiments involve operationally credible fidelity (although still with limited breadth of scenario), force mix and combat actions. Intel capabilities of both sides are made more realistic: their knowledge of the opposing force is now limited to direct observations by own troops. Thus, at any given moment each force is aware of only a fraction of the enemy assets and actions. This provides opportunities for concealment and deceptions. blue force may also have incomplete knowledge of the actual terrain features, e.g., blue troops may not know about an existence of a basement in a building. Communications and information processing modeling now adds processing delays and differentiated treatment of voice and data. Casualty management representation gains an explicit action of medical treatment and delayed evacuation; this impacts mobility of the units. Supplies are no longer magically replenished; there are finite amounts of supplies on hand and resupply can be randomly delayed causing a unit to run out of ammo, water, etc. The repertoire of a unit's actions is broadened to include a majority of what can be realistically represented in the Combat Simulation Model.

RAID is now aware of tactics that each force prefers due to its training and doctrine. Examples include coordinated ambushes; coordinated capture of multi-story buildings. This helps RAID to formulate most likely enemy actions as opposed to most dangerous.

The red force actively uses several forms of concealment and deception: stealthy moves, stealthy reinforcements from reserves, infiltration and exfiltration, demonstrations and feints. The red force also makes use of non-combatants: concealment by blending with civilians; execution of resupply, communications and intelligence functions with the help of nominal non-combatants.

It is expected that the complexity measure of the problem addressed in these experiments will exceed 10**20,000. Like in Phase I, the goal of Phase II is to demonstrate in a statistically significant manner that the small blue cell supported by

RAID (i.e., the test wargames) can be at least as successful as the larger all-human blue cell (i.e., the benchmark wargames). In addition, predictive accuracy of RAID (in the test wargames) should be at least comparable to that of the human staff (in the benchmark wargames). RAID must provide its products to the user in less than 120 seconds after the user's request, while looking up to 60 minutes into the future.

*D.2.3.3 Phase III Experiments and Metrics*

The purposes of these experiments include: increased breadth and robustness of coverage suitable for a transition-ready product and effective human and system interfaces tailored to the target transition environment.

Each experimental series includes 5 benchmark games (without RAID) and 5 test games (with RAID) of longer duration (4-6 hours each) in CPX-like environment and integrated with systems like FBCB2, DCGS-A and ASAS-L. The scenario increases in complexity and combines elements from the scenarios of earlier phases. Blue objectives, priorities and intent are partially entered by the blue commander and partially inferred by RAID.

The red force consists of up to 200 fighters dynamically organized and re-organized into teams. The red weaponry is further enriched with mortars, rockets, booby traps and flamethrowers. The blue force gains joint close supporting fires, fixed wing CAS and air mobility. The terrain representation is further complicated by adding underground corridors of mobility, overpasses, fences and walls, urban clutter, rubble of destroyed buildings. Intel capabilities include ground and airborne sensors. The failures of intel may include misidentified assets, incorrect BDA and sporadic loss of BFT. The blue force allows dynamic reorganization and reattachment. Communications are represented as differentiated nets with realistic delays and sporadic loss.

Casualty management involves treatment and medevac actions modeled and executed explicitly. Similarly, resupply actions are reasoned about and simulated explicitly. Further consideration is given to the impact of doctrinal pre-trained tactics (in addition to emergent tactics) on both the red and blue side, e.g., advance through intersections with and without support of armor; coordinate with air support and field artillery.

The red force practices even greater manipulation of non-combatants for the purposes of blocking the blue force and for diversions; blue force in turn employs explicit management of non-combatants. Both forces practice a broader range of concealment and deception: decoys, information planting, use of civilians for concealment, attacks, resupply, intel, diversion, red masquerading as blue, etc.

Goals are similar to those of Phase II although it is expected that the complexity of the problem addressed in these experiments will exceed 10**50,000. RAID must provide its products to the user in less than 30 seconds after the user's request, while looking up to 5 hours into the future.

### D.2.4 Performers' Tasks by Phases

The tasks identified below are intended to convey the intent of the effort and not the exact statement of work. Proposers should use this information only as a general guideline and formulate specific tasks that meet the intent of this solicitation as well the technical and programmatic approach of the proposer.

*D.2.4.1 Phase I Tasks*

**System Integration:**

Design and build the overall architecture, interfaces, representations and formats of the RAID system, components and testbed, including but not limited to RAID User Input Interface, RAID System Input Interface, RAID User Output Interface, RAID System Output Interface, Past Predictions DB. Modify as necessary the interfaces and entity behaviors of the Combat Simulation System. Replace notional parameters and models with validated and realistic ones in connection with system-wide experiments (ongoing task). Develop software and/or procedural means to control the repertoire of behaviors used by human players. Implement elements of the experimental scenario and terrain as designed by the Experimentation and Evaluation performer. Provide hardware, software, networking and facilities for experiments, including the necessary observation and data collection instrumentation and after action review means.

**Experimentation and Evaluation:**

Design and verify wargame scenarios and terrain. Perform several illustrative manual wargames as samples for technologists. Design experiments. Refine system- and component-level metrics. Design methodology and instrumentation for data collection. Provide and train human players (ongoing task). Manage and execute experiments (ongoing task). Collect and analyze data (ongoing task). Provide subject matter expertise to the RAID technology developers (ongoing task). Liaison with potential users of RAID and transition partners (ongoing task).

**Adversarial Reasoning:**

Develop representation of combatants, actions, terrain features. Design and build the Adversarial Reasoning Module, the Terrain Model, the COP DB, the Red Blue Green Models. Share the content of the Terrain Model, the COP DB, the Red Blue Green Models with the Deception Reasoning Module via the interfaces constructed by the System Integrator. Support integration and program-wide experiment execution (ongoing task). Evaluate the development progress via component-specific experiments (ongoing task). Provide documentation, reporting, participation in program meetings (ongoing task).

**Deception Reasoning:**

Produce conceptual design and evaluate it against a set of examples. Design and build the Deception Reasoning Module, evaluate in a stand-alone mode. Demonstrate feasibility of extended set actions and types of actors. Support integration and program-wide experiment execution (ongoing task). Evaluate the development progress via component-specific experiments (ongoing task). Provide documentation, reporting, participation in program meetings (ongoing task).

*D.2.4.2 Phase II Tasks*

**System Integration:**

Maintain and extend the products developed in earlier phases (ongoing task). Modify the Combat Simulation System and related interfaces to account for additional features of the Phase II experiments: terrain, weapons, platforms, combatant actions, sensors, communications, logistics, use of deception and concealment. Extend user interface to enable fast, easy changes in objectives and priorities by the user. Develop requirements and design for integration into target transition systems.

**Experimentation and Evaluation:**

Modify scenario to account for additional features of the Phase II experiments: terrain, weapons, platforms, combatant actions, sensors, communications, logistics, use of deception and concealment. Modify the design of experiments, metrics, methodologies and instrumentation to include comparative analysis of prediction accuracies.

**Adversarial Reasoning:**

Extend representation and algorithms of the ARM to account for additional features of the Phase II experiments: terrain, weapons, platforms, combatant actions, sensors, communications, logistics. Extend the ARM to enable it to identify (in cooperation with the DRM) the types of concealment and deception defined in Phase II experiments. Extend the ARM to enable the blue force to use concealment and deception. Develop capabilities to generate several different prediction options, including most dangerous and most likely, ranked in terms of likelihood. Enable predictions that take into account a bias toward use of doctrinal tactics.

**Deception Reasoning:**

Integrate with other RAID components. Extend representation and algorithms of the DRM to account for additional features of the Phase II experiments: terrain, weapons, platforms, combatant actions, sensors, communications, logistics. Extend the DRM to enable it to identify the types of concealment and deception defined in Phase II experiments. Develop capabilities to develop several different deception and concealment options, ranked in terms of likelihood. Enable detections of deception and concealment that take into account a bias toward use of doctrinal tactics.

