

Modeling Adversarial Intent for Interactive Simulation and Gaming: The Fused Intent System

Eugene Santos Jr.^a, Bruce McQueary^b, Lee Krause^b

^aThayer School of Engineering, Dartmouth College, Hanover, NH 03755

Eugene.Santos.Jr@dartmouth.edu

^bSecurboratorion, Inc., 695 Sanderling Drive, Indialantic, FL 32903

{bmcqueary,lkrause}@securboratorion.com

ABSTRACT

Understanding the intent of today's enemy necessitates changes in intelligence collection, processing, and dissemination. Unlike cold war antagonists, today's enemies operate in small, agile, and distributed cells whose tactics do not map well to established doctrine. This has necessitated a proliferation of advanced sensor and intelligence gathering techniques at level 0 and level 1 of the Joint Directors of Laboratories fusion model. The challenge is in leveraging modeling and simulation to transform the vast amounts of level 0 and level 1 data into actionable intelligence at levels 2 and 3 that include adversarial intent. Currently, warfighters are flooded with information (facts/observables) regarding what the enemy is presently doing, but provided inadequate explanations of adversarial intent and they cannot simulate *'what-if'* scenarios to increase their predictive situational awareness. The Fused Intent System (FIS) aims to address these deficiencies by providing an environment that answers *'what' the adversary is doing, 'why' they are doing it, and 'how' they will react to coalition* actions. In this paper, we describe our approach to FIS which includes adversarial 'soft-factors' such as goals, rationale, and beliefs within a computational model that infers adversarial intent and allows the insertion of assumptions to be used in conjunction with current battlefield state to perform what-if analysis. Our approach combines ontological modeling for classification and Bayesian-based abductive reasoning for explanation and has broad applicability to the operational, training, and commercial gaming domains.

Keywords: Abductive Reasoning, Adversarial Intent, Bayesian Knowledge-Bases, Bayesian Fragments, Soft Factors, Ontology

1. INTRODUCTION

To achieve the Joint Vision 2020 objective for full spectrum dominance [1] requires technological advancements in a variety of areas, including next generation sensor systems, data integration, networking, dissemination, simulation, and fusion across all levels of the Joint Directors of Laboratories (JDL) fusion model [2]. Simulating and understanding adversarial intent [3] is a key element necessary for this dominance. With previous adversaries, the process of locating, collecting and decoding intelligence was the challenge, but once acquired, the adversaries behavior could be simulated based on established doctrine and assessed largely against attrition. Our current asymmetric and highly dynamic adversaries have necessitated new changes in intelligence collection and dissemination. This has led to a proliferation of advanced sensor and intelligence gathering techniques which when coupled with unprecedented access to information via Network Centric Warfare (NCW), and the advent of open source intelligence (OSINT) has resulted in new challenges. The problem is not as much collecting intelligence but translating it into actionable intelligence, which is difficult because current adversary tactics and doctrine change rapidly. We are collecting unprecedented amounts of Joint Directors of Laboratories level 0 and level 1 intelligence but technological limitations have inhibited transforming it into actionable levels 2 and 3 intelligence that includes meaning, such as adversarial intent [4][5]. As Figure 1 highlights, the goal of the Fused Intent System (FIS) is to leverage computational modeling in conjunction with simulation to support this transformation. A key element that enables FIS to do this is that FIS considers soft factors (or human factors), such as religious, social, political, psychological and economic factors, which influence people's decision making and behavior.

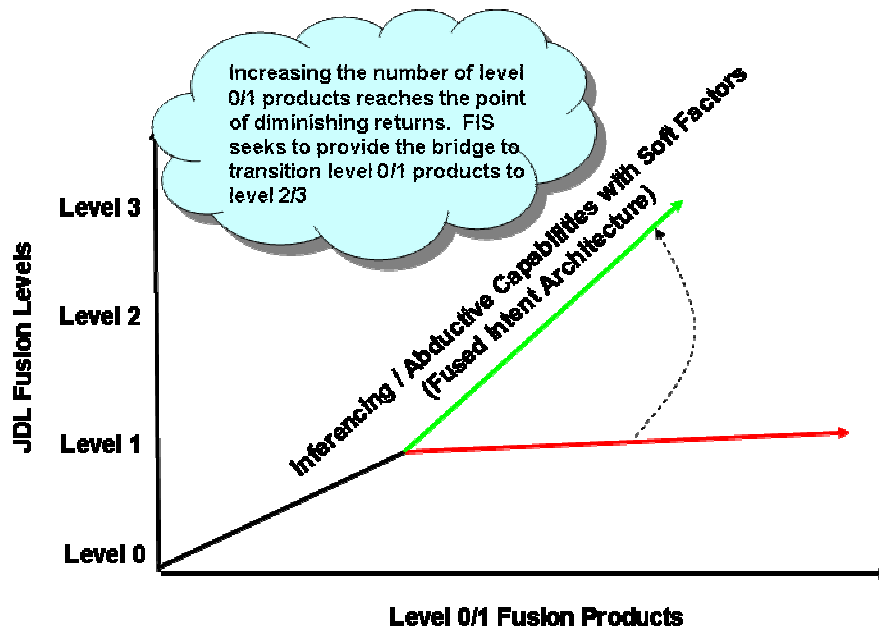


Figure 1. Transforming Level 0/1 to Level 2/3

This paper discusses how FIS fuses soft factors with level 0/1 evidence to forecast and explain adversary behavior; and how ‘what-if’ scenarios can be inserted into the analysis. The result enables situational awareness to evolve from a tactical, reactive mode, to a strategic and preemptive mode. Benefits that FIS seeks to bring to the intelligence community include:

- Maximizing the contribution of extensive sensor coverage provided by U.S. and coalition forces including aircraft, high-endurance unmanned vehicles, expeditionary sensor grids on land; and assets on, over, and under the surface of the ocean.
- Maximizing the speed, accuracy, and comprehension of expert analysts by automatically and continuously evaluating and inferring the meaning of events in relation to other potentially important events throughout the current and future battlespaces, which include regional challenges as well as transnational threats.
- Enabling an understanding of relationships among battlespace events; political, social, economical, industrial, and infrastructure effects; and, the goals, rational, and belief system of the adversary; and understanding how these relationships impact adversarial intent.

