Abstract—One of the major challenges in counter-terrorism analysis involves connecting the relatively few and sparse terrorism-related dots embedded within massive amounts of data flowing into the government’s intelligence and counter-terrorism agencies. Information technologies have the potential to empower intelligence agencies or analysts with the ability to find pertinent data faster, conduct more efficient and effective analysis, share information with others if necessary, relay concerns to the appropriate decision-makers, and ultimately put the data into a form that allows senior decision-makers to understand and act on it so that they can anticipate and preempt terrorist plots or attacks from occurring. Advanced collaboration among multiple analysts or tools is one such crucial technology. In this paper, we introduce NEMESIS (NEtwork Modeling Environment for Structural Intervention Strategies), a collaborative environment to integrate and share information among different counter-terrorism analysis tools. Two component tools, ASAM (Adaptive Safety Analysis and Monitoring System) and ORA (Organizational Risk Analysis), are described in this paper. The functionality of these two tools, along with the NEMESIS collaboration is illustrated via a real world example gleaned from open sources.

1. INTRODUCTION

A report filed by Congress assessing the events leading up to the 9/11 attacks suggests that there was sufficient amount of intelligence available for the “dots” to be connected — if it was not for the overwhelming amount of data available at that time, this could have been achieved. In order to prevent this from happening again, researchers within the intelligence community have begun working on advanced intelligence analysis tools using state-of-the-art information technology. These tools can empower intelligence agencies with the ability to find pertinent data faster, conduct more efficient and effective analysis, share information with others, relay concerns to the appropriate decision-makers, and support them with better information to make effective decisions [12].

From the perspective of an intelligence analyst, the majority of their time is spent on collecting data, when ideally it should be spent on analysis. Key information technologies for counter-terrorism analysis include advanced collaboration, decision support, hypothesis generation, automated data management and data processing. These technologies represent broad categories and are meant only to provide a relative framework for counter-terrorism analysis and encompass the many new advanced technologies under development. In order to collaborate efficiently and effectively, distributed teams within the intelligence community require a forum in which they can share ideas and solve complex problems, monitor their own effectiveness and dynamics as a team, systematically evaluate differing opinions, and generate alternative scenarios. Considering the massive amount of information and the difficulty in connecting the dots, a set of tools capable of automated evidence collection, evaluating alternative hypotheses, and supporting evidential reasoning would be invaluable [1]. In this paper, we focus on a set of collaborative tools for identifying, tracking, and mitigating terrorist activities. Three major components of the collaborative environment are described and illustrated using an Indian Airlines (IA) hijacking example: (1) NEMESIS, which provides a forum for information exchange among multiple modeling or analysis tools, and model-based team collaboration; (2) ASAM, which is based on a novel combination of hidden Markov models (HMMs)
to detect and provide soft evidence on the states of terrorist activities using partial and imperfect observations, and Bayesian network (BN) model that integrates the soft evidence from multiple HMMs and estimates global threats; and (3) ORA, which combines ideas from social network analysis, organizational theory, and computational sociology to model the information flow and diffusion within terrorist networks, evolution of terrorist networks, and other related concepts.

The paper is organized as follows. Section II describes the NEMESIS collaborative environment for modeling and analysis. Section III summarizes the ASAM system that provides early warning to facilitate preemption and increase the range of options for counter-terrorism agencies. Section IV provides a brief description of the ORA tool that detects risks and vulnerabilities in the terrorist organizations. In section V, the utility of the ASAM and ORA tools as well as the NEMESIS environment is illustrated by way of application to the IA hijacking example. Section VI concludes the paper with a summary and current research direction.

2. COLLABORATION VIA NEMESIS

NEMESIS is an IT-based collaborative environment for counter-terrorism analysis, which provides access to different modeling and analysis tools. With a set of collaborative analysis tools, intelligence and policy analysts can improve their capabilities to identify, understand, and mitigate terrorist activities from an organizational perspective using a well-designed XML-Schema-based language termed ODL (Organizational Descriptive Language).