*D.2.4.3 Phase III Tasks*

**System Integration:**

Design and build interfaces required for integration of RAID capability into target transition environment. Modify user interfaces to generate, manage and use doctrinally compliant graphic and textual products. Enhance user interfaces for fast, effective, transparent interactions between user and RAID, including user modification of red and blue combatant and action parameters, entry of diverse ROEs and editing of doctrinal products. Modify as necessary the interfaces and entity behaviors of the Combat

Simulation System, elements of the experimental scenario and terrain, hardware, software, networking and facilities for the experiments of Phase III.

**Experimentation and Evaluation:**

Support transition process. Modify scenarios, experiment design, and methodology to enable Phase III experiments aimed at transition into target environment.

**Adversarial Reasoning:**

Add system's capability to automatically estimate red objectives and priorities independently or in addition to those entered by the user. Enable system to automatically estimate adjustments of red parameters (e.g., rate of advance, probability of hit) based on observations of the wargame. Handle a range of blue ROEs. Extend representation and algorithms of the ARM to account for additional features of the Phase III experiments: terrain, weapons, platforms, combatant actions, sensors, communications, logistics, concealments and deception, flexible command structures. Extend representation and algorithms of the ARM to account for additional blue and red tactics. Account for red preferences induced by culture, doctrine and training preferences (e.g., dislike of night operations, risk aversion of an individual commander, etc.). Upgrade robustness and performance of the software for the purposes of transition.

**Deception Reasoning:**

Extend repertoire of deception and concealment: decoys, information planting, use of civilians for concealment, attacks, resupply, intel, diversion, red masquerading as blue. Extend representation and algorithms of the DRM to account for additional features of the Phase III experiments: terrain, weapons, platforms, combatant actions, sensors, communications, logistics, concealments and deception, flexible command structures. Extend representation and algorithms of the DRM to account for additional red tactics. Account for red preferences induced by culture, doctrine and training preferences. Upgrade robustness and performance of the software for the purposes of transition.

### D.2.5 Expected Transition Path

As discussed in Section C.1, requirements for the capabilities offered by RAID do exist. Potential transition partners and target system environments have been tentatively identified and are also expected to emerge in the course of the program. It should be recognized that significant adjustments in the foci of development efforts could be mandated in order to meet the needs of transition partners.

In Phase II, special emphasis will be placed on identifying the requirements associated with the target transition environments and on adjusting system designs and program plans to meet the needs of the chosen transition. The performer in the Experimentation and Evaluation area is expected to support the development of relations with the future RAID user community and prospective transition partners. The System Integration performer and the developers of the ARM and DRM are expected to adjust their efforts as necessary to respond to the requirements of the transition environment and CONOPS. The work of Phase III will be dedicated largely to transition.

# E TECHNICAL OBJECTIVES

## E.1 ADVERSARIAL REASONING

### E.1.1 Scope of Adversarial Reasoning

The purpose of components associated with adversarial reasoning (i.e., Adversarial Reasoning Module, the Red Blue Green Models, the Terrain Model and the Common Operating Picture DB) is to generate, either on-demand or in response to battle situation changes, predictions of red actions and assumption about blue actions.

As information regarding battlefield situation (locations, strengths, postures, actions, etc.) of enemy and friendly troops becomes available or changes, either in the deliberate IPB and wargaming mode or during the execution of the operation, the ARM determines the nature and extent of the change, and the extent to which it confirms, disconfirms or invalidates prior predictions. If an updated prediction is indicated, the ARM generates a new or modified set of predictions, including most dangerous and most likely prediction, each characterized by its likelihood and assumptions on which it is based.

In formulating the predictions, the ARM takes into account such factors as high-level objectives, intents and preferences of the friendly and enemy commanders (these are either entered by the RAID user or estimated and assumed by RAID), physical capabilities and needs of the assets available to both sides, mutual influence of actions of blue and red forces, terrain, weather, non-combatants, cultural and doctrinal aspects, psychological factors affecting troops and commanders, prior evolution of the operation, etc. Description of phased experiments provided in Section D.2.3 offers a more detailed view of the factors and considerations the ARM must take into account.

With this input information, the ARM generates a detailed prediction looking forward anywhere from 30 to 300 minutes (as specified by the user) from the current moment, including sequence of actions, situated in time and space, performed by each element of the enemy force. In the application domain selected for RAID -- battalion and below urban combat -- the granularity of predictions can be exemplified as follows: an example of a force entity is a squad, or a fire team, occasionally even an individual combatant, and an individual platform such as a tank or a helicopter, an example of an action is a movement between two significant terrain features or fire on an enemy force element, or breaching of a wall, an example of a terrain feature is a corner or roof or a floor of a building.

Because the actions of red and blue forces are closely connected and influence each other, the ARM also necessarily generates its estimates of the friendly actions similar to the predictions of enemy actions. These can be seen as assumption or recommendations regarding the friendly course of action.

Additional examples of actions for a specific unit, e.g., a squad, may include: Move (specifying location of an objective, e.g., a building, formation, possibly a path, etc.), Clear a building (specifying the building, possibly a floor, entry position, etc.); Halt (specifying location, possibly formation and posture); Establish a position; Fire and move; Suppressive fire; Break contact, etc.

The ARM outputs should include dependencies between the actions (e.g., a suppressive fire action by one red unit is in support of a move by another red unit), including dependencies between red and blue actions (e.g., an attack by fire by red is a reaction to a move by blue) and a form of rationale or purpose for each task (e.g., a blue unit is to establish position at intersection X in order to block a potential move action by a red unit). An action should include timing estimates (e.g., start and end time windows, absolute or relative to other actions) and the action's impact on the units or terrain involved (e.g., attrition, consumption of supplies, new mobility corridor through a building, etc.).

The predictions of red actions should also have links to the underlying (fused) intelligence data and its pedigree. E.g., a predicted ambush action may be linked to a location and posture of a red unit that has been identified by a fusion system external to RAID, and also linked to a suspected decoy estimated by the Deception Reasoning module of RAID.

The assumptions of blue actions should include enough information to allow the blue commander, if he so desires, to permit a selected subset of these assumptions to become executable orders to the simulated forces and potentially even become a basis for semi-automated translation into orders to real troops. Although the primary function of RAID is to anticipate red actions, the capability to suggest blue actions is a natural, valuable byproduct that can be effectively utilized by an integrated C2 /Intel system.

Because adversarial reasoning cannot in principle provide the exact prediction of the future, the ARM should generate a set of predictions, each accompanied by estimates of its likelihood, and assumptions on which it is based. In particular, the set should include the most likely course of red action and the most dangerous one. The set of predictions should be broad enough to provide the commander with a sense of possible alternative futures, and yet small enough that it can be rapidly reviewed in the tempo of tactical combat. In particular, the ARM should provide a suitable abstraction of each alternative prediction so that it could become a basis for displaying graphically as a rapidly comprehensible, simplified sketch.

User interfaces are not within the scope of adversarial reasoning effort; these will be provided by the system integrator. However, the computational mechanisms for supporting user interactions with RAID, i.e., the means to accept and utilize user guidance and to generate products with semantics that is readily translated into user-friendly displays, are within the scope.

Because it will be primarily the developers of the ARM who will carry the heavy responsibility for proving the initial capabilities of RAID at the end of Phase I, the program assigns those developers the responsibility and authority to design and develop the supporting data stores: the Red Blue Green Models, the Terrain Model and the Common Operating Picture DB. In Phase I, the ARM developers should be unencumbered by considerations of other uses of these data, particularly for DRM purposes. However, in Phase II and beyond, all technology developers and the System Integrator are expected to make the greatest use of these data stores. Thus, the ARM developers should work closely with the System Integrator and the DRM developer to enable the common representation, access and reuse of this information.

