Title: **Identifying Critical Resources and Operations of the Adversaries from Incomplete Data**

Topic 6: **Modeling and Simulation**

Authors:

Georgiy M. Levchuk
Aptima Inc.,
12 Gill Street, Suite 1400
Woburn, MA 01801
Phone: 781-496-2467
Fax: 781-935-4385
e-mail: georgiy@aptima.com

Bruce Skarin
Aptima Inc.,
12 Gill Street, Suite 1400
Woburn, MA 01801
Phone: 781-496- 2405
Fax: 781-935-4385
e-mail: bskarin@aptima.com

Krishna R. Pattipati
Professor, ECE Dept., UCONN
Storrs, CT
Phone: 860-486-2890
Fax: 860-486-5585
e-mail: krishna@engr.uconn.edu

Correspondence:

Georgiy M. Levchuk
Aptima Inc.,
12 Gill Street, Suite 1400
Woburn, MA 01801
Phone: 781-496-2467
Fax: 781-935-4385
e-mail: georgiy@aptima.com

This paper was cleared by 88 ABW/PA on 19-MAR-09 as Document Number 88ABW-2009-1094.

Identifying Critical Resources and Operations of the Adversaries from Incomplete Data

Georgiy Levchuk[1a], Bruce Skarin[a], Krishna R. Pattipati[c]
[a]Aptima Inc.
[c]University of Connecticut

Abstract

To succeed against superior resources and technology, modern adversaries typically adopt asymmetric tactics to wage unconventional warfare. Current adversaries organize activities through small covert groups based primarily on existing relationships among family and friends. Identifying the networks of individuals, organizations, activities, places, and resources that constitute these operations presents a significant intelligence challenge. A tool is needed that can rapidly and accurately identify the relationships among the resource components that make up a terrorist network.

In this paper, we describe a technology that Aptima Inc. is developing called the Behavior Signatures of Terrorist Networks (BESTNET). The BESTNET system will help analysts to identify and track the people, places, activities, and resources most critical to adversarial operations. To achieve high decision accuracy under severe information gaps, BESTNET integrates three technologies developed and empirically validated by Aptima: an adversarial network and mission identification system to determine the dynamic state of the hostile operations and their supporting organization; a socio-cultural simulation to predict the support to hostile organization in the areas of interest; and an organizational performance assessment tool to determine the adversarial actors and resources most critical to their operations.

Motivation: Analyzing Networked Patterns and Discovering Resources Critical to Enemy's Operations

A drug cartel offloads its cargo from a merchant ship to an unoccupied warehouse in Boston. A gun running organization makes a large transaction at an old farmhouse in a sparsely populated area in Georgia. An insurgent organization manufactures IEDs in a small house in northeastern Iraq. Each of these operations have their own "hidden" **mission** and **organization**: hostile actors perform their roles, interact and execute coordinated activities. Each activity must be conducted in some concrete geophysical location by some actual actor(s) – organizations, groups, individuals, – but the mission must stay invisible for operations to succeed. Many of these activities, if considered alone, look normal. It is often only the dynamics of activities in a pattern that constitute the threat. Identifying these patterns and the roles of actors performing hostile activities is critical to intervention and disruption of hostile actions before it is too late.

These patterns of activities do not happen in a vacuum, but rather in a *social and cultural environment* that is both dynamic and multi-faceted. In this environment, conditions may exist that are either *conducive* or *prohibitive* to adversary objectives. In addition to identifying hostile missions and networks, any forecasting solution will also have to address the conditions influencing their dynamics over time.

The facilities (needed to store weapon materials), knowledge (needed to manufacture weapons), transportation equipment (needed to transport materials), financial means (needed to acquire materials and equipment), ties in the society (needed to recruit personnel and collect intelligence against opposition), etc. – all these resources can be critical at different stages of the enemy's operations. Therefore, to have robust identification of key hostile resources and develop efficient counter-action plans, a technology is needed that can recognize the human and non-human elements of the adversarial

[1] georgiy@aptima.com; phone 781-935-3966x267; fax 781-935-4385; www.aptima.com

organization, analyze their interactions and influencing mechanisms with other elements in the environment, and understand the utilization of these adversarial elements over time.

Patterns of activities can be tracked by analyzing attributes of and relationships among *entities* – individuals, groups, organizations, places, knowledge, or physical resources. Entities can be linked based on data about their *relationships*, including communications, ownership, geo-spatial location , material flow, etc. Both entities and relationships can have other qualitative or quantitative information as *attributes* or *features* – e.g., capabilities of individual actors, group size, cultural identities, etc. Together, entities, relationships, and their attributes form *attributed relational graphs* (ARGs). In ARGs, entities are defined as nodes and relationships as edges/links.