Collaboration artifacts such as E-mails, chats, or forums, are rarely or never need to be revised. However, modern collaborations produce artifacts that are subject to revisions. Some examples include collaboratively authored documents, scenarios and models of terrorist organizations, structured argumentation, strategies, and plans. The revisions come about because participants in the collaboration agree that new data, new analysis, or new discussion should be reflected in the official “best guess.” Multiple hypotheses about the best representation of the actual state of the world, exploratory investigation, and changes to subordinate collaboration artifacts on which a super-ordinate artifact depends should be accommodated. It is important to keep the revisions of the collaboration artifacts synchronized, so that multiple analysts can work on an intelligence problem independently and concurrently. The collaboration artifacts thus need to be controlled to prevent work from being lost or delayed.

One of the key purposes of NEMESIS is to integrate different modeling methods. Figure 1 illustrates that different modeling methods \( M_A, M_B, \ldots \), may have their own data sets \( D_A, D_B, \ldots \), and that each data set has a reference to an organizational description \( C \) expressed in the ODL. ODL represents commonalities among modeling methods with a core set of constructs, and accommodates unique requirements of specific methods with ODL extensions.

As shown in Figure 2, NEMESIS has a service-oriented architecture, and ODL provides a focal point for integration. Multiple applications extract or produce ODL descriptions via adaptors, and models and associated data are stored via a collaborative artifact version server (CAVS). Collaboration tools include Groove™ workspace from Groove Networks and clients for CAVS such as RapidSVN [6]. Network visualization is a tool that graphically visualizes the organizational network described in ODL. The NEMESIS repository is hosted on the server side and the ODL files are saved in an appropriate mainline or branch of the repository.

ODL provides a platform to experiment with ways to represent organizations in NEMESIS. It builds on the foundations of DyNetML [9] and is designed for modularity following the general approach of XML. ODL consists of groups of node types: agents, knowledge, tasks, events, resources, locations, communications, and organizations. Each node type has attributes such as name, ID, delta, and binding. A delta element describes the difference between the same nodes in different time slices, and a binding expresses a placeholder to represent uncertain or incomplete facts. The major objective of ODL is to integrate organizational analysis tools by expressing core organizational facts. However, these organizational analysis tools are quite diverse and require significant
amount of specialized information in addition to the core organizational facts. In the following two sections, we introduce two tools which have been integrated into the NEMESIS environment, viz., ASAM (shown as a transactional network tool in Figure 2) and ORA (shown as a social network tool in Figure 2). Models in ASAM are represented in an extension to ODL named AsamML. HMMs in AsamML are described as organizational elements that are snapshots of an actual organization. That is, one HMM corresponds to one organization. BNs are captured in an ODL extension similar to a well-known representational format named XMLBIF. Models in ORA are represented in DyNetML, which has a rich representation of organizations. NEMESIS provides XSLT-based translations between ODL and DyNetML.

3. THE ASAM SYSTEM

The ASAM system, developed by the University of Connecticut, is an information analysis tool designed to support strategic decision-making, provide early warning to facilitate preemption, increase the range of options and probability of success, and integrate information in a scalable way. The basic premise of the ASAM system is that terrorist networks can be evaluated using transaction-based models. This type of model does not rely solely on the content of the information gathered, but more on the significant links appeared in certain sequences between data entities (people, places, things) that appear to be suspicious. For example, an unknown person withdraws money from his/her bank account, uses that money to purchase chemicals that could be used to make a biological weapon, and then buys a plane ticket destined for the United States. This sequence of events suggests a reason to be concerned; it may or may not arise from terrorist activity, but ought to be flagged for more careful scrutiny. The ASAM system interprets the information by comparing a repository of a priori story schemas to actual observations of temporal data stored in an intelligence database. Based on the similarities between the observed temporal data and the given story schemas (templates), the likelihood of observed data given the templates is assessed. The following section summarizes the methods by which the ASAM system models and detects terrorist activities.