### E.1.2 Metrics for Adversarial Reasoning

In addition and in support to the system-level evaluation discussed in Section D.2.3, proposers in this area should define and recommend a self-evaluation approach to be used in in-house experiments and other evaluation events. For illustration purposes, a few examples of metrics that might be suitable for such a self-evaluation are:

- **Red predictions error rate**: false positive - red actions that are predicted but do not occur, false negative - red actions occur but are not predicted. Lower is better.
- **Blue assumption error rate**: false positive – blue actions are assumed but are not appropriate, false negative -- blue actions are necessary but not considered. Lower is better.
- **Coverage**: the fraction of action types, force types, weapon types, effects types that are captured in relevant models and are considered in generating the predictions. Higher is better.
- **Performance**: time required to produce a specified set of predictions. Faster is better.
- **Problem complexity**: the computational complexity (e.g., measured by theoretical size of the search space) of the problems that the component can solve within a permissible time period. Higher is better.
- **Depth of look-ahead**: the time horizon that the component can cover in computing the predictions. Further into future is better.

## E.2 DECEPTION REASONING

### E.2.1 Scope of Deception Reasoning

Continually observing the evolution of the battlefield (as represented in the COP DB) and the evolution of the predictions made by the ARM, the DRM infers: possible concealed enemy force elements or movements of elements, incorrectly identified enemy assets, decoys, actions designed to mislead friendly forces, etc. For example, the DRM may notice that recent actions of the enemy can be best explained if the enemy has moved concealed assets into an ambush position.

If available, the DRM uses user-provided estimates regarding overall strength of concealed enemy assets, types of most likely deceptions, etc. As needed, the DRM uses the ARM to produce predictions under different assumptions and uses such predictions to infer likely concealments and deceptions. The DRM's estimates are also used by the ARM as a corrected view of the battlefield situation. Thus, the ARM may produce a set of predictions based on the enemy situation as it appears to the friendly sensors and fusion system, then the DRM uses this estimates in conjunction with prior observations of enemy actions to estimate that a particular enemy asset has in fact moved to a different location, and then the ARM uses this hypothesis to generate an improved prediction.

The DRM also accesses and uses data and models in the Red Blue Green Models, the Terrain Model and the Common Operating Picture DB. The DRM developers may also find it necessary to build additional stores of data and models if the three mentioned above cannot meet the needs of the DRM.

The primary responsibility and focus of the DRM is on identifying concealments and deception that the enemy executes at the current moment, i.e., at the time when the DRM's product is generated. However, also of interest to the RAID program would be additional capabilities: (a) to foresee an enemy deception that may occur in the future, and (b) to devise a deception scheme that can be suggested to the blue commander.

In formulating its estimates of enemy concealment and deception, the DRM takes into account many of the same factors that are considered by the ARM. However, in addition, the DRM considers the state of red knowledge about the blue, the red beliefs about blue sensor capability, the known red tactics of concealment and deception, the costs and efforts of actions and measures involved in execution of concealment and deception, and the ability of the red to use non-combatants for the purposes of concealment and deception. Description of phased experiments provided in Section D.2.3 offers a more detailed view of the factors and considerations the DRM must take into account.

The granularity of the DRM-generated estimates should be comparable to the ARM's.

Like the ARM, the DRM should generate several alternative estimates of red concealments and deception, if multiple alternatives are indeed likely. Each estimate should be accompanied by its likelihood, and assumptions on which it is based. Elements of the estimates should be linked to the underlying evidence.

Similarly to Adversarial Reasoning, user interfaces are not within the scope of deception reasoning. However, the computational mechanisms for supporting user interactions with RAID, i.e., the means to accept and utilize user guidance and to generate products with semantics that is readily translated into user-friendly displays, are within the scope.

Unlike the ARM, in Phase I, the DRM is not expected to be integrated into the overall RAID system and is not subject to system-wide evaluation. Thus, during Phase I, the developers of the DRM will have the necessary freedom to experiment with alternative representation and algorithmic approaches. Moving into Phase II, considerations of using data and models in common with the ARM will become important.

### E.2.2 Metrics for Deception Reasoning

In addition and in support to the system-level evaluation discussed in Section D.2.3, proposers in this area should define and recommend a self-evaluation approach to be used in in-house experiments and other evaluation events. For illustration purposes, a few examples of metrics that might be suitable for such a self-evaluation are:

- **Red deceptions error rate**: false positives, e.g., the DRM claims a red squad is concealed in a building but there is no such squad there; false negatives - there is in fact a red squad concealed in the building but the DRM fails to identify it. Lower is better.
- **Coverage**: the fraction of action types, force types, weapon types, effects types that are captured in relevant models and are considered in generating the estimates. Higher is better.
- **Performance**: time required to produce a specified set of estimates. Faster is better.
- **Problem complexity**: the computational complexity (e.g., measured by theoretical size of the search space) of the problems that the component can solve within a permissible time period. Higher is better.

## E.3 OVERARCHING TECHNICAL CHALLENGES OF ADVERSARIAL REASONING AND DECEPTION REASONING

Both Adversarial Reasoning and deception Reasoning components must address several overarching challenges. Proposers are to explain how their technical approaches would handle:

- Tight interdependence, coupling of blue and red actions. Blue course of action cannot be assumed or generated independently from the red course of action, and vice versa.
- Blue knowledge of red assets and actions is inevitably limited. Observations as well as interpretations of the observations are subject to a significant degree of errors and latency. The same is true of red with respect to blue. Observations are also functions of actions undertaken by the forces, and therefore actions and observations are tightly coupled.
- In addition to partial, delayed and often erroneous observations, the battlefield knowledge is limited by a purposeful, continuous, aggressive, intelligent concealment and deception.

- It is not enough to consider the most dangerous course of action, i.e., the one that can be expected to bring the greatest degree of success to the red force. The actions of the red force (as well as blue force) are heavily influenced by force training and experiences, by doctrinal, cultural and psychological factors. Thus the most likely course of action can be significantly different from the theoretically most advantageous one.
- The already high complexity of the problem is amplified by the complex urban terrain that offers a high density of threats and opportunities for forces. Further, the terrain itself is dynamic because it is modified by human actions.
- The presence of non-combatants on the battlefield must be explicitly considered. The behavior of non-combatants, the need to minimize the collateral damage, and the potential use and manipulation of non-combatants by unscrupulous adversary – all add yet another layer of complexity to the problem.
- Fire and maneuver of forces are not the only actions that must be carefully considered. Intelligence gathering, communications, and logistics (including casualty evacuation) are tightly coupled with fire and maneuver and are inseparable elements of the overall problem.
- The scale of the computational problem is immense and solutions must be generated in near real-time.
- To be of practical value, a successful technical approach must allow for easy modification and extension of the coverage, i.e., it should be easy to add new types of terrain elements, force units, weapons, actions, etc. without modifying the entire system or redesigning the algorithms.

## E.4 CANDIDATE TECHNICAL APPROACHES TO ADVERSARIAL REASONING AND DECEPTION REASONING, AND RELATED CHALLENGES

Any technology or a combination of technologies that addresses the problem and the challenges discussed in relation to the Adversarial Reasoning and Deception Reasoning, and which can be developed in a manner consistent with the RAID program concept, would be of interest to this BAA. Potential candidate groups of technologies include but are not limited to:

- **Game-theoretic and game-playing** approaches: Devising sequences of actions for both red and blue forces in a manner that assumes both sides strive to maximize the achievement of their respective objectives. Such approaches must pay special attention to the need of solving very large scale problems in near real time, recognizing the stochastic nature of outcomes for most moves, and addressing partial observability and deception issues.