Anticipated or hypothesized activity patterns and organizational networks can be defined by experts, based on what analysts are looking for, and extracted from historic data by automated means. In a hypothesized threat pattern, or *model network*, instead of specific entities we define the roles of hostile actors in RED organization and operations which are part of the mission that RED may execute. The goal of intelligence analysis is then to match model threat patterns with observed activity patterns and to assess how well observed interactions and attributes are supported by the hypothesized, potentially hostile model network. Matching enables not only assessing the current situation (“who *is doing* what to whom”), but also predicting future activities and roles of adversarial actors and resources (“who *will do* what to whom”). The BESTNET can automate such threat pattern matching achieving high accuracy in identifying adversarial organizational networks and missions, and calculate the criticality of resources to the mission objectives of the adversary.

Method: Integrating Behavior Prediction, Resource Support Forecasting, and C2 Simulation Models

Aptima developed a working prototype of the BESTNET decision support system that fused data from multiple intelligence sources to identify and track critical human and resource entities in adversarial organizations. BESTNET builds upon Aptima’s three empirically validated technologies: adversarial organization and mission identification, social and cultural dynamics modeling, and organizational performance assessment (Figure 1). The first technology -- **NetSTAR** (Network, Structure, Tasks, Activities, and Roles) -- performs probabilistic network pattern identification based on noisy observations about network nodes, links, and their attributes. The NetSTAR work, sponsored by DARPA, investigated the problem of recognizing the roles and relationships among individual actors and their resources to predict the structure and operations of networked adversaries in order to develop targeted counteractions against them. In an empirical study, NetSTAR significantly outperformed unaided human analysts in identification accuracy and handled significantly greater uncertainty and data complexity (Levchuk et al., 2007; Entin et al., 2007). The second technology -- **SCIPR** (Simulation of Cultural Identities for Prediction of Reactions) -- sponsored by AFRL, models social and cultural identities and interactions in the environment, and can forecast the support adversaries could receive from other organizations and members of the society. In a case study on Northern Ireland, SCIPR successfully simulated the polarization and voting behaviors observed throughout the Northern Ireland conflict. SCIPR has also been successfully transitioned to an operational group for COA analysis. The third technology -- **MOST** (Models of Organizations, Systems, and Technologies) -- has grown from years of successful modeling and experimentation on adaptive command and control organizations sponsored by ONR. It was developed to assess the performance and fragility of organizations performing planned missions. MOST was also empirically validated through a series of experiments to identify critical functions in both conventional and non-conventional command and control organizational structures. Together, these technologies can increase the accuracy of identifying critical enemy’s resources and reduce associated false alarms.

The main adversarial prediction functionality of the BESTNET decision support tool is based on NetSTAR. NetSTAR significantly outperformed unaided human analysts in identification accuracy and

handled significantly greater uncertainty and data complexity (Levchuk et al., 2006; Levchuk et al., 2007). NetSTAR algorithms identify **adversarial organizations** and **missions** from noisy data sources using a probabilistic attributed graph matching algorithms (Levchuk and Chopra, 2005; Levchuk, Levchuk, and Pattipati, 2006; Levchuk et al., 2007). The algorithms find a mapping of observed actors and events (the entities, or nodes, in observed data reports such as from HUMINT, IMINT, and COMINT sources) to organizational roles and mission tasks (nodes in the model networks from the hypothesis library). The outcome is a rank-ordering of hypothesized models of enemy organizations and missions by their likelihood values based on the match between observed data and each model network. This rank-ordering is returned to the analysts so they may see which of the hypothesized adversarial organizations and missions are most likely to be present in the observed data.