As shown in Figure 3, the ASAM process is a hierarchal combination of HMMs and BNs. HMMs are well known for modeling embedded stochastic processes and are therefore an ideal way to make inferences about the evolution of terrorist networks [3]. HMMs function at the lowest level of the ASAM process by taking observations of temporal data and comparing them to a priori story schemas via data association methods. As the HMMs track the evolving terrorist activities, they continuously evaluate the likelihood of the observed events. If and only if the accumulated observations are significant enough for the HMM detection schema (CuSum statistics) to be above a pre-specified threshold, the HMM will report its confidence of the occurring of the modeled terrorist activity to the higher level BN (or sub-BN). BNs combine the updating from many different HMMs (story schemas) to evaluate the overall threat of terrorist activities in a form of probability distributions. In other words, the BN represents the overarching terrorist plot and the HMMs – which are related to each BN node – represent more detailed terrorist subplots. It is important to note that the HMMs function in a faster time-scale than BNs because the HMMs model the evolution of the transaction space, i.e., they process new information every time a transaction occurs. Each HMM can be viewed as a detailed stochastic time-evolution of a particular node represented in the BN. In other words, HMMs can be viewed as distributed sensors to collect and preprocess the information and the BNs are acting as fusion centers in different granularity. Figure 4 shows an example of ASAM model, where the node A and node B in BN has HMM_A and HMM_B as evidential sensor, respectively. A more detailed example highlighting the interrelationships between the HMM and BN models is provided in section V.
transactions are made in the transaction space. One of the benefits of using HMMs is that there exist ways to detect the presence of an HMM among noisy benign data – this is analogous to finding a needle in a haystack and is one of the major problems associated with counter-terrorism analyses.

By using advanced detection methods and standard HMM algorithms such as the forward-backward, Viterbi, and Baum-Welch [7], we can detect suspicious activities and develop models for counter-terrorism that are more accurate and effective than is possible with manual methods being practiced today.

In addition to the two major inference engine, i.e., HMM detection engine and BN Bayesian inference engine, the architecture within the ASAM system consists of three more modules: graphical modeling interface, web-based visualization, and knowledge repository. All of these modules have the ability to communicate via a local host or network so that different agencies can work together on developing models, sharing information, and exchanging opinions. The graphical modeling interface is imbedded in TEAMS®, which can create a concrete ASAM model including the BN and HMM structures and all the necessary parameters. The web-based visualization provides users with the ability to obtain real time information about the state of the terrorist threat and the ability to test new hypotheses (so called what-if analysis). In order to facilitate collaboration within the intelligence community, the ASAM system has been designed to communicate with a central repository in NEMESIS via ODL. Whenever ASAM detects new activity or receives a new transaction, it updates the corresponding model and inference results for analysts to view from the NEMESIS repository. Once received, the NEMESIS system reports any new transaction data to the analyst, and provides the capability to analyze the new data using other counter-terrorism analysis tools, such as the ORA.

4. THE ORA TOOL

Carnegie Mellon University has developed a series of integrated tools for dynamically extracting terrorist network data, visualizing terrorist networks, identifying the “network elite” and points of vulnerability, and then evaluating the potential impact of various types of attacks on those networks. These tools include network-vis, a network visualization tool; ORA [8], a statistical toolkit for analyzing dynamic networks composed of multiple organizations; AutoMap [10], an automated text analysis tool that can extract relational data including social and role network data from text; and DyNet [11], a tool for simulating the evolution of these networks in general and after they have been attacked. Figure 5 shows the interoperability of these tools.

As part of NEMESIS, we have focused mostly on ORA, with network-vis as the network visualization tool and DyNetML as a way to exchange information with the ODL in the NEMESIS environment.