- **Adversarial planning**: Forming plans for both red and blue actions that lead to the achievement of the respective desired goals while preventing the attainment of the goals of the other side; often using significant amounts of domain-specific knowledge. An important challenge in application of such approaches is to make use of relatively few elements of domain-specific knowledge, as domain-independent as possible and easy to acquire, modify and manage.
- **Deception discovery**: Analyzing the information state from risk-sensitive perspective to determine which of alternative hypotheses would benefit the enemy the most if accepted by the friendly forces; analyzing the significance of preconditions for feasibility of alternative enemy course of action to identify the once that are more likely to be subject of deceptions; comparing earlier expectations with current evidence to find unexplainable deviations. Such approaches would have to find ways to deal with the complex, multi-dimensional nature of the RAID problem; to work without the benefit of relying on significacnt amount of human analyst's input (if any), and cooperate with adversarial reasoning component that may use a very different representational paradigm.
- **Pattern recognition**: Identifying patterns and anomalies in spatial and temporal locations, movements and other actions of the red force that could indicate concealment, deception and future intended course of action; often using learning techniques to build and extent the repertoire of such patterns. Among the challenges relevant to such approaches are the need for effective generalization, especially in very complex terrain; the need to align pattern analysis with enemy's objectives and goals; and ways to prevent the red from using such pattern recognition means as effective approach to deceiving the blue.

## E.5 SYSTEM INTEGRATION

The purpose of the System Integration effort is to provide a framework in which all components of the RAID system, the experimental testbed, and the transition systems can interact effectively. This effort will include formulating and designing the overall architecture, interfaces, representations and formats in close cooperation with other developers within the RAID program. The specific system components that the system integrator will build include but are not limited to RAID User Input Interface, RAID System Input Interface, RAID User Output Interface, RAID System Output Interface, Past Predictions DB. The BAA is looking for highly cost-effective solutions to the system integration needs; unnecessary technical innovations or technical risks in the integration infrastructure are not desired. The proposer should also note that the first fully working integration should be accomplished quite early in the program – see the schedule of experiments in Section D.2.3.

Specific technical challenges involved in the system integration effort include but are not limited to:

### E.5.1 Combat Simulation System

System Integrator is responsible for identifying and recommending (in the response to this BAA) a specific software system that would be most suitable to technical and programmatic goals of RAID, modifiable to suit the evolving needs of experimentation process, and within the experience and skill set of the proposer. It is unlikely that one can identify an existing simulation system that would meet all the needs of RAID experimentation, particularly the sufficient representation of the urbanized terrain, the entity behaviors required for the RAID problem, the non-combatant representation and behaviors, the APIs and user GUIs. Thus, the proposer must identify the simulation system that can be readily modified to address such inevitable shortfalls; identify the shortfalls that are immediately obvious, and propose technical approaches to remedy the shortfalls in a time- and cost-effective manner.

The system integrator must provide the technology developer with easy-to-use interfaces to the simulation system; the intent is to minimize the investment of time and resources necessary for the technology development teams to learn and use the system interfaces. It is important that the simulation system should be available to the technology developers for the purposes of performing continuous in-house testing of their software. Providing the technology developers with such a capability is also the responsibility of the system integrator. It should be preferably an unclassified version of the simulation system and should be available to the developers either by installing at their development sites or by accessing remotely (without imposing unusual networking requirements) a simulation system server maintained by the system integrator.

To enable the technology developers to analyze and debug the performance of their software, it is necessary to provide a means for play back and a game analysis capability if they are not already available within the selected simulation system. Because some of the RAID experiments (e.g., Phase I) rely on restricting the repertoire of actions / behaviors available to the operators, the system integrator will have to build some means to control such a repertoire. If the proposed combat simulation system is such that the Government owns the requisite rights, the proposer can assume that the combat simulation system software will be supplied as GFP; otherwise the proposer should plan on acquiring the necessary software.

### E.5.2 Experimentation and Evaluation Environment

In coordination with the performer of experimentation and evaluation efforts, the system integrator is to build and integrate the physical and software environment of the RAID experiments. This includes acquiring and integrating the necessary hardware, software, networking and facilities for experiments, including the necessary observation and data collection instrumentation and after action review means; and implementing elements of the experimental scenario and terrain as designed by the Experimentation and Evaluation performer. Although it is likely that the terrain datasets would be provided by the Government, but the system integrator should also be prepared to produce the necessary terrain dataset, or to reformat the one provided by the Government. It is also possible that the physical facilities would be provided by a

Government organization. Therefore, the system integrator should plan for installing the computer hardware, software and networking equipment at such a facility and also consider the possibility that different locations and facilities will be used for different experiments. This requires provision for inexpensive and rapid transportation, assembly, on-site test and disassembly of experimental setup (hardware, software, auxiliary equipment).

### E.5.3 User Interfaces

The user of RAID will require user interfaces to input information to RAID, as well as to view, examine and process the information arriving from RAID. A key challenge is to build easy-to-use, easy –to-learn, un-encumbering interfaces that use very little time to accomplish user's goals and allowing a number of interactions, including but not limited to: input red and blue objectives and priorities; modify red and blue combatant and action parameters, input diverse ROEs, generate, manage, edit and use doctrinally compliant graphic and textual products. For the purpose of RAID experiments in Phase I and II, these user interfaces should be optimized for easy of executing the experiments and should be designed and implemented either as extensions or transparent additions to the combat simulation system organic user interfaces. For the purposes of transition efforts in Phase III, the system integrator is to design and build system and user interfaces required for integration of RAID capability into target transition environment; this entail challenges and constraints associated with the systems of that environment. The system integrator will be responsible for system and requirements analysis and well as design and implementation of such interfaces. Matching the user CONOPS, and GUI look and feel of the target transition systems will be important.

## E.6 EXPERIMENTATION AND EVALUATION

The purpose of the experimentation and evaluation effort is to provide an independent design, execution and evaluation of RAID experiments. This effort will include designing: the experiments, the scenarios, the requisite datasets, the detailed metrics, the methodology and instrumentation for data collection. This effort also includes execution of the experiments: provision of highly competent human players, training and management of the players, overall scheduling, management and control of all experimentation effort, collection and analysis of data, preparation and presentation of evaluations and recommendations to the program members and management. The experimentation performer is also expected to act as the source of domain expertise and as liaison to potential users and transition partners.

The BAA is looking for highly cost-effective solutions to the RAID experimentation needs. The proposer should also note that the first experimental wargames should be accomplished quite early in the program – see the schedule of experiments in Section D.2.3. Furthermore, to provide technology developers with insights into the general nature of the domain and wargame requirements, the experimentation performer will be required to perform several illustrative manual wargames as samples for technologists no later than 30 days after the contract.

Because there is a strong possibility that the Government will provide at least part of the experiment players, the experimentation provider should be prepared to integrate and manage a players team that consists partly of Government personnel and partly of the personnel hired by the performer.

# F PROPOSAL MANAGEMENT

## F.1 GENERAL INFORMATION

### F.1.1 Definition of BAA as Contemplated in the FAR

The information provided in this Proposer Information Pamphlet (PIP), in addition to that provided in the FedBizOps BAA 04-16, constitutes a Broad Agency Announcement as contemplated in the FAR 6.102 (d)(2)(i). The FedBizOps announcement and this document are available online at http://www.darpa.mil/ixo/solicitations/raid/index.htm.

### F.1.2 BAA Correspondence

DARPA will use electronic mail for all technical and administrative correspondence regarding this BAA. Administrative, technical or contractual questions should be sent via e-mail to BAA04-16@darpa.mil and must be received by 12:00 NOON (ET) 13 April 2004. All requests must include the name, address, and phone number of a point of contact. Technical and contractual questions should include the originator's full name, email, and postal address in the text.

### F.1.3 Frequently Asked Questions

All questions and answers of relevance to the community will be posted to a "Frequently Asked Questions (FAQ)" accessible at http://www.darpa.mil/ixo/solicitations/raid/index.htm.