Operationally, FIS will contribute to the Joint 2020 vision by bringing automation to:

- Transforming level 0/1 isolated pieces of information to level 2 contextual information that includes adversary activity, behavior, and organizations.
- Predictive battlespace awareness by applying the adversary’s belief system to the contextual level 2 information to predict the adversary’s course of action and understand why the adversary is acting in the predicted manner (i.e. level 3).
- Linking level 2/3 fusion products to the overall goals and objectives of the coalition forces and products from the Intelligence Preparation of the Battlespace process (e.g. priority intelligence requirements, task orders, reports, etc.).

We begin in Section 2 describing prior and related work. Section 3 details our approach and system architecture for FIS. This is followed by Section 4 which presents our prototype FIS system and demonstration. Finally, we conclude our discussion with thoughts on future work.

2. RELATED WORK

The benefit of including socio-cultural soft factors in the intelligence fusion process is a natural evolution as adversaries have changed from large state-sponsored doctrinally based armies to loosely coupled ideologically driven groups that have proven to be capable of declaring war on large nations [6]. These socio-cultural factors are intrinsic to understanding the goals, motivations, and perceptions of the adversary and their environment – e.g., being able to grasp the basis behind local societal support mechanisms (say, the successful conversion/recruitment of child soldiers) – which ultimately leads to comprehension of adversary intent. However, most modern systems/tools that have been deployed codify human behavior without accounting for (evolving) adversary intent.

The System Effectiveness Analysis Simulation (SEAS) tool is representative of such systems [7]. SEAS is designed to model multi-missions and perform campaign level analysis. Agents can represent entities (e.g. military units) at any level within the hierarchies of military structure on the battle field. The interactions between agents and the environment, as well as the interactions among agents themselves are conducted through devices, including weapons, sensors and communication device. Interactions among agents are resolved in time increments, at one minute spreads. Decision making of an agent is based on pre-programmed logic that has been encoded in a component called “user programmed behaviors”; and agent behavior can be changed by modifying the code in a war file.

The Synthetic Environment for Analysis and Simulation (also abbreviated as SEAS) is another multi-agent based simulation system [8]. It has been used to simulate the Department of Defense’s wargaming paradigm in business and economics settings. In one simulation, situation-specific economies based upon mathematical rule-sets are created, which provide functioning goods, labor, asset, bond, and currency markets. The roles and groups have been modeled were the government regulators, firms, households and perpetrators. Households were endowed with demand functions, firms with production functions, perpetrators with political and economic objectives, and government regulators with laws. Typical attacks on an economic system include denial of service, disruption of service, and theft. It has been noted that perpetrators have varied capabilities, intentions and motivations to carry out threats.

As we can see, the agents in these two systems behave mainly based on the capabilities and doctrines that are encoded into them as rules. More recently, it has been realized that understanding the motivations that are influenced by value systems, personality, cultural factors, emotions, and social relationships behind certain behaviors is very important. Thus, a cognitive framework should be introduced into the modeling system to cover the soft factors from the human side of the equation. Socio-cultural gaming and simulation is a result of such an effort [10]. It focuses on modeling behaviors of leaders and followers and identifying the components needed for a role playing game. One assumption is that the majority of conflicts are centered around resource control. In the model, resources available to a group and its members include political goods (jobs, money, food, training, healthcare, etc.), rules within the group and security measures to impose on other groups, and popularity and support for the leadership as voted by its members. Each agent includes an intelligent component, called a performance moderator function server for simulating human behavior such as perception, stress and coping style, personality and culture, social relationships, and emotional reaction and affective reasoning about world. In the simulation, the environmental situations are categorized, and each category implies that certain strategies should be applied by an agent. Under each strategy category, there are sub-tasks and missions that can be carried out. For example, under “Grand Strategy Category” “Economic War on C”, there are missions like “Block Goods” and “Deny Infrastructure”. The cultural values and personality traits are represented through Goals, Standard and Preferences trees. Each tree nodes are weighted with Bayesian importance weights. Each agent acts in attempt to maximize its utility within the iteration of games.

With regards to intent, the Dynamic Adversarial Gaming Algorithm (DAGA) project [9] aims to provide a wargaming environment for automation of simulating the dynamics of geopolitical crisis, and eventually be applied to military simulation and training domain, and/or commercial gaming arena. The focus of DAGA is on modeling communities of interest (COIs), where various individuals, groups, and organizations as well as their interactions are captured. The framework provides a context for COIs to interact with each other and influence others’ behaviors. These behaviors must incorporate soft factors by modeling cultural knowledge. This is achieved by representing cultural variables and their influence on behavior using probabilistic networks. It is obvious that, when solving problems, each entity (either a specific individual or a group) acts based on its viewpoint and context. Furthermore, attitudes, values and perceptions of an entity are not based simply on the here and now, but also one’s previous histories, experiences, context, and, in essence, the cultural environment/group they originated from or are currently immersed. An entity’s perspective of environment and the meaning of other entity’s actions will be very different from those that are from a totally different

cultural background. In responding to this challenge, we take the approach of modeling each individual or group as an agent and incorporate cultural knowledge into the agent model in the form of cultural fragments, where cultural fragments are small probabilistic networks that can be instantiated and composed to define the specific culture necessary within the domain. As a result, each agent's behavior is under the influence of the cultural information currently encoded in its behavior model and, more importantly, how it ultimately affects intent [3].

In the FIS project, we take this one step further to incorporate soft factor impacts explicitly into our knowledge representation structure for abductive reasoning. It should provide a systematic way of representing causal relationships between the cultural, political, economic elements and the goals/interests of an intelligent entity, and enables a multi-agent based system to produce simulation environment that is more realistic.