![Figure 5. Suite of CMU Tools](image)

ORA is a network tool that detects risks and vulnerabilities in an organization’s design structure. The design structure of an organization is the relationship among its personnel, knowledge, resources, tasks, and entities. These entities and their relationships are represented by a collection of networks called the Meta-Matrix. Table 1 lists the available Meta-Matrix in ORA.

<table>
<thead>
<tr>
<th>Entities</th>
<th>Actor</th>
<th>Knowledge/Resources</th>
<th>Events/Tasks</th>
<th>Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>Social Network</td>
<td>Knowledge/Resource Network</td>
<td>Attendance Network</td>
<td>Membership Network</td>
</tr>
<tr>
<td></td>
<td>Who talks to, works with, and reports to whom</td>
<td>Who has what expertise, or has access to which resource</td>
<td>Who is assigned to which task, who does what</td>
<td>Who belongs to which organization</td>
</tr>
<tr>
<td>Knowledge/Resources</td>
<td>Information Network</td>
<td>Connections among types of knowledge, resources, substitutions</td>
<td>Needs Network</td>
<td>Core Capabilities</td>
</tr>
<tr>
<td></td>
<td>What type of knowledge/resource is needed for that event/task</td>
<td>Which organization has what kind of knowledge/resources</td>
<td>Which organization has what kind of knowledge/resources</td>
<td></td>
</tr>
<tr>
<td>Events/Tasks</td>
<td>Precedence/Dependencies</td>
<td>Which events/tasks are related to which</td>
<td>Sponsorship Network</td>
<td>Which organization is sponsoring which task</td>
</tr>
<tr>
<td>Organizations</td>
<td>Inter-organizational Network</td>
<td>Alliance</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Meta-Matrix Showing Networks of Relations
ORA measure is a function that takes a Meta-Matrix and examines a particular aspect of its mathematical structure. ORA contains over 50 measures, and provides three classifications of them based on risk and vulnerability, input requirements, and type of output produced. For example, Critical Actor Risk is the risk based on the actors having exclusive knowledge, resources, or task assignments. ORA reads and writes network data in multiple formats to make it interoperable with existing network analysis software, such as DyNet [8]. In NEMESIS, the Meta-Matrix data is formatted as DyNetML. DyNetML supports multiple Meta-Metrics to be written in the same file, and each Meta-Matrix can have different Agent, Knowledge, Resource, Task, and Organization node sets. ORA generates the risk and vulnerability report from the measure analysis, both for a single organization and for comparing two Meta-Matrix organizations.

ORA advances the state of the art in network analysis tools by being organized around the unifying concept of the Meta-Matrix. Measures are organized to facilitate their coherent use. In particular, they are categorized by how they measure the risk and vulnerability of an organization’s design structure. ORA reads and writes in multiple data formats and is interoperable with existing network analysis software. Entire Meta-Matrices can be visualized using different layout algorithms. The integrated Optimizer adapts an organization’s design structure according to user specified criteria, and the resulting organization can be visualized and analyzed with ORA. ORA is being actively developed and tested in a wide range of context.

5. Example

The Indian Airlines (IA) hijacking example we illustrate here is extracted from open source information from the Embassy of India [4] and the Frontline magazine [5]. The example contains patterns of actions and responses that are present in the actual hijacking of IA’s IC-814 flight, which occurred on December 24th, 1999 in Kathmandu and ended on December 31st when the government of India released three high profile terrorists. The following sections describe the analyses of IA hijacking example via the ASAM system and ORA tool in NEMESIS.

The organizational model of IA hijacking is represented in such a way that the ASAM and ORA tools can work with the ODL data. Figure 6 shows that multiple organizations analyze the same problem via diverse tools under the NEMESIS environment. The key feature of NEMESIS for collaboration is its capability to store, and manage different versions and configurations of models. ODL is structured to allow for modular extensions to accommodate current and future specific tool requirements.
The analysis of IA hijacking model is done by importing the model from the NEMESIS repository to the local repository in the ASAM system. The top level of the ASAM process is a BN, which represents the causal relationships among the events. Figure 7 illustrates the BN model of the IA hijacking example. In the following simulation, the prior probabilities associated with the BN nodes are held constant, while the statistical inferences calculated by the underlying HMMs (‘Planning and Strategy’, ‘Collect Resources’ and ‘Preparations for Hijacking’) update the global beliefs of the BN. The global effect of these numerous terrorist activities causes the belief of the BN node, ‘Hijack’, to change. The state of ‘Hijack’ BN node is a probability mass function which shows the posterior probability of hijacking. All the BN nodes are assumed to have discrete states.