### F.1.4 Briefing to Industry

DARPA intends to hold a Briefing to Industry for the RAID program on 17 March 2004 at the Executive Conference Center, 3601 Wilson Blvd Suite 600, Arlington VA. Interested organizations should register by 15 March 2004, through the web at https://www.tfims.darpa.mil/bti/.

### F.1.5 Multiple Proposals

Proposers responding to multiple areas of this BAA should submit one complete proposal per topic. Each proposed effort should stand alone, and not be predicated on the award of any other effort.

### F.1.6 Contract types

Awards are anticipated to be in the form of Procurement Contracts or Other Transactions. Grants or Cooperative Agreements are also possible.

## F.2 SUMMARY OF IMPORTANT DATES

Table 2 provides a schedule of important events and dates associated with the RAID BAA:

| DATE | EVENT | URL |
|---|---|---|
| 1 March 2004 | FedBizOpps Announcement and Proposer Information Package published | http://www.darpa.mil/ixo/solicitations/raid/index.htm |
| 17 March 2004 | DARPA Briefing to Industry on proposal process and BAA technical topics | https://www.tfims.darpa.mil/bti/ |
| 14 April 2004 | Proposal registrations due at DARPA | http://www.tfims.darpa.mil/baa |
| 21 April 2004<br>1500 Hours | Proposals due at DARPA | http://www.tfims.darpa.mil/baa |
| 21 May 2004 | Selections expected to be announced | |
| Aug 2004 | Kick-Off meeting | |

*Table 2. Significant BAA events and deadlines*

## F.3 SUBMISSION GUIDELINES

Proposal abstracts ARE NOT requested in advance of full proposals. DARPA will employ an electronic upload process for proposal submissions for BAA 04-16. Performers may find guidance for proposal submission at http://www.darpa.mil/ixo/solicitations/raid/index.htm.

Organizations planning to submit proposals must register at http://www.tfims.darpa.mil/baa**.** Only the lead or prime organization should register. One registration per proposal should be submitted. This means that an organization wishing to submit multiple proposals should complete a single registration for each proposal. The deadline for registration is 14 April 2004. By registering, the Proposer has made no commitment to submit.

## F.4 T-FIMS REPORTING REQUIREMENTS

Technical-Financial Information Management System (T-FIMS) is a DARPA/IXO developed interactive reporting system which facilitates technical and expenditure reporting on line. Information on this system may be found at http://www.tfims.darpa.mil/. Proposers shall satisfy the T-FIMS reporting requirements presented at http://www.tfims.darpa.mil/T-fims_req.doc/ as part of their proposed deliverables.

## F.5 SECURITY

The technologies for the RAID Program will be developed in an UNCLASSIFIED environment, especially in the early phases of the program. However, the RAID experiments will eventually produce classified data and results. Hence, the RAID Program will require periodic development, testing, and demonstration in classified facilities and ranges in the later phases. Therefore, proposers must show that the personnel needed for integrated evaluations, or who will have access to RAID experiment results, have SECRET clearances. They must also show that they (or a partner/subcontractor) have facilities available to store and, if needed, process data at the SECRET level. See the attached DOD Contract Security Classification Specification (DD Form 254) for additional security requirements associated with this program.

All proposed efforts must meet the requirements established by U.S. National Security and Export Control Laws. All prime contractors (in the Experimentation and Evaluation and System Integration areas) must be a U.S. company with SECRET-level capabilities. Performers in the technology areas must be U.S. companies/institutions. As it is deemed appropriate to the statement of work and National Security concerns, contractors employing foreign nationals may perform development tasks that constitutes basic research.

Proposals submitted in response to this BAA shall be UNCLASSIFIED. If the proposer finds it necessary to submit classified documents, these will NOT be included in the review process and must be submitted in accordance with the following guidance:

For Collateral Classified Information: Use classification and marking guidance provided by previously issued security classification guides, the Information Security Regulation (DoD 5200.1-R), and the National Industrial Security Program Operating Manual (DoD 5220.22-M) when marking and transmitting information previously classified by another original classification authority. Classified information at the Confidential and Secret level may only be mailed via U.S. Postal Service (USPS) Registered Mail or USPS Express Mail. All classified information will be enclosed in opaque inner and outer covers and double wrapped. The inner envelope shall be sealed and plainly marked with the assigned classification and the addresses of both sender and addressee. The inner envelope shall be addressed to:

Defense Advanced Research Projects Agency
Attn: Information Exploitation Office
Reference: BAA 04-16
3701 N. Fairfax Dr
Arlington VA 22203-1714

The outer envelope shall be sealed with no identification as to the classification of its contents and addressed to:

Defense Advanced Research Projects Agency
Security and Intelligence Directorate, Attn: CDR
3701 N. Fairfax Dr
Arlington VA 22203-1714

All Top Secret materials should be hand carried via an authorized, two-person courier team to the DARPA Classified Document Registry (CDR)

# G PROPOSAL EVALUATION

## G.1 GENERAL CONSIDERATIONS

Proposers are encouraged to submit concise, but descriptive, proposals. The Government reserves the right to select for award all, some, or none of each of the proposals received. All responsible sources capable of satisfying the Government's needs may submit a proposal. Historically Black Colleges and Universities (HBCUs) and Minority Institutions (MIs) are encouraged to submit proposals and join others in submitting proposals; however, no portion of this BAA will be set aside for HBCU and MI participation due to the impracticality of reserving discrete or severable areas of technology for exclusive competition among these entities.

It is the policy of DARPA to treat all proposals as competitive information and to disclose the contents only for the purposes of evaluation. The Government may use selected support contractor personnel to assist in administrative functions only. For this solicitation, non-Government advisors from Solers, Inc., Schafer Corporation, CACI International, and McNeil Technologies, who have signed appropriate non-disclosure and conflict of interest statements, may assist in the proposal administration when their assistance is required. However, they will not participate in the final source selection process.

Proposers are advised that only contracting officers are legally authorized to contractually bind or otherwise commit the Government.

## G.2 CRITERIA FOR AWARDS

The selection of one or more sources for awards will be based on an evaluation of a Proposer's response (both technical and cost aspects) to determine the overall merit of the proposal in response to the announcement. Proposals shall be evaluated against the following criteria, in descending order of importance:

G.2.1 Technical Depth and Feasibility

- Understanding of the current and projected research and development in predictive analysis
- Understanding the challenges of the problem domain and their technical ramifications
- Soundness of the technology approach at the component and systems levels
- Potential for revolutionary advancements in addressing the technical challenges
- Justification of design choices as compared to alternative techniques

G.2.2 Consistency with RAID Program Concepts

- Consistency with the RAID system and program concepts
- Depth and specificity of the proposed effort's system and program concepts
- Precision and coverage of the proposed effort's metrics
- Plan for collaborating with other technology developers and the System Integrator, as described herein

G.2.3 Cost Realism and Value of Proposed Work to the Government

- The total cost relative to benefit
- The realism of cost levels for facilities and staff
- The cost-effective use of existing equipment and software
- Competitive costs on procurements

G.2.4 Personnel and Corporate Capabilities and Experience

- Qualifications and experience of proposed technical personnel
- Availability of personnel for the duration of the contract
- Soundness of the team composition, personnel assignments and expertise management
- Ability to collaborate in off-site integration and field experimentation
- Adequacy of proposed facilities

# H PROPOSAL CONTENT

## H.1 GENERAL INFORMATION

Technical and cost proposals must be submitted as separate volumes (Technical as Volume I, Cost as Volume II), and must be valid for 180 days.

This BAA solicits proposals from all interested and qualified sources. Foreign participants and/or individuals may participate to the extent that such participants comply with any necessary Non-Disclosure Agreements, Security Regulations, Export Laws, and other governing statutes applicable under the circumstances.