3. FIS SYSTEM DESIGN

Transformation of level 0/1 observables into level 2/3 knowledge is a complex problem requiring innovative application of modeling, inference, and abductive reasoning techniques, supplemented by what-if simulation. The Fused Intent System consists of two primary service-based subsystems: the **Observable Inference Subsystem** and the **Abductive Reasoning Subsystem** that work in conjunction to ultimately infer level 3 knowledge. The Observable Inference Subsystem uses ontology-based inference to continuously infer level 2 adversarial behaviors and organizations from level 0/1 observables. The Abductive Reasoning Subsystem uses the inferred level 2 knowledge in conjunction with adversarial 'soft factors' such as social, cultural, economic, and political considerations, to develop a ranked ordering of predicted adversary courses of action that represent the adversary's intent, motivations, and goals; providing analysts and Commanders with level 3 awareness. Incorporation of 'soft factors' provides an additional dimension that enables the Fused Intent System to support tactical operations against asymmetric threats (such as militias and clans). Level 0/1 observables and intelligence provide an indication of the current state and resources of the asymmetric threat, and soft factors enable the threat's 'mindset' to be included along with observables in the inference process. This general concept of the Fused Intent System is depicted in Figure 2.

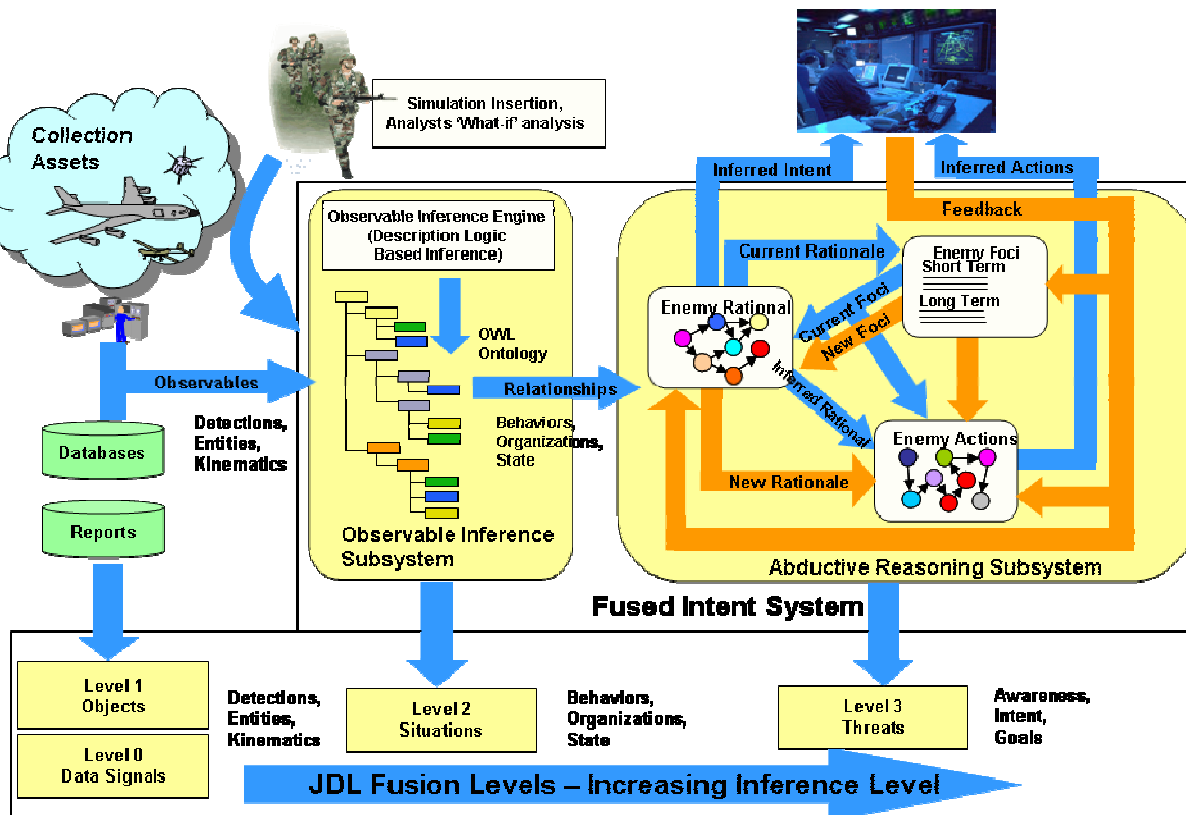


Figure 2. Fused Intent System Architecture

As shown in Figure 2, FIS supports a natural transformation spanning the JDL fusion levels, with the highest form of awareness being derived from the Abductive Reasoning Subsystem based on a general classification of events by the Observable Inference Subsystem. Inputs to the system can driven by level 0/1 detections and reports, and/or supplemented by analysts inputting additional data to understand how potential actions propagate and ultimately effect adversary actions. The primary components of FIS are discussed in the following paragraphs.

3.1 Observable Inference Engine

The Observable Inference Engine, or OIE, encodes domain knowledge regarding the adversary and the battlespace necessary to perform generalization of level 0/1 detections, entities, and kinematics into level 2 behaviors, organization, and states. The OIE is encoded as an ontology developed using the World Wide Web Consortium (W3C) OWL Web Ontology Language. Ontological modeling represents a major advancement in the science of modeling, particularly in encoding semantics or knowledge by mapping complex relationships that exist in the domain of interest. An ontology consists of an explicit description of concepts or classes in a domain of discourse; properties describe various features, attributes of the classes, and relationships to other classes; and, constraints on those relationships. OWL is a formalized specification language for ontology development and is critical because it:

- formalizes a domain by defining classes and properties of those classes,
- defines individuals and assert properties about them, and,
- supports inferential reasoning about these classes and individuals based on formal semantics of the OWL language.

