ABSTRACT: Military and domestic security analysts and planners are facing threats whose asymmetric nature will sharply increase the challenges of establishing an adversary's intent. This complex environment will severely limit the capabilities of the classic doctrinal approach to diagnose adversary activity. Instead, a more dynamic approach is required - adversary decision modeling (ADM) - that, while a critical capability, poses a range of daunting technological challenges. We are developing methodologies and tools that represent a tractable approach to ADM using intelligent software-based analysis of adversarial intent. In this paper we present work being performed by our team (University of Connecticut, Lockheed Martin Advanced Technology Laboratories, and the Air Force Research Laboratory Human Effectiveness Directorate) toward a preliminary composite theory of adversary intent and its descriptive models, to provide a coherent conceptual foundation for addressing adversary decision processes, tasks, and functions. We then introduce notional computational models that, given own system-of-systems actions (movements and activities) and observations of an adversary's actions and reactions, automatically generate hypotheses about the adversary's intent. We present a preliminary software architecture that implements the model with: (1) intelligent mobile agents to rapidly and autonomously collect information, (2) information fusion technologies to generate higher-level evidence, and (3) our Intent Inference engine that models interests, preferences, and context.

1. Need for Adversary Decision Modeling

The United States military faces a world in which it will overmatch in size and armament most threats it may encounter. In order to make up for these mismatches, the asymmetric threat will be creative in its approach to warfare. These threats may be distributed, performing small strategic attacks across specific points within a wide area. The short timeframes and uncertain intentions of adversaries representative of 21st century operations will force planners to forego a predetermined "menu" of targets and instead dynamically select targets from among a more general list based on current priorities and opportunities. This mode of planning is inimical to target-based approaches, and it strains the objectives-based approach (at least as that approach has been employed to date). Within this complex environment,
the use of static doctrinal reasoning in ascertaining adversary actions and reactions offers severely limited utility. Instead, a more dynamic approach to inferring and tracking adversary intent is needed.

The basis for such an approach is emerging from USAF-sponsored research. Dr. Maris “Buster” McCrab has recently submitted a draft CONOPS [1] for a novel approach to planning, executing, and assessing military operations. This approach — termed effects-based operations (EBO) — is the best candidate to serve as the basis of the operations model we require. EBO is a “…set of processes, supported by tools and done by people in organizational settings, that focuses on planning, executing and assessing military activities for the effects they produce rather than the targets or even objectives they deal with.” ([1], p. 3)

As such, EBO is framed with respect to outcomes produced (and/or predicted to be produced) in the battlespace.

One of the greatest technological challenges for the EBO approach is that of adversary decision modeling [2]. An example of a composite adversary decision model based on Llinas et al. ([3], [4]) is given in Whitaker and Brown [5] as shown in Figure 1.

![Figure 1. Composite adversarial decision model](image)

We have defined five broad research issues raised by adversary decision modeling:

1. What critical human factors (e.g., interests, technology, emotions, knowledge and/or expertise, culture, environmental context) must be modeled?
2. What knowledge representations are necessary and sufficient for effective and efficient adversarial intent inference (i.e., how do we model the human factors and at what level of abstraction)?
3. How do we perform the necessary initial and subsequent knowledge acquisition (to include obtaining observational cues of effects) for prescriptive adversarial decision models given the non-cooperative nature of the adversary?
4. How do we use the models to inform friendly decision makers and increase their predictive battlespace awareness?
5. How do we test and evaluate our models to determine how well they perform?

In the remainder of this paper, we articulate the challenges facing adversary decision modeling and introduce an approach to overcoming these challenges that employs intent inference, probabilistic reasoning, information fusion and intelligent agents.

2. Background

Deriving hypotheses about future actions of an adversary requires information about the adversary's current actions and inferences about the adversary's motivations. The informational requirements can be approached by bringing data collection and fusion capabilities to bear; the inferential requirements can be approached by creating models to generate descriptive probabilities (to what extent does motivation X account for the set of observations Y?) and predictive probabilities (how likely is future action Z given motivation X?). Before discussing the details of our approach, we provide a brief synopsis of these informational and inferential capabilities.

