Making Sense of Adversaries' Plans

Tatiana Kichkaylo (Workshop Participant)
Robert Neches, Michael Orosz, Ke-Thia Yao (Other Team Members)
University of Southern California Information Sciences Institute
Marina del Rey, CA, 90292
{tatiana, rneches, mdorosz, kyao}@isi.edu

What should be of highest priority in the analytic process – the attempt to decide what the adversary has decided – is often shunted aside…
-- Cynthia M. Grabo, **Anticipating Surprise**

A key challenge for counterterrorism analysts is to anticipate terrorist actions – i.e., to infer potential terrorist goals and plans by combining knowledge of capabilities with observations of activity and use those inferences to predict critical likely next steps which are important to attempt to observe or forestall. Accomplishing this effectively requires collaboration of multiple experts with different areas of expertise, consideration and winnowing of large numbers of alternatives, and analysis of masses of historical data. Human participants in the process are often separated by space (or administrative boundaries) and time. In addition, the problem itself is continually and rapidly evolving – the adversary constantly obtains new equipment, develops new strategies, and changes goals. To keep up, a tool for collaborative sense-making of adversarial plans must support various modes of distribution and offload from humans the burden of keeping track of details and dependencies – but still allow human knowledge and intuition to guide the process.

In our group at USC Information Sciences Institute we are developing just such a tool. The Risk Analyses and Models of Plans for Attacks to Recognize Terrorist Schemes (RAMPARTS) system is based on collaborative planning technology (CMMD [1]) previously developed for NASA Human Space Exploration program, and models and expertise from the National Center for Risk and Economic Analysis of Terrorist Events (CREATE). RAMPARTS will allow experts in different areas to add their knowledge to the system in the form of plan snippets. The system will match these snippets against observed data, such as historical records, and highlight discrepancies and missing pieces. The experts can then extend the knowledge base by adding new snippets to address the discrepancies. When multiple alternative snippets are applicable, RAMPARTS will compute multiple options, evaluate their feasibility based on available data, estimate relative likelihood of various options, and present all this information to the human expert. In the real-time mode (as opposed to historical analysis), RAMPARTS will use the same snippets to predict next steps of the adversary's plans, i.e. not yet observed data.

We believe our approach has a number of benefits:

- Experts in different areas can focus on what they know best. There is no need for a single omniscient analyst.

- Knowledge is accumulated over time (and space). Snippets provided by one expert to explain one scenario can be later reused in a different situation.
- The system helps maintain continuity of thinking on the part of analysts using it, because historical and real-time analyses are performed in the same system using the same data representation and user interface.
- The system supports both bottom-up and top-down exploration, allowing the users to figure out adversaries' goals based on observed activity and to predict their next steps.
- The system supports continuous self-evaluation and improvement during use, precisely because it integrates historical and real-time analyses, as well as top-down and bottom-up exploration, in a single system that records audit trails of its usage.
- By keeping track of dependencies and alternatives, RAMPARTS allows its users to explore many options and focus on their significance. Taking over some of the bookkeeping in this fashion uses computers for things at which they excel, and at the same time makes better use of human expertise and intuition.
- Although RAMPARTS reduces mental effort on bookkeeping, it does not prevent users from tracking issues themselves which have not yet been communicated to the system. This avoids the "all-or-nothing" problem of many other systems which can only offer utility in a prospective but never-arriving future when their data and models are complete.

We originally developed the snippet-based planning engine for the CMMD project to facilitate collaborative mixed-initiative planning and what-if analysis. In RAMPARTS, we plan to focus on helping users make sense of observed activity by helping them investigate the composite plans with which the observations are consistent that can be constructed from available snippets – as well as helping them capture their own sense-making of adversaries' actions as additional new snippets reverse-engineered from observed activity. We also plan to add support for Bayesian reasoning to model confidence in observations and likelihood of different possible explanations of the observations.

Our previous projects allowed us to investigate various aspects of the mixed-initiative planning process, such as data representation and user interface for helping users make sense of plans, evaluate alternative plans, and understand decisions made by the automated algorithm. We hope to share our expertise with other workshop participants, explore synergies between making sense of plans vs. making sense of data, and learn more about collaborative aspects of the sense-making process.

[1] E. Balaban, M. Orosz, T. Kichkaylo, A. Goforth, A. Sweet, and R. Neches. "Planning to Explore: Using a Coordinated Multisource Infrastructure to Overcome Present and Future Space Flight Planning Challenges", *AAAI 2006 Spring Symposium on Distributed Plan and Schedule Management*.