Within FIS, as evidence is fed into the OIE, rules are applied and the ontology generalizes (through inference) *what* is happening in the battlespace. For example, in the context of Iran and the Strait of Hormuz, SIGINT may indicate anti-ship missile batteries activating; IMINT may depict speedboats operating in formation, as this information is input to the Observable Inference Subsystem, it will infer the behavioral conclusion, for example that ‘Iran is increasing naval activity in Strait of Hormuz’. This ability is key since at the higher levels of reasoning and in trying to understand the adversary’s goals and intent, it is not necessarily important which exact detections, entities, or kinematics cause a general level of behavior, organization, or state. This first-stage classification is necessary because it is impossible to model each type of detection, weapon system, etc. Rather we seek to use ontological concepts to define general characteristics and use the ontology for reasoning to support classification, and produce a result that indicates a generalized group behavior. This result is fed to the Abductive Reasoning Subsystem to determine higher level goals and intent.

3.2 Abductive Reasoning Subsystem

While the Observable Inference Engine determines *what* is happening in the battlespace, the Adversarial Inference Engine determines what this means, i.e. *why* is the adversary acting in particular manner. Ontologies support formal, complete descriptions of the problem domain, and can perform ‘binary’ classification by inference. However, they do not address uncertainty and statistical probability. For example, the ontology can infer Iran is ‘Increasing Naval Presence’ in the Strait of Hormuz, but not give that probability that they will take the next action of ‘*Visit, Board, Search, and Seize*’ vessels. Due to this inherent uncertainty involved in behavior modeling, we use Bayesian Knowledge Bases (BKBs) [11][12][13] as the knowledge representation within the Abductive Reasoning Subsystem.

BKBs are comprised of compact, modular, and composable Bayesian Knowledge Fragments (BKF). The BKF provide a highly flexible and intuitive representation following a basic “if-then” structure in conjunction with probability theory that minimizes the combinatorial explosiveness inherent with pure Bayesian Networks, or BNs. BKF were designed with domain incompleteness in mind, to retain semantic consistency as well as soundness of inference in the absence of complete knowledge. Bayesian Networks, on the other hand, typically assume a complete probability distribution is available from the start. Also, BKF have been shown to capture knowledge at a finer level of detail as well as knowledge that would be cyclical (hence disallowed) in BNs. Additionally, BNs often require probabilistic information that is unavailable and the combinatorial nature of the conditional probability tables is a significant limiting factor.

The Abductive Reasoning Subsystem provides Bayesian-based reasoning that enables FIS to accurately explain observations from the Observable Inference Engine and predict ‘next’ actions. This is accomplished by using BKF which support belief updating and belief revision. Belief updating concerns the computation of probabilities over random variables, while belief revision concerns finding the maximally probable global assignment to the random

variables. Abductive Reasoning Subsystem uses belief revision to come up with the set of hypothesis that together constitutes the most satisfactory explanation/interpretation of the evidence at hand.

As shown in Figure 2, the Abductive Reasoning Subsystem is based on a three-component architecture for intent [14]: Rationale Network (*why*), Action Network (*how*), and Goals (*what*). The rationale network is a BKF consisting of cultural axioms (beliefs about themselves such as “divine mandate”), beliefs (beliefs of the region with respect to U.S.), goals (what they want to achieve), and, actions (e.g. deploy decoy IEDs).

These are described as follows:

1. **Goals/Foci:** Probabilistically prioritized short- and long-term goals list, representing Leadership intents, objectives or foci. The goal component captures what the entity is doing
2. **Rationale:** A probabilistic network, representing the influences of the entities beliefs, both about themselves and about us, on their goals and on certain high level actions associated with those goals. The rationale component infers why entity is doing it.
3. **Actions:** A probabilistic network, representing the detailed relationships between entity goals and possible actions to realize those goals. The action component captures how the adversary might do it.

To account for uncertainty, BKF, are used as the primary knowledge representation for the rationale and action networks. Each random variable (RV) involved in the BKF is classified into one of four classes: **axioms, beliefs, goals, and actions**.

- a) Entity Axioms(X) – represent the underlying beliefs of the entity about themselves (vs. beliefs about other forces). Axioms typically serve as inputs or explanations to the other RVs such as a leader’s goals (e.g. Sovereign Right to the Strait of Hormuz)
- b) Entity Beliefs (B) – represent the entities beliefs regarding other forces (e.g. beliefs that the U.S. will avoid confrontation in Strait at all cost).
- c) Entity Goals (G) – represent the goals or desired end-states of the entity (e.g. Implement Economic Reforms).
- d) Entity Actions (A) – represent the actions of the entity to achieve their goals (e.g. Visit, Board, Search, and Seize).

Figure 3 shows how these are arranged within a BKB.