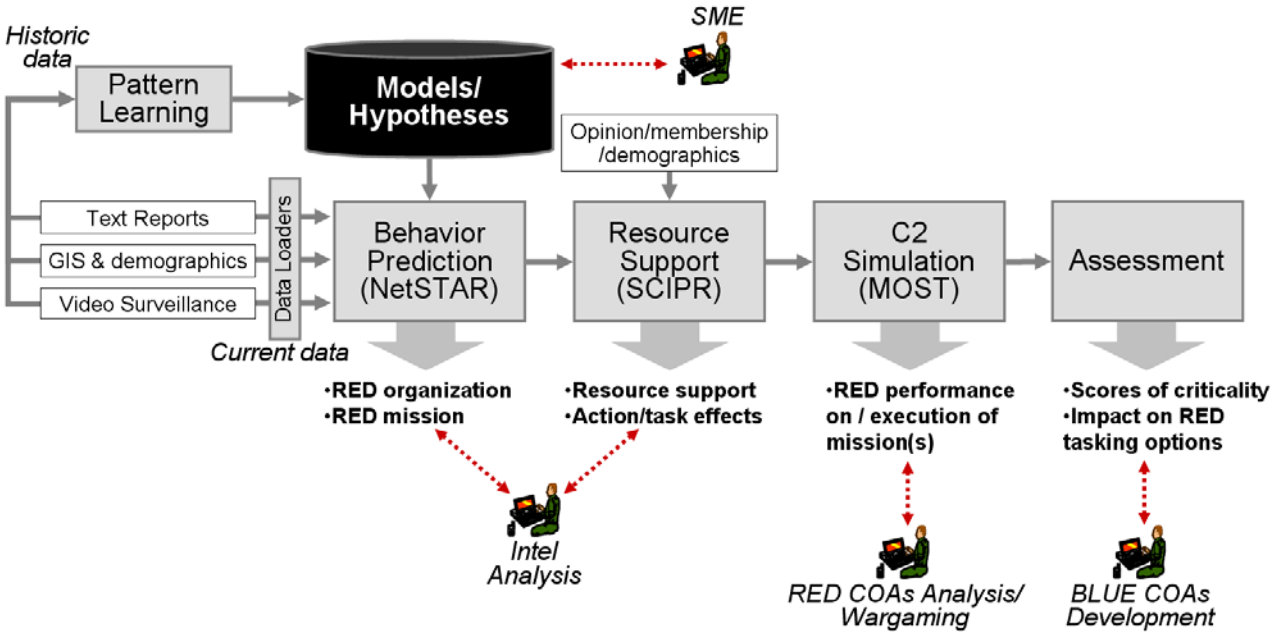


Figure 1: BESTNET Components, Technologies, and System Workflow

The probabilistic graph matching algorithms developed in NetSTAR have several advantages over traditional approaches of individual actor mapping and network analysis, due largely to the fact that the essential phenomenon is not executed at the individual actor level: terrorist activities are carried out by groups of organized adversaries who plan and use resources. These groups and their activity patterns leave potentially detectable traces in information space and are the focus of analysis by NetSTAR. It combines individual and network properties to perform threat pattern mapping and uses relational and temporal information to remove noise transactions from the data. This combination of domain-specific predictions of socio-organizational information and enemy’s mission objectives results in effective discovery of the most critical adversarial activities and resources. The calculation of criticality of adversarial resources is based on a novel fusion of the socio-cultural dynamics models of SCIPR and the organization-mission performance analysis of MOST.

Example of the Situation and Data

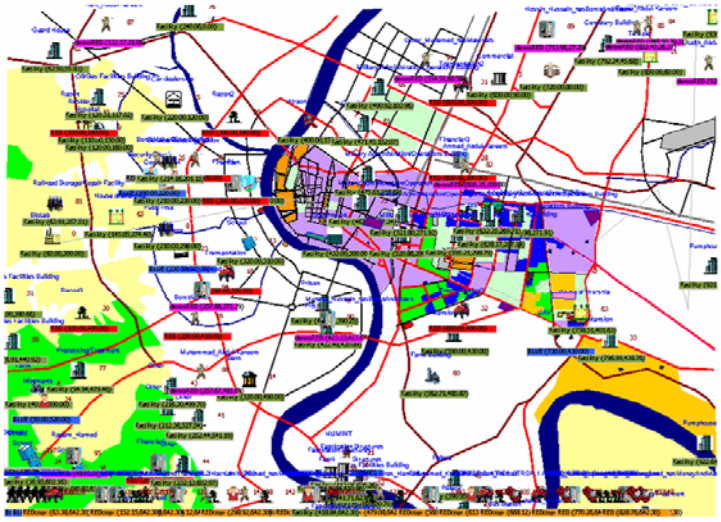
We developed and conducted analysis on a simulated synthetic scenario of adversarial behavior incorporating various types of hostile behaviors that might occur in real world. Synthetic data is needed because real-world data is often classified and rarely contains the ground truth about the reasons or prerequisite actions of the adversaries. This ground truth is required to measure the accuracy of predictive algorithms. We also needed situations with diverse hostile behaviors to test the accuracy of

predictive algorithms in recognizing different types of hostile operations. Usually, single real-world data set would contain similar attack types and therefore is not enough for thorough sensitivity analyses.