2.1. Informational Elements

Inference depends centrally on information, or evidence, and the more complete and accurate the information, the more reliable and predictive the inference. We employ a two-step process to generating a critical mass of useful information. In Step 1, intelligent agents are dispatched to autonomously migrate across own-force networks and collect information relevant to a specific need. An agent can then collect whatever information it encounters on the spot, or post itself as a "sentinel," persistently monitoring a data source until its criteria are met for migrating back with the collected information. The second step is to combine (or "fuse") the collected information, to merge information from different sources that describes the same event or entity, and to reconcile contradictory information.

2.1.1. Intelligent Agents

Agents are autonomous software processes that can migrate throughout a network, execute instructions, make decisions, collect data, and return to the original host. Intelligent agents can play a key role in adversary decision modeling by providing a stream of observed events to the intent inference mechanism. Lockheed Martin Advanced Technology Laboratories (LM-ATL) and the University of Connecticut (UConn) have employed agents for a variety of purposes, among
In automated intent inference, data representing based on observations of that individual's actions in inference involves deducing an individual's goals. Sophisticated information fusion capabilities are required in order to transform what the agents gather from a raw form to an integrated, consistent and complete form. Information fusion can occur at multiple levels of abstraction. A widely adopted lexicon advanced by the Joint Directors of Laboratories has characterized four levels of fusion as object refinement (Level 1), situation refinement (Level 2), threat refinement (Level 3), and process refinement (Level 4).

Work performed by LM-ATL under the Army's Rotorcraft Pilot's Associate program has resulted in a technology base for Level 1 and Level 2 fusion. This technology base provides a fusion architecture and near real-time fusion engine for handling multi-sensor, multi-track fusion ([11], [12]).

On-going efforts in our group are exploring the integration of fusion and agents for situation awareness applications ([13], [14]). Our approach to adversary decision modeling seeks to leverage this promising synergy.

### 2.2 Inferential Elements

Creating a fused picture that reflects the current tactical situation provides the critical inputs from which to reason about an adversary's intent. Our approach to this second phase relies on user-intent inference, to generate expectations about goals based on observations, and adversary intent inference, to propagate those expectations through a reasoning engine that considers not only observed actions and their corresponding goals but inferred motives as well.

#### 2.2.1. User Intent Inference

User Intent Inference (hereafter called simply "intent inference") involves deducing an individual’s goals based on observations of that individual’s actions [15]. In automated intent inference, data representing observations of an individual, the individual’s actions, or the individual’s environment (collectively called observables) are gathered by direct and indirect mechanisms. These data are then fused to merge the raw information into higher-level constructs. Finally, the fused information is interpreted against one or more behavioral models, constructed and optimized for the individual’s behavior patterns. The models match the observed and fused information against patterns of behavior and derive inferred intent from those patterns.

Intent Inference can be employed to provide three kinds of hypotheses [16]. Descriptive intent inference provides insight into the motivations behind actions that have just occurred. Predictive intent inference can anticipate future actions given the individual’s inferred goals. Diagnostic intent inference detects deviations between predicted and observed actions to reveal possible user errors.

User intent inference involves the use of observations of an individual’s use of an application or system to automatically infer the user’s goals with respect to the user’s tasks. These data can be direct observations of human-system interface interactions or indirect observations of the user’s environment, including operator biometrics, interactions between operators, and inputs from decision support tools. The results of the inference can be used to proactively aid the user, balance the user’s workload, filter incoming information, or monitor the user’s task progress.

UConn has continued to refine the work on the Core Interface Agent (CIA) Architecture [17]. CIA uses Bayesian networks to infer intent given sets of observables. CIA has been used to infer user intent in an expert system shell called PESKI ([18], [19], [20]) and in an intelligent information retrieval system called Kavanah ([21], [22]). In the former application—the probabilistic expert system development environment (PESKI)—a suite of intelligent knowledge engineering tools (agents) was developed to help the knowledge engineer construct intelligent systems that managed uncertainty. The ultimate goal for PESKI is to guarantee that all actions taken by the expert and machine in building a decision support system are done as efficiently as possible, always consistent, and always correct. Given that knowledge engineering is rife with many incremental choices and alternatives at each stage, making the right choices by the human/machine is paramount. Employing user intent, an intelligent user interface was developed for PESKI that attempted to help select the appropriate tools for the expert. This project led to the development of CIA that demonstrated that the ability of user intent inference to adapt to changing situations and contexts is a critical component even in very controlled/targeted domains such as building specialized decision support systems.