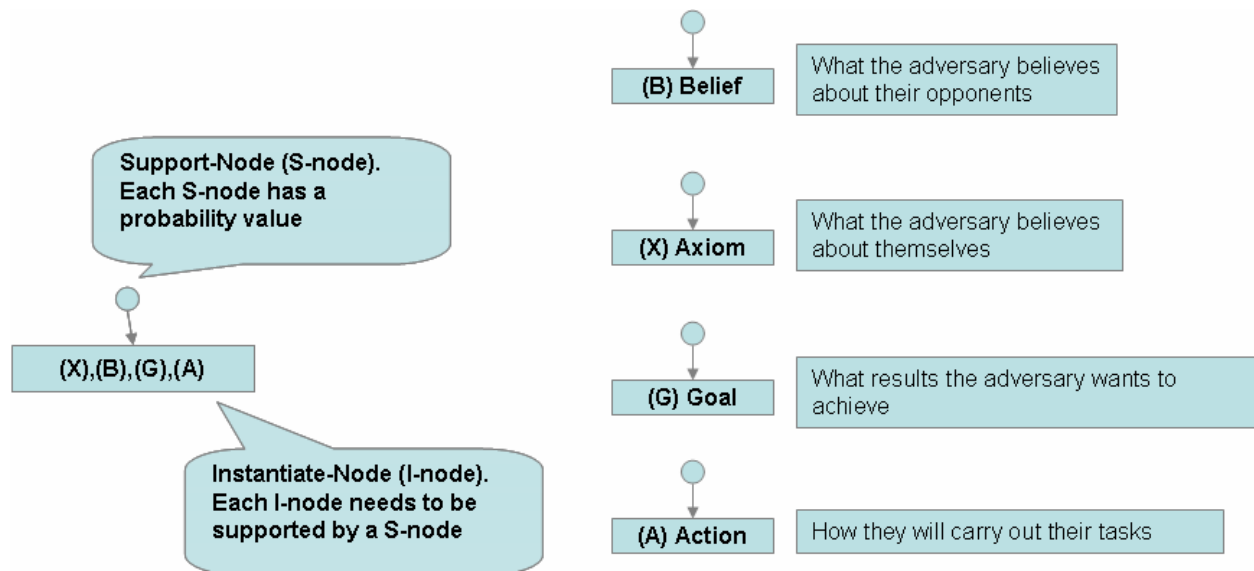


Figure 3. BKB Structure with Beliefs, Axioms, Goals, and Actions

Within the Abductive Reasoning Subsystem, these four random variable types are arranged into the two networks: rationale network and action network. The rationale network contains all of the Belief (B), Axiom (X), and Goal (G) variables, as well as any Action (A) variables which have goals as inputs. This network is used to infer what short- and long-term goals the entity may have. Once the goals are determined, the action network is used to reason out what the most likely actions will be that entity may carry out. The action net contains the entire set of Action (A) variables and any concrete Goal (G) variables. The Adversarial Reasoning Subsystem works iteratively adapting to changes in the goals and intentions over time as reflected in the entity foci lists. Note that in Figure 2 there are feedback and explanation paths within the Adversarial Reasoning Subsystem. This allows for direct updating of the internal network components.

3.3 Simulation Insertion Points / ‘What if’ Analysis

The modeling aspect of FIS enables analysts to enter assumptions and step through ‘what-if’ scenarios. The entry point for evidence is via the Observable Inference Subsystem. From the FIS computational perspective, it does not matter whether the evidence comes from actual intelligence reports, or is entered by intelligence analyst. The inference and abductive threads through the system are the same. This enables analysts to selectively insert U.S. actions and evaluate all aspects of their effects on adversary goals, axioms, beliefs, and actions. For example, an analyst may evaluate the *action* of taking out anti ship missile batteries, and see how that effects Iran’s internal *belief* the U.S. will not act militarily, their *axiom* that they can ‘bait’ the U.S. military in action, their *goals* of unifying Iranians against U.S. and distracting local populace from their economic dissatisfaction; and the changes to Iran’s next likely courses of action. This highlights the flexibility of the FIS architecture where it can be driven entirely by a simulation, or driven by real world intelligence feeds such as DCGS, or used in a mixed mode. To date, as discussed in the next section, our development has focused on the computational modeling as opposed to the ingestion technicalities of level 0/1 data.

4. PROTOTYPE AND DEMONSTRATION

The prototype FIS system has been demonstrated for a scenario entitled “*Showdown with Iran*” and is representative of current tensions regarding the Strait of Hormuz. This scenario describes Iranian goals, actions, beliefs, and axioms that may be used to construct complex combinations of situations that lead to escalating tensions and military conflicts with Iran. The result is a non-scripted scenario that provides numerous ‘starting’ points, outcomes, and progressions driven by the ‘evidence’ presented to it. This provides a great deal of flexibility in terms of ‘what if’ scenarios, and renders a single thread of scenario trivial, while focusing on a central theme: potential confrontation with Iran in this case. Observables are used to indicate increasing posturing, and confrontation which may begin with overt acts such as Iran firing missiles across the Persian Gulf at Saudi Arabian oil facilities, or subtle acts such as sponsoring piracy off the coast of Somalia to divert attention of the Fifth Fleet stationed in Bahrain, etc.

Initially, FIS maintains a nominal or initial ‘state of the world’. As events unfold FIS is populated with changing evidence and the next state of the adversary’s goals, actions, axioms, and beliefs are calculated, presented to the analyst, and feed back into the system to be used in subsequent calculations. The abductive reasoning subsystem within FIS provides explanations to analysts regarding the evidence in terms of the adversary’s goals, beliefs, axioms, and actions. For example, evidence that Iran is increasing purchases of Sunburn missiles, while ramping up rhetoric about their rights to the Strait of Hormuz (SOH), may be explained in terms of a ranked ordering of likely actions (in terms of increasing probabilities) such as “Iran preparing to close the Strait of Hormuz” being the most likely explanation for the evidence. This action can be explained in terms of the adversary’s goals, beliefs, and axioms as well. For example FIS can infer Iran’s goals in closing the Strait of Hormuz – e.g. to charge tariffs to help build up economy; to use as a bargaining chip in nuclear negotiations, etc. FIS also factors in how Iran’s axioms or beliefs about themselves help to explain observations – e.g. is Iran’s increasing belief regarding their right to nuclear technology influencing their increased belligerence? Iran’s belief about the U.S is also used to explain observations – e.g. their belief that the U.S. will not react militarily while engaged in Iraq contributes to the explanation that Iran is willing to take military action to close the Strait. Further evidence (e.g. increased rhetoric and threats, Naval exercises, swarming/harassment of tankers, etc) may further bolster (or diminish) that explanation. The interdependency among these complex factors are captured and modeled within FIS.

We began by developing a high-level set of actions, goals, beliefs, axioms that in general apply to the asymmetric adversary the U.S. faces and then incorporate elements specific to the current Iran situation. Tables 1 through 4 depict a sampling of the Goals, Actions, Axioms, and Beliefs, which were developed in significantly more detail in the scenario.