Our synthetic data scenario intentionally resembled the data that can be obtained using open source and classified data collection. We focused our example on a fictitious 3-rd world country with simulated adversary, U.S., and local police and government actions taken in the ongoing conflict. The data included time-stamped events describing the activities and various attacks. Each event included geo-coordinates, event category, name of the group/person conducting the activity, attack mode, target type, among others. The event stream included precursor operations to different attack patterns. We manually developed synthetic patterns of attacks that resemble different adversarial behaviors and intents. The event data was supplemented with structural geo-spatial data, including knowledge of the buildings, roads, and their attributes for the area of analysis. In addition, we simulated the data of the population profile for the terrain, which included the distribution of specific types of homes, people’s social, family, economic, and cultural information.

The terrain and actors

The simulated terrain in our dataset included structural information about buildings and geo-political areas. Our data consisted of a list of buildings/areas together with their location, size, and function. We have used seven functions: plant, transportation, government, military, infrastructure, social, and residential. The area had several types of facilities and areas, including houses of worship, military administration facilities, water treatment facilities, schools, oil service facilities, shopping centers, government office buildings, police stations, parks and entertainment centers, manufacturing and laboratories, storage and warehouse facilities, automotive repair centers, rental facilities, etc. We used these types and functions to create a scenario diverse for the analysis and resembling the real-world urban landscape. Figure 2 shows buildings/areas layout in our scenario, and provides an example of their functions. In addition to size and function of buildings, we used other attributes, including data about the neighboring population, cultural trends, demographics of the region, etc.



Building/Area	Function
BioLab	plant
Mall	infrastructure
Airport	infrastructure
Park	Social
Farm	infrastructure
Government	Government
Temple	Social
Oil/Gas Facilities	Military
House of Worship	Social
Military Administration	Military
Single-family Home	Residential
Service/Refueling Station	infrastructure

(a) Building Layout for BESTNET Use-case

(b) Example of Building List and Functions

Figure 2: Building Layout and Functions

Buildings and areas in the use case were passive actors, to which we sometimes refer to as targets. The active actors in the use-case have been defined to represent the members of RED team, the elements of BLUE forces and their assets, and other actors such as non-government organizations (NGOs), normal people in the environment, etc. The adversaries were represented by a set of teams, including reconnaissance (RT), explosives specialists (ET), truck and transportation (TT), financial (FT), attackers

(AT), and support teams (ST). The types of teams have been selected based on the activities and groups taking responsibility in the real-world open source data we have obtained from our customers.

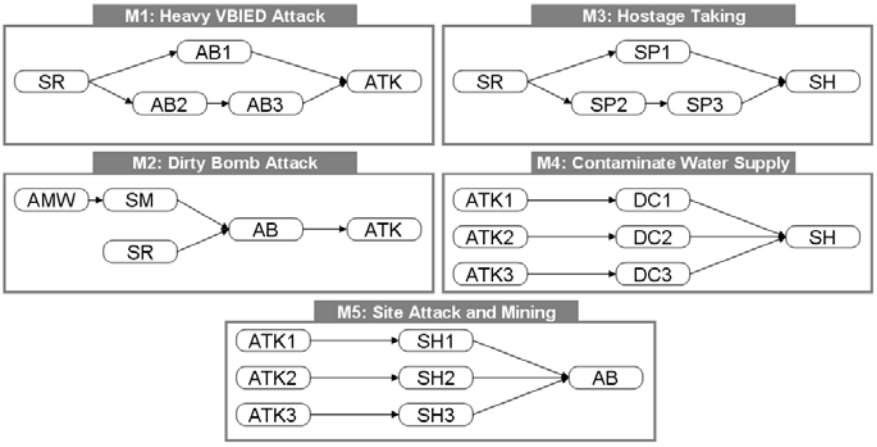
The situation, RED missions, activities, and organization

In the area of interest, several adversarial attacks were simulated over time. Each attack became a record event in the dataset with time- and location-stamping. We simulated several different types of hostile actions in the data, including bombings, kidnappings, small-arms engagements, etc. All the attacks must be prepared and will progress in multiple stages. For example, the bombing attack requires acquisition of explosive materials, bomb assembly, and transportation. We thus generated a set of mission patterns to represent the different types of attacks and their preparations. The execution of preparation activities and final attacks has been simulated by our performance simulation engine. Knowledge of the ground truth in synthetic data, resembling in nature hidden adversarial operations, gave us the ability to analyze the predictive power of BESTNET and to measure its recognition accuracy. We have developed manually several synthetic adversarial mission patterns and ran the simulation comparing the predictive algorithm capability against each of them. An example of five such patterns is shown in Figure 3.