In this model, three HMMs symbolize the planning and strategy, resource collection and the preparations for hijacking. Due to space limitations, only the Markov chain of ‘Collect Resources’ is shown here. Details of other HMMs are discussed in [2].

Figure 8 shows the HMM corresponding to ‘Collect resources’, while it includes the transactions that are involved in collecting the necessary resources to carry out a hijacking. The ‘Collect Resources’ HMM has eight states which are indicated by S1, S2, …, S8, and the transition probabilities are indicated next to transitions. Planners hold meetings with hijackers, and assign individual roles and identities for the hijacking. Planners obtain money through the high command of the terrorist organization, and they utilize the money to purchase forged passports, fake driving licenses, and satellite phones. Planners also acquire and transport the arms, ammunition through connections with local organized crime cells.

The BN merges all the available information from diverse sources and generates a global alarm, which is shown in Figure 9. For simulation purposes, we speeded up the flow of the new transactions to every few seconds, with the actual dates associated with the IA hijacking events labeled in the figure.

**ORA Analyses of the IA Hijacking Example**

Based on the ODL file for the IA Hijacking model, a customized extraction engine for ORA pulls out the relevant networks and puts the data into DyNetML. This data is then read into ORA and analyzed and visualized with networkvis. In this example, there are 20 actors, 13 resources and 13 tasks. There is a one-to-one mapping of resources and knowledge. Further, all the actors are associated with a single group.
Currently, ORA simply reports the results, as shown in Table 2, as part of the Intel report. We are currently expanding this report to include confidence in the results, comparative evaluation with other networks, and key possible actions indicated by that data. For example, a typical network might have a density closer to .28, and an average degree centrality of .28 and betweenness of .06. Thus, the individuals who stand out here are much less connected than we would see in typical western networks. This may suggest a different mode of conducting operations; however, a more likely explanation is that there is substantial missing information – possibly as high as 87%.

The full meta-matrix is shown in Figure 10. One of the keys in facilitating analysis will be to extend ORA to display visually changes in these networks over time and to highlight critical actors.

Table 2. Intel Report from ORA for IA Hijacker Data

<table>
<thead>
<tr>
<th>Measure</th>
<th>Value</th>
<th>Definition</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cognitive Demand</td>
<td>.069</td>
<td>Akhtar</td>
<td>Actor with highest Cognitive Demand</td>
</tr>
<tr>
<td>Total Degree</td>
<td>.079</td>
<td>Abdul Latif</td>
<td>Actor with highest Total Degree Centrality</td>
</tr>
<tr>
<td>Betweenness Centrality</td>
<td>.012</td>
<td>Harkat-Ansar</td>
<td>Actor with highest Betweenness Centrality</td>
</tr>
<tr>
<td>Task Exclusivity</td>
<td>2</td>
<td>Akhtar</td>
<td>Actor with highest task</td>
</tr>
</tbody>
</table>

7. SUMMARY

Information technologies are essential for the global war on terrorism [1]. This paper proposed a collaborative analysis environment, termed NEMESIS, that utilizes various information technologies to collaborate, evaluate, share, and act on the information faster to detect and prevent terrorist attacks. We described the versioning of collaboration artifacts in NEMESIS when multiple tools or analysts are concurrently working on the same problem but may from different point of view. The two analysis tools integrated within the NEMESIS environment, the ASAM system and the ORA tool, were then introduced. The ASAM system combines the HMM and BN methods to detect terrorist activities and generate global threats. The ORA tool, based on social network analysis, models the information flow within terrorist networks and the evolution of the terrorist networks over time. The feasibility and functionality of the NEMESIS collaboration was demonstrated using a real world example, the 1999 Indian Airlines hijacking problem, extracted from open sources.