These form the basis for the modeling, both in the Observable Inference Engine and the Abductive Reasoning Subsystem. For example Iran's goal to "Restore Country to Super Power" can be deconstructed into lower-level indicators that are modeled within the OIE, enabling it to conclude that based on current 'lower level' indicators, that Iran's goals are to "Restore Country to Super Power" (among others). This relationship to possible actions and other goals, axioms, actions, and beliefs are captured within the Abductive Reasoning Subsystem using Bayesian Knowledge Base/Fragment structure.

Table 1. Iranian Goals

Restore country to superpower.
Export radical Islam ideology.
Disrupt oil exports to U.S.
Cause transfer of wealth from western to Islamic nations.
Hasten the coming of 12 th Imam.
Safeguard regime.
Acquire nuclear weapon technology.

Table 2 Iranian Actions

Purchases of centrifuges (WMD manufacturing equipment).
Withdraw from NPT (Non Proliferation Treaty).
Transfer of money from Western banks.
Swarming of Tankers in SOH (Strait of Hormuz).
Missile attack on Tankers in SOH.
Missile attack on Saudi oil fields
Deployment of EM-53 bottom tethered mines in SOH.

Table 3. Axioms (Beliefs about themselves)

Have a divine mandate.
Relenting is a sign of weakness.
Sovereign right to 'own' SOH.
General Iranian population supports hardline position.
General Iranian population supports Theocracy.
General Iranian population believes voting is futile.
Muslim states will affirm Iran rights to nuclear technology

Table 4. Beliefs (What Iran Thinks about US)

US will accede to nuclear demands.
US does not have the will for another confrontation.
US driven by regime change.
US wants to destroy Islam.
US has double standards regarding nuclear technology.
US will land ground forces east of Bandar Abbas.
US economy can be disrupted by closing SOH.

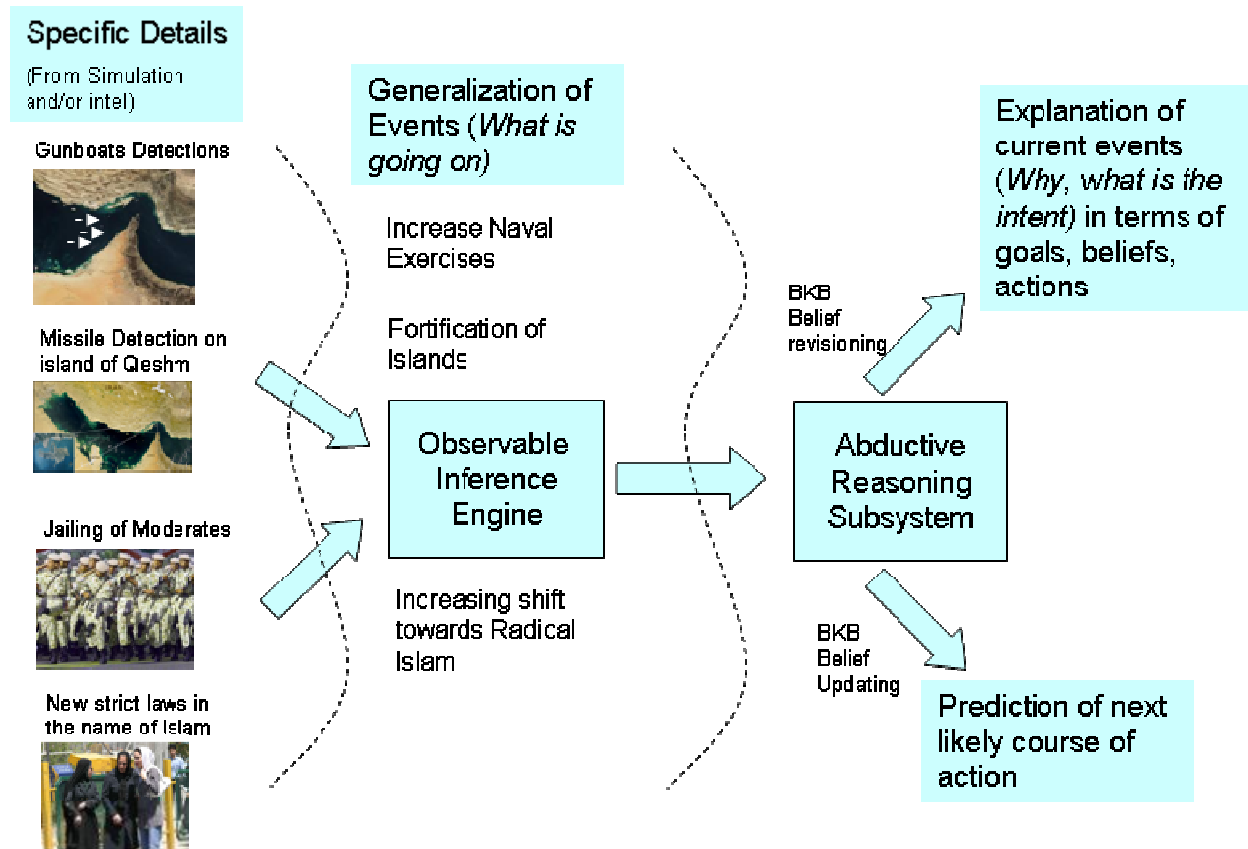


Figure 4. Fused Intent System Information Flow – from indicators into the OIE where they are generalized into behaviors representing what is happening, to the Abductive Reasoning Subsystem where how that behavior relates to intent is evaluated.

The flow depicted in Figure 4 was codified within the FIS Demonstration Prototype execution environment, which is shown in Figure 5.