Proposals with fewer than the maximum number of pages will not be penalized. Proposals exceeding the page limit will not be reviewed beyond the maximum page limit. Non-cost information incorporated into the unrestricted size Volume II cost proposal will not be considered. Proposers are encouraged to submit concise, but descriptive, proposals.

Proposal questions should be handled according to the process described in Section F. Proposers are advised that only contracting officers are legally authorized to contractually bind or otherwise commit the Government.

Proposers should apply the restrictive notice prescribed in the provision at FAR 52.215-12, Restriction on Disclosure and Use of Data, to trade secrets or privileged commercial and financial information contained in their proposals.

It is DARPA's policy to treat all proposals as competitive information and to disclose the contents only for the purposes of evaluation. The Government may use selected support contractor personnel to assist in administrative functions only.

### H.1.1 Procurement Integrity, Standards Of Conduct, Ethical Considerations

Certain post-employment restrictions on former federal officers and employees may exist, including special Government employees (Section 207 of Title 18, United States Code). If a prospective Proposer believes that a conflict of interest exists, the situation should be raised to the DARPA Contracting Officer specified in Section 1.7 before time and effort are expended in preparing a proposal. All Proposers and proposed sub-contractors must therefore affirm whether they are providing scientific, engineering, and technical assistance (SETA) or similar support to any DARPA technical office(s) through an active contract or subcontract. All affirmations must state which office(s) the Proposer supports and identify the prime contract numbers. Affirmations shall be furnished at the time of proposal submission. All facts relevant to the existence or potential existence of organizational conflicts of interest (FAR 9.5.) must be disclosed. The disclosure shall include a description of the action the Proposer has taken or proposes to take to avoid, neutralize, or mitigate such conflict.

The Government intends to comply with procurement integrity statutes and regulation and DFARS 252.227-7016 in its treatment of information submitted in response to this BAA solicitation and marked with the individual or company's legend (see paragraph 4.1.1 below). The proposer is cautioned, however, that portions of the proposal may be subject to release under terms of the Freedom of Information Act (FOIA), 5 U.S.C. 552, as amended. In accordance with FOIA regulations, the proposer will be afforded the opportunity to comment on, or object to, the release of proposal information.

### H.1.2 Subcontracting

Pursuant to Section 8(d) of the Small Business Act (15 U.S.C. 637(d)), it is the policy of the Government to enable small business and small disadvantaged business concerns to be considered fairly as subcontractors to contractors performing work or rendering services as prime contractors or subcontractors under Government contracts, and to assure that prime contractors and subcontractors carry out this policy. Each Proposer who submits a contract proposal and includes subcontractors is required to submit a subcontracting plan IAW FAR 19.702(a) (1) and (2) with their proposal. The plan format is outlined in FAR 19.704.

## H.2 TECHNICAL PROPOSAL

Each technical proposal shall be limited to a total of 70 (seventy) or fewer pages (including cover, index, charts, figures and tables). Each proposal shall include the following sections and items.

| SECTION | PAGE LIMIT | TOPICS |
|---|---|---|
| Cover page | 1 | Offer identification |
| Table of contents | 2 | Proposal outline and page counts |
| Proposal roadmap | 1 | Summary of key elements of the offer |
| Problem statement | 5 | Challenges of predictive analysis<br>Limitations of current approaches<br>Opportunities for improvement |
| Program concept | 15 | Proposed enabling capabilities<br>Proposed capability development<br>Proposed performance metrics |
| Technical approach | 25 | Survey of the current state of the art<br>Approach for technology development<br>Key ideas for future development<br>Self-evaluation methodology |
| Management plan | 20 | Statement of work<br>Program schedule<br>Deliverables<br>Cost summary<br>Personnel<br>Related experience<br>Facilities<br>Security plan<br>Statement of rights claimed for software deliverables |
| Evaluation factors | 1 | Summary of proposer's self-assessment of evaluation factors |

*Table 3. Summary Of Required Technical Proposal Contents.*

Format specifications include 12 pitch or larger type, single spaced, single-sided, and 8.5 by 11 inches with 1 inch margins all around the page. Each section should begin at the top of a page. All pages shall be numbered. The page limitation includes all attachments, etc. Pages in excess of this limitation will not be considered by the Government.

Proposers should include material contained in the PIP only by reference (e.g., [PIP E.2.3]), not by verbatim quotes nor by simple paraphrasing. Specific examples of problems, approaches, or goals are preferred to qualitative generalities.

### H.2.1 Cover Page

The cover page should uniquely identify the offer, including at least the following information:

- BAA number
- Assigned DARPA control number
- Proposal title
- BAA category addressed (e.g., Adversarial Reasoning, Deception Reasoning, System Integration, or Experimentation and Evaluation)
- Proposer's single point of contact for all correspondence and communications

### H.2.2 Section A: Table of Contents

The Table of Contents should, at a minimum, provide an index to all primary and secondary headings in the technical proposal.

### H.2.3 Section B: Proposal Roadmap

This page should summarize, preferably in bullet format, the major points and themes of the proposal, in terms of a) problem addressed, b) program structure, c) technical approach, and d) management plan.

### H.2.4 Section C: Problem Statement

This section should define and delineate the problem to be addressed by the proposed effort. It should define the aspects of predictive analysis in support of urban operations that pose the greatest technical challenges to the proposer; identify areas where increased automation of the type proposed can make the greatest contribution; and describe the military payoff if the proposed effort succeeds.

### H.2.5 Section D: Program Concept

This section should establish the intellectual framework for the proposed effort in three parts:

**Section D.1**: **Proposed Enabling Capabilities.** Define the capabilities to be in place at the end of the program, either as functions, services, or procedures. Explain relationships among them, and relationships to other elements of RAID. Amplify, and recommend improvements to, the RAID system concept.

**Section D.2**: **Proposed Capability Development.** Explain how the capabilities defined in Section D.1 may evolve over time, either through a development sequence, performance enhancement, or the phased introduction of new technology. Show how this evolution supports the RAID program-level goals, and recommend amplifications and improvements to the RAID program concept.

**Section D.3**: **Proposed Performance Metrics.** Define the metrics by which the effort will internally assess progress towards the final set of capabilities. For component development efforts, explain how these metrics relate to the program-level metrics. For integration and experimentation, explain how these metrics capture the level of support provided to the component developers. For each metric, project specific values that can be expected to be achieved at the end of each Phase, and the assumptions on performance required of other program elements in order for these projections to be valid.

### H.2.6 Section E: Technical Approach

Explain, with specific examples relevant to predictive analysis for urban operations if possible, the key technical ideas on which the program concept is based. Include at least:

- A summary of past and current efforts on which the proposed effort builds, or which were rejected as part of the design process;
- The baseline capability proposed to accomplish the program technical objectives for each phase. For component developers, emphasize algorithms, interfaces, data models, and capabilities that would most influence system design and experimentation efforts. For system integrators and experimenters, emphasize the technical and procedural frameworks into which component developers will be asked to fit.
- Key ideas that will form the basis for progress beyond the baseline capability. Include specific examples illustrating how the ideas address crucial factors encountered in predictive analysis. Emphasize any experimental evidence, formal theories, performance analyses, or quantitative tradeoffs that lend weight to claims of performance.
- The process that the proposer will use to assess the rate of progression of technical capability over time.

This is the critical section of the proposal. It must address the specific technical approach, technical rationale and strategy for accomplishment of technical goals, and should elaborate upon (but not be redundant with) Section D. The technical rationale section must include technical arguments to substantiate claims made in Section D. Include comparisons with other ongoing research indicating both advantages and disadvantages of the proposed effort/approach. Include a discussion of design decisions made.