The current implementation of NEMESIS provides collaboration among different tools by sharing the same set of data. In the future, ODL will be extended to describe transactions so that the adaptors associated with analysis tools are able to accept ODL formatted transactions as inputs. The NEMESIS environment has the potential to be integrated with additional organizational modeling tools. Meaningful collaboration and tool effectiveness measurement will also be developed.

There are some major extensions being pursued for both the ASAM system and ORA tool. For example, the ASAM system is incorporating feature-aided (attribute-aided) threat tracking to include the features of people, places and infrastructure targets into the HMM models. In addition to the analysis of terrorist activities, we are also working towards the optimization of possible counter-terrorism actions to preempt terrorist attacks. The website and repository are under improvement at the mean time. Future work on ORA will address all aspects of its core functionality, including: extending the meta-matrix manager to allow multiple matrices of a single type; allowing the
user to specify the input for measures; displaying matrix data in an editable spreadsheet window; generating reports with multiple types; and improving the user interface.

![The IA Hijacking Meta-Matrix](image)

**Figure 10.** The IA Hijacking Meta-Matrix

**REFERENCES**


**BIOGRAPHY**

Robert Popp is presently serving as the Deputy Director of the Information Exploitation Office (IXO) at the Defense Advanced Research Projects Agency (DARPA). Dr. Popp
previously served as a Special Assistant to the DARPA Director for Strategic Matters, and earlier as the Acting and Deputy Director of the Information Awareness Office (IAO). Prior to DARPA, Dr. Popp served as an Assistant Deputy under Secretary of Defense for Advanced Systems and Concepts (AS&CC). Before joining the government, Dr. Popp was a Senior Scientist and Program Manager with BBN and ALPHATECH. Dr. Popp received his B.A. and M.A. degrees in computer science from Boston University, and his Ph.D. degree in electrical engineering from the University of Connecticut. Dr. Popp has authored three book chapters, over seventy journal and conference papers, and is the holder of two patents. Dr. Popp presently serves as the Associate Editor for both the IEEE Transactions on Systems, Man and Cybernetics, and the Journal of Advances in Information Fusion. Dr. Popp is a member of the ACM, AAAS, senior member of the IEEE, and a lifetime member of HOG—Harley Owners Group.

Krishna R. Pattipati is a Professor of Electrical and Computer Engineering at the University of Connecticut, Storrs, CT, USA. He has published over 285 articles, primarily in the application of systems theory and optimization techniques to large-scale systems. Prof. Pattipati received the Centennial Key to the Future award in 1984 from the IEEE Systems, Man and Cybernetics (SMC) Society, and was elected a Fellow of the IEEE in 1995. He received the Andrew P. Sage award for the Best SMC Transactions Paper for 1999, Barry Carlton award for the Best AES Transactions Paper for 2000, the 2002 NASA Space Act Award, and the 2003 AAUP Research Excellence Award at the University of Connecticut. He also won the best technical paper awards at the 1985, 1990, 1994, 2002 and 2004 IEEE AUTOTEST Conferences, and at the 1997 and 2004 Command and Control Conferences. Prof. Pattipati served as Editor-in-Chief of the IEEE Transactions on SMC-Cybernetics (Part B) during 1998-2001.