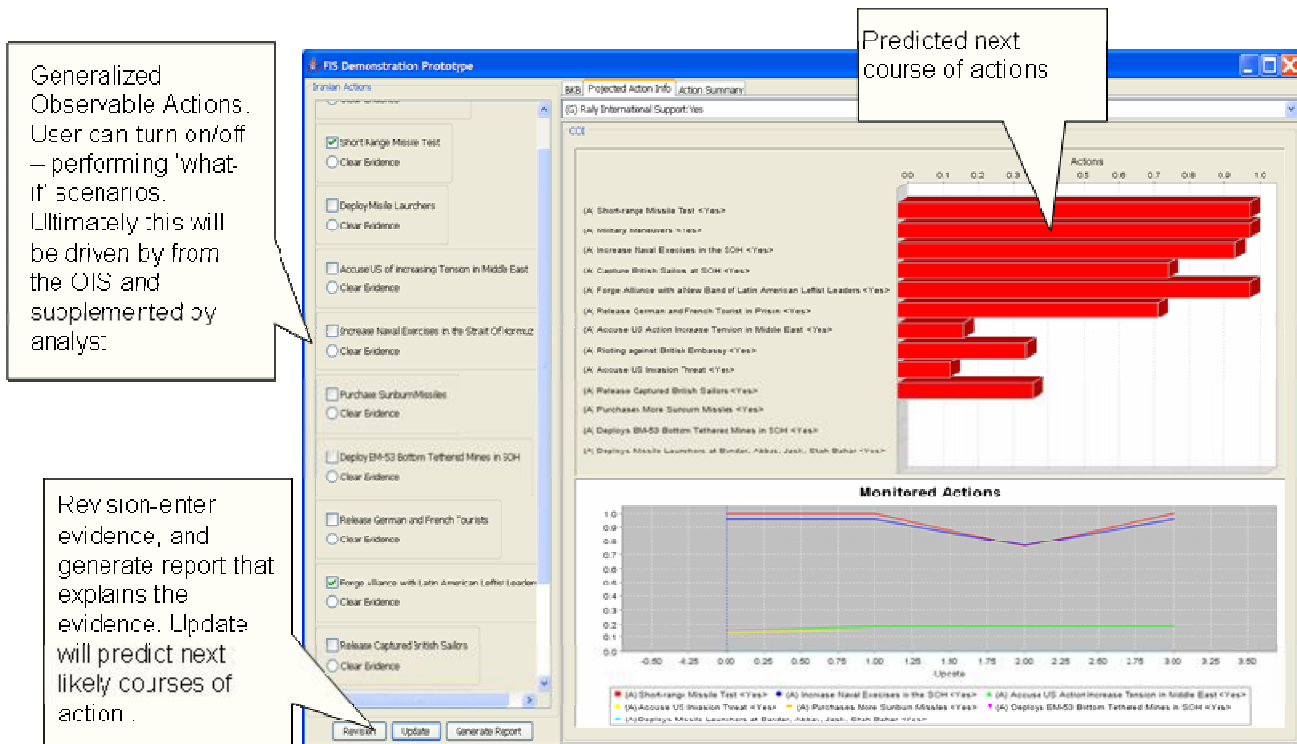


Figure 5. FIS Prototype Demonstration Environment

On the left side of the FIS environment, potential actions are listed. These represent outcomes from the Observable Inference Engine. For the purposes of demonstration, and to focus on analyst interaction and simulation, analysts can directly select which actions take place. These can be based on intelligence reports, or used interactively to simulate what next course of actions will likely take place, given the current state. When the analysts selects the action(s) and performs an update, the ranked listing on likely courses of actions are represented in the bar chart. The trends of the changing actions, goals, axioms, and beliefs, are captured in the X-Y graph. It should be noted that the Abductive Reasoning Subsystem acts in a cumulative manner. Goals, beliefs, and axioms feed back into each other and affect their next state.

Then to further support analysts, the FIS prototype also includes auto-generation of detailed HTML reports that explain the results FIS comes up with in terms of the evidence presented to it. The complete FIS cycle is shown in Figure 6:

1. This screenshot depicts the BKB residing within the Abductive Reasoning Subsystem and as evidence is set by the analysts via the checkboxes on the left of the screen, and the state updated, the relevant nodes will change color to indicate they contribute to the overall computation. This is a visualization of the traceability that FIS provides. Each result FIS derives can be traced back through the modeling components.
2. The explanation of the evidence – *why* FIS believes the adversary is acting in the manner they are.
3. Nodes contributing to the explanation are highlighted.
4. A detailed report of the forecasted courses of action is generated as a web page and available for the analyst to review. This contains the details regarding *why* FIS derived the values it did. This is critical to achieving but in from analysts. The first question they get when presenting their conclusions to their Commanders is “*why* do you think that?”. FIS provides a means to get away from the ‘gut’ feelings of the analysts and allows them to point to well defined rationale behind the adversary’s behavior that is formalized within the FIS modeling structure.
5. This allows analysts to adjust / weight their evidence, and evaluate the effects.