Proposals from both Technology Component developers and System Integrators should include detailed descriptions of capability goals, performance goals, informal evaluations and formal evaluations for their individual modules and systems. These plans should include estimates of the amount and kind of data needed to conduct evaluation. These goals and evaluation plans will be reviewed and coordinated in program-wide meetings after program initiation.

Proposers can include references, including web addresses, to publications and other materials, such as for example illustrative graphics and video clips of system demonstrations, which substantiate their technical claims. However, the review of such materials is at the discretion of the reviewer. Therefore, the proposal itself must be the primary and sufficient source of information about the proposer's technical approach.

### H.2.7 Section F: Management Approach

This section should describe the tasks and resources offered to carry out the technical approach described.

**Section F.1: Statement of Work.** In plain English, clearly define the technical tasks/subtasks to be performed, their durations, and dependencies among them. For each task/subtask, provide:

1) A short description of the objective of task;
2) A short description of the approach to be taken to the task;
3) Identification of which organization is responsible for task execution;
4) The resources allocated to each task (funds, person-months and duration);
5) The exit criterion for each task - a product or event that defines its completion

**Section F.2**: **Program Schedule.** Provide a GANTT charts of the major activities and milestones for the proposed effort, aligned with the three Phases of the RAID program. Indicate delivery of baseline technologies suitable for the integration and experimentation process.

**Section F.3**: **Deliverables.** Define deliverables associated with the proposed research, both software (e.g., to the System Integrator) and reporting. See also Section F.4 of this PIP.

**Section F.4**: **Cost Summary.** Summarize the cost of the proposed effort as indicated by the two tables here. Funding levels have not been predetermined for this program. Therefore, cost proposals must reflect accurate estimates fo staffing and other costs. For costing, assume a program start date of 1 October 2004, so that contract years align with Government fiscal years. However, the RAID program will commence as quickly as contracts can be signed. Note that RAID plans to end 3 years after contract start.

| Cost Element | GFY 05 | GFY 06 | GFY 07 |
| --- | --- | --- | --- |
| Technical labor[1] | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |
| Administrative labor[2] | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |
| Other direct charges | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |
| Indirect charges | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |
| Fee | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |
| SubTotal | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |
| Option 1 | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |
| Option 2 | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |
| TOTAL | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |

*Table 4. Summary Of Funding Request By Cost Element.*

| Organization | GFY 05 | GFY 06 | GFY 07 |
| --- | --- | --- | --- |
| Prime | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |
| Subcontractor A | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |
| Subcontractor B | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |
| Subcontractor C | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |
| Total | $x,xxx,xxx | $x,xxx,xxx | $x,xxx,xxx |

*Table 5. Summary Of Funding Request By Performing Organization.*

**Section F.5**: **Personnel.** Provide a one-page summary of the qualifications of each person proposed for this effort. Describe their education, clearance level, work history, specific achievements relevant to the RAID Program, and areas of expertise. Clearly state the portion of each person's time that will be dedicated to RAID during Phase I. Do not include resumes for people who will spend less than 50% of their time on RAID. Smaller teams of dedicated full-time developers are preferable to larger teams of part-time participants. If the expertise is resident in only 1-2 key personnel, the proposer should identify risk reduction measures.

**Section F.6**: **Related Experience.** Provide short summaries of related work accomplished or in progress by any member of the proposer's team that offers technology or transition potential for RAID. Emphasize projects on which proposed staff have worked, and indicate this fact when applicable.

[1] Technical labor includes designers, software engineers, analysts, and other staff with degrees in science or engineering who contribute directly to the technical objectives of the program.

[2] Administrative labor includes contractual, financial, secretarial, and other staff with non-technical degrees who support the technical staff.

**Section F.7**: **Facilities.** Briefly describe corporate facilities that will be available to support this effort.

**Section F.8**: **Security Plan.** Briefly describe the plan to place people into the secure experimentation facility during classified experiments and evaluations, and to process data collected and derived from those evaluations.

**Section F.9: Submission Handling/Rights In Technical Data And Computer Software/Patent Rights – General.**

**Noncommercial Items: (Technical Data and Computer Software)**

Proposers responding to this BAA shall identify all noncommercial technical data, and noncommercial computer software that it plans to generate, develop, and/or deliver under any proposed award instrument in which the Government will acquire less than unlimited rights, and to assert specific restrictions on those deliverables. Proposers shall follow the format under DFARS 252.227-7017 for this stated purpose. In the event that Proposers do not submit the list, the Government will assume that it automatically has "unlimited rights" to all software the Proposer has produced under this contract. The Government may use the list during the source selection evaluation process to evaluate the impact of any identified restrictions, and may request additional information from the Proposer, as may be necessary, to evaluate the Proposer's assertions. If no restrictions are intended, then the Proposer should state "NONE."

Table 6 shows a sample format for complying with this request.

| **NONCOMMERCIAL** | | | |
|---|---|---|---|
| Technical Data Computer Software To be Furnished With Restrictions | Basis for Assertion | Asserted Rights Category | Name of Person Asserting Restrictions |
| (LIST) | (LIST) | (LIST) | (LIST) |

*Table 6 Noncommercial Items*

**Commercial Items: (Technical Data and Computer Software)**

Proposers responding to this BAA shall identify all commercial technical data, and commercial computer software that may be embedded in any noncommercial deliverables contemplated under the research effort, along with any applicable restrictions on the Government's use of such commercial technical data and/or commercial computer software. In the event that Proposers do not submit the list, the Government will assume that there are no restrictions on the Government's use of such commercial items. The Government may use the list during the source selection evaluation process to evaluate the impact of any identified restrictions, and may request additional information from the Proposer, as may be necessary, to evaluate the Proposer's assertions. If no restrictions are intended, then the Proposer should state "NONE."

Table 7 shows a sample list for complying with this request.

| COMMERCIAL | | | |
|---|---|---|---|
| Technical Data Computer Software To be Furnished With Restrictions | Basis for Assertion | Asserted Rights Category | Name of Person Asserting Restrictions |
| (LIST) | (LIST) | (LIST) | (LIST) |

*Table 7 Commercial List*

Where the rights to any technical data/computer software are more restrictive than "Government Purpose Limited Rights" as defined by the FAR, provide a plan for mitigating the impediments such restrictions pose to transition to field users.

### H.2.8 Section G: Evaluation Factors

This page should summarize, preferably in bullet format, the proposer's self-evaluation of the proposal against the factors defined in Section G of this PIP.

## H.3 COST PROPOSAL

For estimating purposes, proposers should assume the 1 October 2004 start date.

There is no page limit for the cost proposal.

The government is currently in ongoing discussions with one or more federal agencies to possibly provide experimentation support in the form of facilities, equipment, subject matter experts, experiment and simulation operations, experiment design and control, experiment data collection and analysis, and simulation modification. For proposals in the area of Experimentation and Integration, please provide cost options with and without government support. For example, provide facility costs for experimentation at a contractor facility versus a government facility; provide computer workstations costs (hardware, software, and sys admin support) for experimentation at a contractor facility versus a government facility; etc. Please cost out as many options as possible and do the cost analysis for each year, since government support may vary by year.

### H.3.1 Cover Page

- Name and address of Proposer (include zip code);
- Name, title, and telephone number of Proposer's point of contact;
- Award instrument requested: cost-plus-fixed-fee (CPFF), cost-contract--no fee, cost sharing contract--no fee, or other type of procurement contract (specify), grant, agreement, or other award instrument;
- Place(s) and period(s) of performance;
- Funds requested from DARPA for the Base Effort, each option and the total proposed cost; and the amount of cost share (if any);
- Name, mailing address, telephone number and Point of Contact of the Proposers cognizant government administration office (i.e., Office of Naval Research (ONR) - if requesting a grant, or Defense Contract Management Agency (DCMA) - if requesting other than a grant) (if known);
- Name, mailing address, telephone number, and Point of Contact of the Proposer's cognizant government audit agency (i.e. Department of Health and Human Services (DHHS) - if requesting a grant, or Defense Contract Audit Agency (DCAA) - if requesting other than a grant) (if known);
- Any Forward Pricing Rate Agreement, other such Approved Rate Information, or such other documentation that may assist in expediting negotiations (if available);
- Contractor and Government Entity (CAGE) Code,
- Dun and Bradstreet (DUN) Number;
- North American Industrial Classification System (NAICS) Number [NOTE: This was formerly the Standard Industrial Classification (SIC) Number]; and,
- Taxpayer Identification Number (TIN).
- All subcontractor proposal backup documentation to include items a. through l. above, as is applicable and available).