Mission design captured the spatial information (information about task locations via specification of target requirements), temporal information (sequencing of tasks according to precedence constraints in the mission), and type information (overlap in the types of activities that need to be performed). The use case contained different modus operandi (missions) for adversaries that, while distinct in the objective for the adversaries, had overlapping operations. For example (Figure 3), mission M1 (Heavy VBIED Attack) and M2 (Dirty Bomb Attack) both contains instances of reconnaissance, attack, and weapons assembly operations, while the operations distinguishing these missions included material acquisition and storage tasks. In addition, we intentionally created the tasks that had overlapping requirements, so that missing action observations could result in the confusion of associating these observations with more than one task.

Tasks	Acronym
Site reconnaissance	SR
Set in position	SP
Overpower security / take hostages	SH
Acquire bomb materials/ chemical waste	AMW
Explosives/weapon attack	ATK
Dump contaminant	DC
Assemble bomb	AB
Store materials	SM

(a) RED Tasks/Activities



(b) Example of RED Missions from Use-Case

Figure 3: The Set of Hypothesized RED Missions in BESTNET Use-case

RED actors can take different roles and form different adversarial organizations depending on the membership of actors in different cells and their subordination to intermediate RED commanders. For our use-case, we manually designed several synthetic organizational structures that might represent different ways in which RED can organize. Figure 4 shows an example of command structures for four alternative organizations. We modeled the same execution actors for all organizations for simplicity, while the number and types of adversarial cell commanders, as well as command structure and responsibilities, is different. For example, multi-cell organization (Figure 4(c)) has thee independent weapons manufacturing and setup cells controlled by the weapons leader, who in turn supports the leader/commander of the enemy organization, and in the flat command structure (Figure 4(d)) all execution actors directly follow commands

from the leader. The main difference between these organizations is in the responsibilities assigned to different commanders and accordingly in how the resources will be allocated to execute mission tasks and who will perform them. A communication structure will differ between these organizations, as the cell commanders would depend differently on one another and would have to jointly involve their respective resources for some operations.

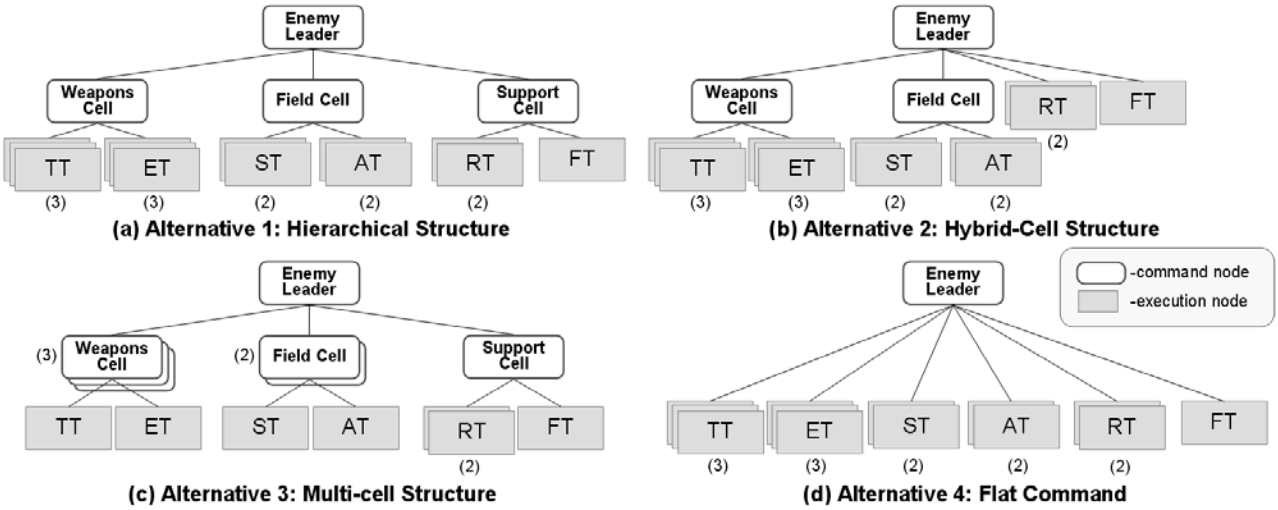


Figure 4: The Set of Hypothesized RED Organizations in BESTNET Use-case

Model specification and observable data

To identify who are hostile actors and what actions they execute, we quantitatively defined models of action and actor *profiles*. The action profile definition also enabled specification of observable action *signals* – i.e., the events that can be observed about the actor executing the action. For example, if the action is to store the weapons, its might require storage facility and possession of weapon materials. Only adversarial actors possessing such materials can conduct this action, and it can only be done at a facility with existing storage capacity. The match between profile of the actor and profile of the task then defines the utility of action to the enemy. On the other hand, this action may result in the events of loading materials from trucks to the facility. Adding this information to utility match helped determine the true occurrence of the action in the area and the actors involved.