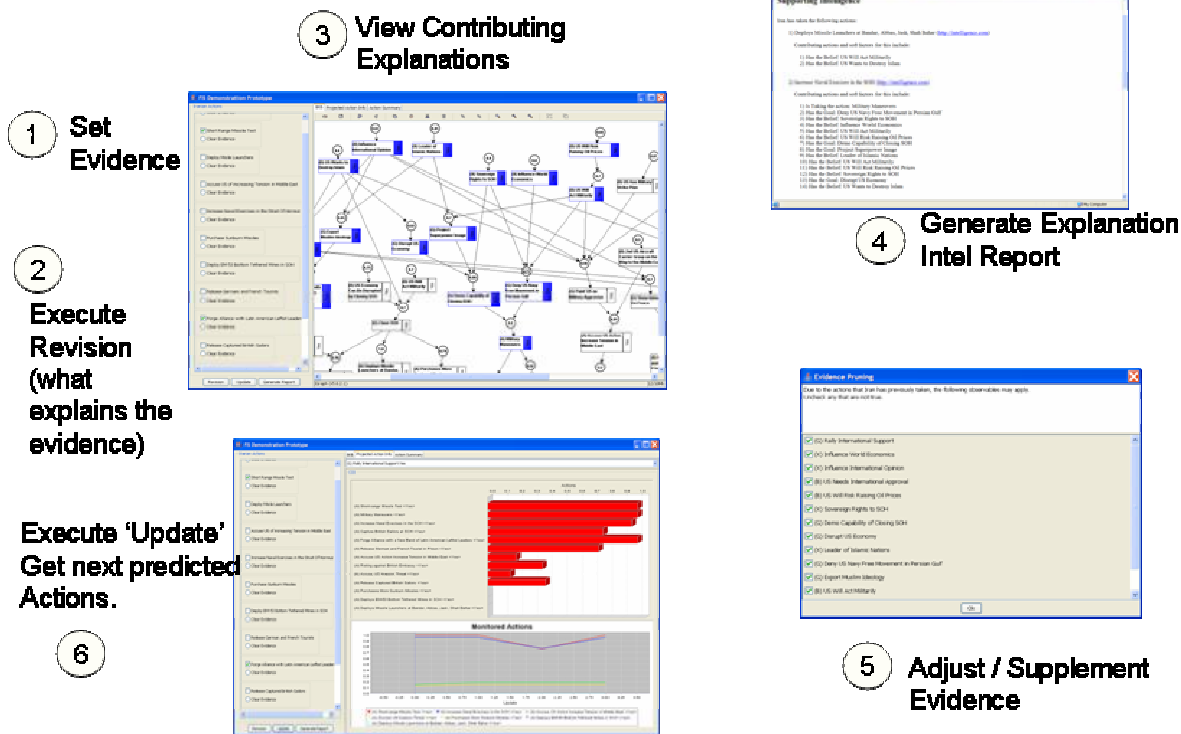


Figure 6. FIS Environment Cycle

5. WHAT'S NEXT

While this research has yielded results analysts can use to simulate and understand adversarial behavior, there is still significant research to be performed, particularly in the area of sensitivity. We are incorporating the ability to determine which elements contribute the most to a particular conclusion. This will allow us to help analysts pinpoint potential tipping points and/or critical centers of gravity in influencing or affecting adversarial behavior and especially intent. Ultimately, with sensitivity/contribution analyses, we can aim for automated what-if mechanisms that assist analysts and planners in how to alter the intent of not just the adversary but an entire adversary network while also providing an understandable explanation of such affectors because of the underlying abductive reasoning employed by our approach.

6. ACKNOWLEDGMENTS

This work was supported in part by ONR Grant No. N00014-06-C-0020 and AFOSR Grant Nos. FA9550-06-1-0169 and FA9550-06-C-0035.

REFERENCES

- [1] "Joint Vision 2020," <http://www.dtic.mil/jointvision/jvpub2.htm>, US Government Printing Office, Washington DC, (2000).
- [2] U.S. Department of Defense, Data Fusion Subpanel of the Joint Directors of Laboratories, Technical Panel for C3, "Data fusion lexicon," 1991.
- [3] Santos, E., Jr. and Zhao, Q., "Adversarial Models for Opponent Intent Inferencing," in *Adversarial Reasoning: Computational Approaches to Reading the Opponents Mind* (Eds. A. Kott and W. McEneaney), 1-22, CRC Press (2006).

- [4] Lehman, L. A., Krause, L. S., Gilmour, D. A., Santos, E., Jr., and Zhao, Q., "Intent Driven Adversarial Modeling," *Proceedings of the Tenth International Command and Control Research and Technology Symposium: The Future of C2*, McLean, VA (2005).
- [5] Bell, B., Santos, E., Jr., and Brown, S. M., "Making Adversary Decision Modeling Tractable with Intent Inference and Information Fusion," *Proceedings of the 11th Conference on Computer Generated Forces and Behavioral Representation*, 535-542, Orlando, FL (2002).
- [6] Thomas, T. S. and Casebeer, W. D., "Violent Non-State Actors: Countering Dynamic Systems," *Strategic Insights*, Volume III, Issue 3, (2004).
- [7] <http://www.teamseas.com/>
- [8] Chaturvedi, A., Foong, C.M., Armstrong, B., and Snyder, D.R., "Bridging Kinetic and Non-Kinetic Interactions over Time and Space Continua," The Interservice/Industry Training, Simulation & Education Conference (IITSEC) (2005).
- [9] Santos, E., Jr., Zhao, Q., Pratto, F., Pearson, A. R., McQueary, B., Breeden, A., and Krause, L., "Modeling Multiple Communities of Interest for Interactive Simulation and Gaming: The Dynamic Adversarial Gaming Algorithm Project," *Proceedings of the SPIE: Defense & Security Symposium*, Vol. 6564, Orlando, FL (2007).
- [10] Silverman, B.G., Bharathy, G., Johns, M., Eidelson, R.J., Smith, T.E., and Nye, B., "Sociocultural Games for Training and Analysis," *IEEE Transactions on Systems, Man and Cybernetics, Part A* 37(6), 1113-1130 (2007).
- [11] Santos, E., Jr. and Santos, E. S., "A Framework for Building Knowledge-Bases Under Uncertainty," *Journal of Experimental and Theoretical Artificial Intelligence* 11, 265-286 (1999).
- [12] Santos, E., Jr., Santos, E. S., and Shimony, S. E., "Implicitly Preserving Semantics During Incremental Knowledge Base Acquisition Under Uncertainty," *International Journal of Approximate Reasoning* 33(1), 71-94 (2003).
- [13] Santos, E., Jr. and Dinh, H. T., "Automatic Knowledge Validation for Bayesian Knowledge Bases," *Data and Knowledge Engineering* 64, 218-241, 2008.
- [14] Santos, E., Jr., "A Cognitive Architecture for Adversary Intent Inferencing: Knowledge Structure and Computation," *Proceedings of the SPIE: 17th Annual International Symposium on Aerospace/Defense Sensing and Controls: AeroSense 2003*, Vol. 5091, 182-193, Orlando, FL (2003).