Peter Willett is a Professor of Electrical and Computer Engineering at the University of Connecticut. Previously he was at the University of Toronto, from which he received his BS in 1982, and at Princeton University from which he received his PhD in 1986. He has written, among other topics, about the processing of signals from volumetric arrays, decentralized detection, information theory, CDMA, learning from data, target tracking, and transient detection. He is a Fellow of the IEEE, is a member of the Board of Governors of IEEE's AES society, and is a member of the IEEE Signal Processing Society's SAM technical committee. He is an associate editor both for IEEE Transactions on Aerospace and Electronic Systems and for IEEE Transactions on Systems, Man, and Cybernetics. He is a track organizer for Remote Sensing at the IEEE Aerospace Conference (2001-2003), and was co-chair of the Diagnostics, Prognosis, and System Health Management SPIE Conference in Orlando. He also served as Program Co-Chair for the 2003 IEEE Systems, Man and Cybernetics Conference in Washington, DC.

Daniel Serfaty is the Principal Founder of Aptima, Inc. Prior to founding Aptima in 1995, Mr. Serfaty was engineering group leader and program manager at ALPHATECH. He has published extensively in the fields of human decision-making, team and distributed processes, command and control, and human-machine interfaces. Mr. Serfaty’s academic background includes undergraduate degrees in Mathematics/Physics, Psychology, and Aeronautical Engineering from the Université de Paris and the Technion, Israel Institute of Technology, an MS in aeronautical engineering (Technion) and an MBA in International Management (University of Connecticut). His doctoral work at the University of Connecticut pioneered a systematic approach to the analysis of distributed decision-making in dynamic and uncertain environments. He is a member of Eta Kappa Nu and Sigma Xi and an active member of several engineering and psychology professional societies.

Webb Stacy is the Vice President of Technology at Aptima. Dr. Stacy has more than 15 years of experience in the software industry, with over 10 years in a management role. Dr. Stacy co-founded Softron. He was awarded a United States Patent on the technology. Prior to joining Aptima, Dr. Stacy was Vice President for Product Development at Clinsight Corporation. Before that, Dr. Stacy was Director of High Performance Computing Software at Compaq Computer Corporation. He was the business lead on a team that released Visual FORTRAN. Dr. Stacy came to Compaq from CenterLine Software, Inc.. Earlier in his career, Dr. Stacy developed a prototype expert system and created new technical approaches to computer-based training delivery for the Army. Dr. Stacy has a Ph.D. in Cognitive Science from SUNY/Buffalo, and a B.A. in Psychology from the University of Michigan.

Kathleen Carley is a professor at the Institute for Software Research International in the School of Computer Science at Carnegie Mellon University. She is the director of the center for Computational Analysis of Social and Organizational Systems (CASOS). Her specific research areas are computational social and organization theory; dynamic social networks; multi-agent network models; group, organizational, and social
adaptation, and evolution; statistical models for dynamic network analysis and evolution, computational text analysis, and the impact of telecommunication technologies on communication and information diffusion within and among groups. She is the lead developer of ORGAHEAD, a tool for examining organizational adaptation, CONSTRUCT-TM, a computational model of the co-evolution of people and social networks, DyNet, a computational model for network destabilization, BioWar a city-scale multi-agent network model of weaponized biological attacks, MECA and AutoMap which are computational tools for automated text analysis.

Jeffrey Allanach is a graduate student of Electrical and Computer Engineering at the University of Connecticut. He received his BS from UConn in December, 2003, and expects to receive his MS in May 2005. His current research interests include signal processing, and target tracking.

Haiying Tu received the BS degree in automatic control from Shanghai Institute of Railway Technology in 1993 and MS in transportation information engineering and control from Shanghai Tiedao University in 1996. She is currently a Ph.D. student of Electrical and Computer Engineering at the University of Connecticut (UCONN). Prior to joining UCONN, she was a lecturer of Tongji University in Shanghai, China and also worked as an employee of Computer Interlocking System Testing Center which belongs to the Ministry of Railway of China. Her current research interests include organizational design, Bayesian analysis, fault diagnosis and decision making.

Satnam Singh is a PhD student at Systems Optimization Laboratory, University of Connecticut. He received his MS degree in Electrical Engineering from University of Wyoming. Currently, he was the chair of IEEE-UConn Students Branch in 2003. His interests are signal processing and optimization.