To define how actors can hypothetically be associated with actions, we defined three classes of attributes:

- *attributes describing capabilities of actors:* this data is current before the start of enemy’s operations; data about facility capabilities be collected from analyzing imagery by automated or manual means (e.g., using radar scans and intelligence data about availability of resources at facilities); data about capabilities of human actors can be collected based on intelligence reports about them, where demographic information about their areas of operation can fill the data gaps.
- *attributes describing current events and actions performed by actors:* this information is dynamic and can be obtained from human collection teams, UAV data feeds, etc.
- *attributes describing previous actions of the actors:* this is historic information that could have been obtained from the past events in the area of interest.

Accordingly, we defined three types of observable events about adversary’s actors and actions:

- **Capabilities events**, which identified “*who can do what*” in the environment; for example, this data can include “individual X is a truck driver”, “building A has wide entrance and can be used as a storage facility”, etc.

- **Interactions events**, which define “*who is connected to/interacted with whom*”, where connections can be of several classes, e.g., financial transactions, information flow, materials exchange, command and synchronization of activities, etc.; for example, interactions can include communication transactions, such as “members of a militant wing engaged in a meeting with weapons suppliers at 11:35 am for 35 min to procure explosives”; financial transactions, such as “a report of a money transfer from accounts of political support groups to an organization of interest”; or geo-spatial link, such as “a member of potential terrorist cell has been seen at the same time in a village where IED attacks occurred”
- **Actions events**, which specifies “*who did/does what*”; for example, action events can include BLUE’s intel about individual and joint operations of adversaries, such as “BLUE team discovered a safe house and apprehended RED operatives attempting to manufacture weapons”, “trucks from company Z were used for transporting refugees”, etc.

Quantitative definition of actors and tasks

In our use-case, we defined actors and tasks based on the following capabilities and current event attributes:

- *Value (VAL):* indicates the significance in attacking a target for RED
- *Transportation (TRS):* indicates the resources/availability/event of transporting the materials/bomb
- *Storage (STR):* indicated ability and conduct of storing materials for extended time periods
- *Reconnaissance (REC):* indicates a capability to conduct recon missions by RED and the needs for task definition
- *Attack (ATK):* the capability acquired when bomb is manufactured
- *Money (MON):* availability of and outcome of financial transaction
- *Security (SEC):* defined the security of conducting hostile actions for RED operatives
- *Materials (MAT):* defined the availability of materials that could be used to manufacture the explosives
- *Technology (TEC):* indicated availability of technology to manufacture dirty bomb or need for/availability of knowledge of how the explosives is manufactured.

We defined the profile of actors (humans, groups, facilities) using capabilities and current events as attributes. When defining tasks (RED operations), we split attributes notionally into two vectors:

- *resource requirement* – what actors should possess to successfully conduct the operation; this vector is matched with the actor profile; and
- *target requirements* – what facilities should possess to support the operation; this vector is matched with the facility profile.

Figure 5 shows some examples of attributes that we have defined for actors and tasks in the use-case. We intentionally created tasks that had overlapping attributes, so that missing action observations could result in the confusion of associating these observations with more than one task. Based on the functions of buildings and areas, we have defined their capability vectors. The capabilities of actors have been defined based on their knowledge, skills, possessed resources, and roles in the enemy organization.

Observable data was extracted from capability, action, and interaction events, which had time, location, and individuals involved in the event. To explain how we defined action events in our use-case, we note that often multiple RED actors participate in the same operation due to the need to satisfy the resource requirements of tasks, while we assumed that a single facility/area is used to conduct an operation. When actors perform their portion of the operation, this is equivalent to them “applying” their capabilities to the task or target of the operation. For example, the task “*assemble bomb*” (AB, see Figure 5) requires three types of capabilities: materials, technology, and security protection. These capabilities can be brought together by explosives specialists (who possess technology capability) and support team (who possess materials and security). Thus, an observable action event is the detection of activity associated with using

these capabilities. The data of action events included the following fields: (i) *time* and geo-spatial *location* of event; (ii) *actor* involved in the event; and (iii) *capabilities* of actor *used* in the action.