The main goal of Kavanah is to use the interface agent (also called active user interface) to assist the users in
getting the right information at the right time using the right tools. The principles behind the design of the system are efficient construction of a model of the user’s long and short-term interests and preferences, dynamic reasoning from the user’s information seeking context, and applying decision theoretic principles and probabilistic reasoning techniques wherever they are appropriate. We clearly separate the concepts of interests and preferences in a dynamic fashion. The term *interests* denotes the topics or subjects that the user is focusing on in the information-seeking task. The term *preferences* denotes how the user would go about acquiring and viewing the desired information. The interface agent in Kavanah proactively constructs the queries on the user’s behalf as it learns the user’s style in searching. It also updates the knowledge base to incorporate the new knowledge that it has learned from the user’s interactions with the system.

Recently, LM-ATL adapted the CIA Architecture for use in team intent inference. Team intent inference is used to deduce the goals of a group based upon observations of the individuals within that group. Although individual intent is used to infer team intent, this team intent can also be used to help infer the intent of other individuals within the group, forming a natural mutual reinforcement positive feedback loop. Team intent inference can also be valuable in diagnosing coordination lapses within a group, such as two members of the group working at cross-purposes or multiple members duplicating actions. In addition, team intent inference, when combined with rigorous individual descriptive intent inference, can be used to identify oversights in a team’s plans. This new architecture has been tested within a theater ballistic missile defense (TBMD) domain in a time-critical targeting demonstration application [23]. The demonstration prototype, named Observer, performs both descriptive and predictive intent inference for a team of operators within a TBMD cell. Observer monitors task progress in the identification of TEL (Transporter-Erector-Launcher) activity and aids cell analysts in the assignment of strike assets against TELs by tasking mobile intelligent agents with proactive information queries within context. The use of team intent inference provides fast coordination between operators in different parts of the cell.

2.2.2. Adversary Intent Inference

User Intent Inference can help answer *what* the individual is doing, *how* the individual might do it, and *why* the individual is doing it. If we substitute the thinking of an adversary for that of a user, we can consider models that might tell us what an adversary’s actions suggest he might do in the future. In other words, we can adapt the User Intent Inference approach to something we can label Adversary Intent Inference. We can thus leverage the natural isomorphism between our prior work in the field of user and team intent inference and the domain of adversary intent inference. While the operational world surrounding an intent inference application would be very different, the inner mechanisms of intent inference map directly between domains. Note that this does not claim to solve the complete unified adversary intent problem. Instead, we offer our approach as a conceptual foundation on which to build a larger unified theoretical solution in the future.

While adversary intent could be construed as having as its overall goal the ability model the enemy in its entirety (stated as “enemy-as-a-system” in the EBO CONOPs), we believe that a necessary starting point is to model an *adversary commander’s intent*. This is a much more manageable and feasible task based on currently available technology and research developments especially in intent inference. Once enemy commander intent is suitably modeled and captured, we can then compose these individual intent models into larger collectives using our work in team intent modeling to address the general problem of adversary intent inference (“enemy-as-a-system”).

The next section highlights some of the challenges that adversary intent inference poses and describes our approach to overcoming those challenges.

3. User Intent to Adversarial Intent

User Intent Inference is the basis for Adversary Intent Inference, so we can use the components of the former as analogs to help structure the latter. Recall from our discussion of User Intent Inference that the process relies on: (1) mechanisms for capturing observations of the user's environment, and interactions between the user and the automation systems; (2) a process for interpreting raw information and generating higher-level (fused) constructs; and (3) one or more behavioral models of the user.

Analogizing to Adversary Intent Inference, we require mechanisms to capture events in the environment, algorithms to fuse raw event reports into a common picture, and one or more behavioral models of the adversary. Although User Intent Inference is itself a difficult enterprise, we have in the adversarial instance greater complexities, reduced access to information, and the likelihood of stealth and deception.