### H.3.2 Detailed cost breakdown

The detailed cost breakdown is to include:

- Total program cost broken down by months within a government fiscal year (GFY) [Note: Government Fiscal Year runs from October 1st to September 30th] and Base and Options; further broken down by major cost items (direct labor by category, subcontracts, materials, travel, other direct costs, overhead charges, etc.). See Table 8 below for an example format;
- Costs of major program tasks by year and month; (See example)
- An itemization of major options (labor by category, travel, materials and other direct costs) and equipment purchases by year and month;

- An itemization of major subcontracts (labor by category, travel, materials and other direct costs) and equipment purchases;
- A summary of projected funding requirements by month (see Table 9); and
- The source, nature, and amount of any industry cost sharing, if applicable. Where the effort consists of multiple phases that could reasonably be partitioned for purposes of funding, these should be identified as options with separate cost estimates for each.

### H.3.3 Supporting cost and pricing information

Provide supporting information in sufficient detail to substantiate the cost estimates above. Include a description of the method used to estimate costs and supporting documentation. Provide the basis of estimate for all proposed labor rates, indirect costs, overhead costs, other direct costs and materials, as applicable.

| | GFY xx | | | | | | | | | | | | | GFY yy | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **BASE** | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | TOTAL | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | TOTAL |
| Direct Labor - Dollars | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Direct Labor - Hours | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Travel | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Equipment | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Subcontractors | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Other ODCs | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Overhead | | | | | | | | | | | | | | | | | | | | | | | | | | |
| G&A | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Fee/Profit | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Total** | | | | | | | | | | | | | | | | | | | | | | | | | | |

*Table 8. Example Detailed Cost Format*

| | GFY 04 | | | | | | | | | | | | | GFY 05 | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | TOTAL | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | TOTAL |
| BASE | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OPTION 1 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OPTION 2 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Total** | | | | | | | | | | | | | | | | | | | | | | | | | | |

*Table 9. Example Cost Summary Format*

# I ACRONYMS

| | |
|---|---|
| AAR | After action report |
| ACO | Administrative Contracting Officer |
| ARM | Adversarial Reasoning Module |
| ASAS-L | All Source Analysis System – Light |
| BAA | Broad Agency Announcement |
| BCBL | Battle Command Battle Lab |
| BDA | Battle Damage Assessment |
| BFT | Blue Force Tracker |
| BLUFOR | Friendly, Blue Forces |
| BTI | Briefing to Industry |
| C2 | Command and Control |
| CAS | Close Air Support |
| CDA | Commanders Digital Assistant |
| CDR | Classified Document Registry |
| CMDR | Commander |
| CMO | Contracts Management Office (at DARPA) |
| CONOPS | Concept of Operations |
| COP | Common Operating Picture |
| COTS | Commercial off-the-shelf |
| CPX | Command Post Exercise |
| DARPA | Defense Advanced Research Projects Agency |
| DB | Database |
| DCAA | Defense Contract Audit Agency |
| DRM | Deception Reasoning Module |
| DCGS-A | Distributed Common Ground System - Army |
| FAR | Federal Acquisition Regulation |
| FBCB2 | Force XXI Battle Command, Brigade-and-Below |
| FedBizOpps | Federal Business Opportunities |
| GFD | Government furnished data |
| GFE | Government furnished equipment |

| | |
|---|---|
| GFP | Government furnished property |
| GUI | Graphical User Interface |
| HBCU | Historically Black Colleges and Universities |
| HTML | HyperText Markup Language |
| ISR | Intelligence, Surveillance, and Reconnaissance |
| IT | Information Technology |
| ITAR | International Traffic in Arms Regulations |
| IXO | Information Exploitation Office |
| JFCOM | Joint Forces Command |
| JSAF | Joint Semi-Automated Forces Simulator |
| JTR | Joint Travel Regulations |
| J-UCAS | Joint Unmanned Combat Air System |
| LOE | Level of effort |
| MAC | Months After Contract |
| MANPADS | Man Portable Air-Defense Systems |
| MG | Machine Guns |
| MI | Minority Institutions |
| MOU | Memorandum of Understanding |
| OneSAF | One Semi-Automated Forces |
| OPFOR | Enemy, Red Forces |
| OTB | OneSAF Testbed Baseline |
| PDA | Personal Digital Assistant |
| PIP | Proposer Information Package |
| RAID | Real-time Adversarial Intelligence and Decision-making |
| ROE | Rules of Engagement |
| RPG | Rocket Propelled Grenade |
| RSTA | Reconnaissance, Surveillance and Target Acquisition |
| S2 | Staff element responsible for Intelligence Products |
| SETA | Scientific and Engineering Technical Assistance |
| SOW | Statement of Work |
| TFIMS | Technical-Financial Information Management System |
| TIN | Taxpayer Identification Number |

| | |
|---|---|
| UAV | Unmanned Air Vehicle |
| UCAR | Unmanned Combat Armed Rotorcraft |
| UCAV | Unmanned Combat Air Vehicle |
| UGV/S | Unmanned Ground Vehicle/Sensor |
| UI | User Interface |
| V&V | Verification and Validation |

# J REFERENCES


1) Interview with General G. S. Martin, Military Aerospace, v.2, issue 6, 2003 pp.17-20; also see AirForce Handbook, http://www.af.mil/library/posture/2002handbook.pdf

2) US Army TRADOC, Force Operating Capabilities, Pamphlet 525-66, TRADOC, Fort Monroe, VA, June 2003, http://tradoc.monroe.army.mil/tpubs/pdf/pams/p525-66.pdf

3) US Army, Field manual 34-130, Intelligence Preparation of the Battlefield, http://www.army.mil/usapa/doctrine/DR_pubs/dr_a/pdf/fm34_130.pdf

4) US Army, Field Manual 101-5, Staff Organization and Operations, http://www.army.mil/usapa/doctrine/DR_pubs/dr_a/pdf/fm101_5.pdf

5) Robert Rasch, Alexander Kott, Kenneth D. Forbus, Incorporating AI into Military Decision Making: An Experiment, IEEE Intelligent Systems, v.18, n.4, August 2003, http://csdl.computer.org/comp/mags/ex/2003/04/x4toc.htm

6) US Army, Field Manual 3-06.11, Combined Arms Operations in Urban Terrain, http://www.army.mil/usapa/doctrine/DR_pubs/dr_a/pdf/fm3_06x11.pdf

7) J. H. Wilbanks, “The Battle for Hue, 1968,” http://www.globalsecurity.org/military/library/report/2002/MOUTWilbanks.htm

8) O. Oliker, “Russia's Chechen Wars 1994 - 2000: Lessons from Urban Combat,” http://www.rand.org/publications/MR/MR1289/

9) P. K. Van Riper, “A Concept for Future Military Operations on Urbanized Terrain”, https://www.mccdc.usmc.mil/futures/concepts/mout.pdf

10) M. Bowden, “Black Hawk Down,” Penguin, 2000

11) “Force XXI Battle Command, Brigade-and-Below (FBCB2)”, http://www.globalsecurity.org/military/systems/ground/fbcb2.htm