	Resource Requirements									Target Requirements								
Tasks	VAL	TRS	STR	REC	ATK	MON	SEC	MAT	TEC	VAL	TRS	STR	REC	ATK	MON	SEC	MAT	TEC
SR	0	0	0	2	0	0	0	0	0	3	0	0	0	0	0	0	0	0
SP	0	0	0	1	1	0	2	0	0	1	0	0	0	0	0	0	0	0
SH	0	0	0	0	0	0	1	0	0	2	0	0	0	0	0	0	0	0
AMW	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	2	0
ATK	0	1	0	0	2	0	1	0	0	3	0	0	0	0	0	0	0	0
DC	0	0	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0
AB	0	0	0	0	0	0	1	1	1	0	0	1	0	0	0	3	0	2
SM	0	1	1	0	0	0	1	0	1	0	0	3	0	0	0	3	0	1

(a) RED Model Tasks/Activities

	Capabilities								
Actors	VAL	TRS	STR	REC	ATK	MON	SEC	MAT	TEC
RT	0	0	0	1	0	0	0	0	0
ET	0	0	0	0	0	0	0	0	1
TT	0	1	0	0	0	0	0	0	0
FT	0	0	0	0	0	1	0	0	0
ST	0	0	1	0	0	0	1	1	0
AT	0	0	0	0	1	0	1	0	0

(b) RED Model Actor Roles

	Capabilities								
Facilities	VAL	TRS	STR	REC	ATK	MON	SEC	MAT	TEC
BioLab	0	0	0	0	0	0	2	2	1
Mall	1	0	0	0	0	0	0	0	0
Airport	2	0	0	0	0	0	0	0	0
Park	0	0	0	0	0	0	2	0	0
Farm	0	0	3	0	0	0	3	1	1
Government	3	0	0	0	0	0	0	0	0
Temple	0	0	2	0	0	0	0	1	0
Oil/Gas Facilities	3	0	1	0	0	0	0	0	1
House of Worship	1	0	1	0	0	0	2	1	0
Military Administration	3	0	0	0	0	0	0	0	0
Single-family Home	0	0	1	0	0	0	2	1	0
Service/Refueling Station	2	0	1	0	0	0	1	0	1

(c) Observed Facilities

Figure 5: Example of Attributes of Actors and Tasks

Thus, for the example of “assemble bomb” operation, BLUE may detect action events describing the operatives of RED conducting security around the building, and actors who brought bomb making materials to the building, while the information about actors with technological bomb assembly knowledge might be missing. Therefore, the observed data might be incomplete, ambiguous, and noisy. Overall, BESTNET can deal with four types of data collection noise:

(1) Event miss: Events about the activities are captured by sensors (SIGINT, HUMINT, IMINT, …), and not all such events might be detectable. For example: *Facility was used to hold a meeting between terrorists, but there was no UAV/patrol at the time in the area*. As an outcome, all attributes from the missed event are excluded from analysis.
(2) Attributes miss: Sensors (humans, algorithms, …) might miss an attribute present in the incoming data/event. For example: *LIDAR data was incorrectly analyzed by the image classification algorithm.* As an outcome, correct attribute was missed and excluded from the analysis.
(3) Irrelevant Attributes/events: Sensors (humans, algorithms, …) might falsely perceive that an attribute was present in the incoming data/event or might falsely add an event due to deceptive information that has never occurred or irrelevant information wrongly associated with event. For example: *Analyst, based on studied imagery, reported a presence of hide-out at the construction site.* As an outcome, incorrect attribute is added as input and is used for analysis.
(4) Attributes errors: Sensors (humans, algorithms, …) might incorrectly assess the value of an attribute in the incoming data/event. For example: *Analyst, based on studied imagery, reported that the building had large footprint, while building had medium-to-small footprint.* As an outcome, incorrect attribute value is used as input for analysis.

The example in Figure 6 shows how the observed information about actors and facilities might get generated. We have developed the uncertainty layer component that takes the true data from the simulation and makes it noisy for the sensitivity analysis of algorithm accuracy versus different noise levels.

Hence, we extract the profiles of actors and facilities from event attribute vectors. Similar data can be collected about linkages between actors and facilities. For example, linkages between actors are related to actor interactions, and linkages between facilities are profiles from the activities on the roads between them. The profiles of actors and facilities are then organized in the form of a *data network* – an attributed graph where the nodes are actors/facilities and links are actor and facility interactions. The nodes and links are labeled with profiles in the form of observed attribute vectors.