In discussing these challenges, it is important to point out that the intelligence community already performs a kind of adversary intent inference, relying heavily on the skills and intuitions of experienced analysts. In fact the steps defined in the intent inference process have corollaries to the intelligence cycle: capturing observables is referred to in the intelligence community
as "collection", fusing the information is closely aligned with "processing", and matching those data against behavioral models is the process of "analysis and production."

3.1. Collection Challenges

Consider first the "observables" that must be captured and interpreted. While observables in the user intent domain stem from data collected from human use of systems, observables in the adversary intent domain take the form of tactical information derived from intelligence databases, observations of the tactical environment, and input from online human experts. In place of window events, keystrokes, and mouse movements, our system in the adversary intent domain will use information about adversary location, movements, and activities to drive its inference.

An inherent problem associated with directly observing an adversary's actions is that an adversary probably does not want his actions observed; a corollary is that actions that cannot be hidden from observation may be masked by conducting similar or co-occurring decoy operations. In addition to the adversary's wishes to confound direct observation, it is often the case that the actions themselves are taking place in areas beyond the reach of direct observation, or in environments where direct observation is difficult. These challenges (addressed by the intelligence community's collection organizations) add a layer of complexity to the adversary intent inference.

3.2. Processing Challenges

Next consider the process of combining raw data into higher-level information. Merging user intent data might consider the state of the application, analyses of information queries, and the content of user dialogue with team members. In the adversarial domain, our system must integrate facts about the local terrain, regional weather, and the salient political climate.

Intelligence analysts who perform this task will examine raw information from multiple sources and ask questions like "are these multiple indicators reacting to the same event or multiple events?", "what does indicator A mean in the context of indicator B?", and "what intermediate conclusion can be drawn from the co-occurrence of these multiple data?" Analysts rely on access to information collected by other intelligence assets and on their own knowledge, expertise, and intuitions to properly process the raw information.

Because information fusion has evolved as an intelligence capability, adversary intent inference does not introduce entirely new challenges. The range of information to be combined, however, is likely to be quite broad, across multiple domains, sources, and levels of abstraction. Merging information from battlefield sources, national assets, and news feeds publicly distributed on the web, for instance, is likely to present some combinatorial problems.

3.3. Analysis and Production Challenges

Developing predictive models of adversary behavior requires detailed histories, comprehensive digests of the intelligence picture, and highly experienced analysts. The intelligence community devotes substantial resources to developing predictions of adversary behavior (principally as a "gray matter" rather than automated process). This "analysis and production" stage is made far more difficult by asymmetric threats, as adversaries need no longer be sovereign states and can exhibit a breadth of political goals that extend beyond conventional sources of international conflict such as border disputes or control of resources.

Finally consider behavioral models. For adversary decision modeling, tactical goals will replace the software application goals (in the user intent case) that result from the intent inference process. Descriptive intent inference in this case would result in identification of an adversary force's objectives and, given models of tactical reasoning, could recommend appropriate reactions. Predictive intent inference would indicate expected activity by the adversary and explain the reasons behind that activity. Diagnostic intent inference could produce alerts of attempted subterfuge or uncover missteps on the part of the adversary.

Similarly, intent inference of echelons of adversary forces provides advantages analogous to those arising from team intent inference. Identification of the goals of one adversary group can be used as a discriminator in identifying the goals of other subsets of the adversary. Intent inference across groups of the adversary could also result in the discovery of breakdowns among those groups – knowledge that can be used for tactical advantage.

4. Approach

Our discussion in the previous section discussed how user intent inference could form the basis for an
adversary intent approach, and outlines some of the challenges unique to the adversarial domain. In this section we summarize our overall approach (Figure 2) and the specific technologies we bring to bear on each of the three phases in the intelligence cycle: collection, processing, and analysis and production.

4.1. Intelligence Collection with Intelligent Agents

Automation support for collection is needed to extend the reach of collection devices and analysts without overextending the human capital required to monitor and gather the data. Instead, analysts require intelligent agents, who can be tasked to monitor one or more information sources and report back when some set of conditions is satisfied. In our approach, intelligent agents provide this persistent monitoring capability. Agents can be created dynamically (by a user or by another agent) and given instructions specifying where to go, what to do upon arrival at the remote host, and what (and when) to transmit information back. Deploying large numbers of intelligent agents addresses the acute collection problems presented by the adversarial domain.

4.2. Intelligence Processing with Information Fusion

Providing automation support for processing of raw information requires systems that can reason about the domain(s) under examination as a prerequisite to combining information drawn from that domain. At lower levels (Level 1 Fusion), data can be merged on the basis of algorithmic approaches with less emphasis on domain knowledge. As information to be combined moves up the abstraction hierarchy (Level 2 Fusion), reasoning plays a more prominent role. In our previous fusion work under the Rotorcraft Pilot's Associate program, for instance, combining track data required both a fusion algorithm and a domain ontology ([11], [12]).

Our approach to overcoming the combinatorial problems likely to be encountered in the adversarial domain rests on carefully controlling how information gets combined via a Threat Evidence Monitor (TEM). The TEM receives requests from the inference element (Bayesian Network; see next section) and then tasks intelligent agents with collecting information relevant to a given request. Information returned by the agents is fused by integrating our Level 1/Level 2 fusion capabilities, domain ontologies, and semantic web technologies being developed for the DARPA Agent Markup Language (DAML) program. One objective of DAML is to provide for semantically-tagged web content, and to create a rich set of ontologies for defining the entities and relationships that are representing in DAML-formatted web pages and databases. The agents tasked by the TEM can then retrieve information from battlefield sources as well as from web pages. After applying its domain-guided fusion process, TEM sends the fused information back into the Bayesian Network.
4.3. Analysis and Production with Adversary Decision Modeling

To help provide automation support for the Intelligence Analysis and Product process, our approach employs user ontology networks (as represented by Bayesian Networks) as a tool for representing the possible decision making behavior of an adversary, while capturing and reasoning about the probabilistic nature of the process. Our model consists of the three components discussed earlier: Interests, Preferences, and Context. Using the observables and inputs from our human analysts, this model performs our intent inference and updates the enemy commander intent model as needed via the CIA sub-module.

We can also apply our team intent inference approaches to collections of enemy commander intent models. The hierarchical structure of team intent models maps naturally to the hierarchical nature of military command. By performing team intent inference with respect to echelons of enemy commanders, we can better understand the goals of individual commanders, identify particularly important objectives (when multiple commanders work toward the same small-scale goal), and detect breakdowns in the enemy’s communications (when multiple commanders work toward cross-purposes).

5. Current Status & Future Work

We have outlined the need for adversary intent inference in order to effectively confront asymmetric threats and to support emerging doctrine such as Effect Based Operations. Our previous research in User Intent Inference was presented as a basis for Adversarial Intent Inference that applies similar techniques but which also poses unique and serious challenges. To better reveal where our technologies fit and where they need to be expanded, we summarized the difficulties of inferring an adversary’s intent, broken down into the discrete phases of the intelligence cycle. We then introduced the specific technologies we bring to bear on each phase as part of our overall approach to adversary intent inference.

Our work is in the definition phase and this document reflects both our past experience and current plans. In the coming weeks and months we will engage with various end-user groups in the intelligence community to build a preliminary adversary intent model and to identify the information sources to be accessed. A preliminary prototype will be developed during the first year.

6. References


Author Biographies

BENJAMIN BELL is in the Artificial Intelligence Laboratory at Lockheed Martin Advanced Technology Laboratories, where he investigates intelligent interactive systems, decision support and training. He previously served on the faculty of Teachers College, Columbia University.

EUGENE SANTOS, JR. is currently Interim Director for The Taylor L. Booth Research Center at the University of Connecticut and an Associate Professor of Computer Science and Engineering in the Computer Science and Engineering Department. His areas of research interest include multi-agent systems, intelligent information systems, decision support, intent inference, human-computer interaction, intelligent user interfaces, uncertainty, and probabilistic reasoning.

SCOTT BROWN is currently the lead engineer for the Information Warfare Planning Capability (IWPC). He previously served as the program manager of an advanced research development program at the Human Effectiveness Directorate, Air Force Research Laboratory. His research interests include knowledge elicitation and representation, intent inference, information visualization, and intelligent user interfaces.