(a) True Attribute Vector

	Capabilities									Current Events								
Facility	VAL	TRS	STR	REC	ATK	MON	SEC	MAT	TEC	VAL	TRS	STR	REC	ATK	MON	SEC	MAT	TEC
BioLab	0	0	0	0	0	0	2	2	1	0	1	1	0	0	1	0	0	0

Static pre-mission intel

Dynamics events/intel

	Capabilities									Current Events								
Facility	VAL	TRS	STR	REC	ATK	MON	SEC	MAT	TEC	VAL	TRS	STR	REC	ATK	MON	SEC	MAT	TEC
BioLab	1	0	0	0	0	0	1	2	0	0	1	0	0	0	1	0	0	0

Irrelevant attribute

Attribute error

Attribute miss

Event miss

(b) Observed Attribute Vector

Figure 6: Example of Observable Data Generation

Solution Details

BESTNET has four main adversarial reasoning components: *Behavior Prediction, Resource Support, C2 Simulation*, and *Criticality Assessment*. The algorithms for these components have been developed and validated by Aptima in our previous work, but required adaptations to BESTNET domain.

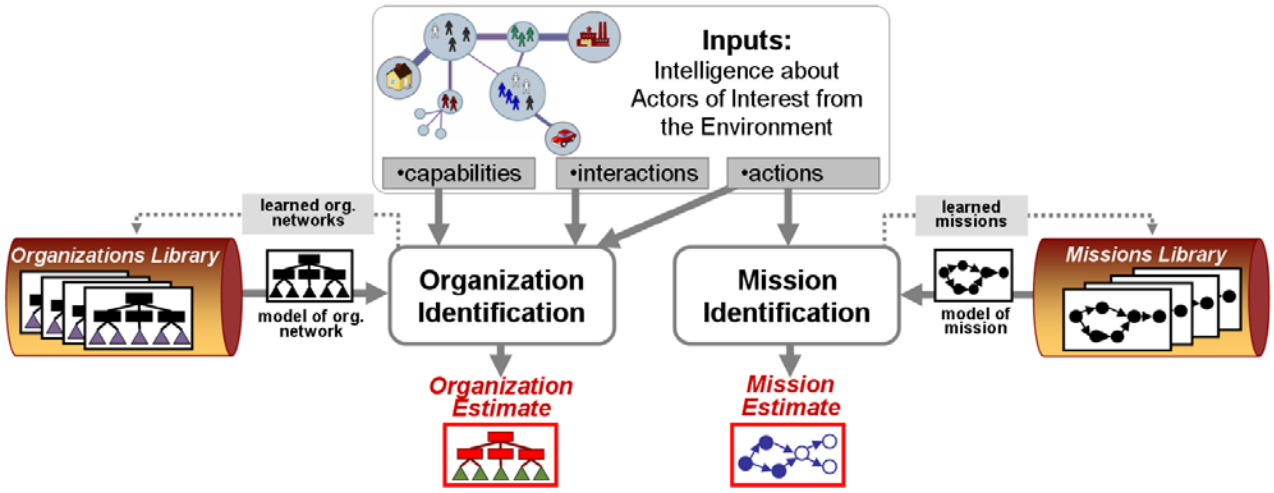


Figure 7: Behavior Identification in BESTNET

The **Behavior Prediction** model consists of two main algorithms: *RED organization identification* and *RED mission identification* (Figure 7; see (Levchuk et al., 2007, 2008) for detailed model descriptions). An **organization** is a group of people and physical resources (facilities, materials, equipment, financial, knowledge, etc.) intentionally brought together to accomplish an overall, common goal or a set of goals. Organizations can range in size from two people to tens of thousands. In BESTNET, we focused on identifying the *command and control (C2) organization* of the adversary, which manages personnel and resources in order to accomplish missions. Knowledge about C2 connections (e.g., command,

information, geo-spatial, resource use, etc.) between individuals in specific roles in a covert organization is needed to identify their involvement in the future operations and thus establish their criticality to the success of the adversaries. A **mission** is a collection of tasks that organizations (including adversaries) plan to perform to achieve desired objectives. A *task* is an activity that entails the use of relevant resources (provided by the organization), and is overseen by individual actors of organizations.

Estimates of RED organization and mission will filter out false observations and fill in information gaps, based on the correspondence between observed data and knowledge about potential organizational networks and mission plans of the adversaries. Hypothetical hostile organizational structures, stored in the organizations library, and potential adversarial missions, stored in the missions library, can be specified by analysts as hypotheses and/or learned over time from the data.

The **Resource Support** model is based on Aptima’s COA analysis tool, SCIPR (Greer et al., 2008). The SCIPR is an agent based model that was developed from social identity and influence theories. It receives the input from NetSTAR of the estimates of RED organization and mission, and combines them with information about current demographics. SCIPR model then develops forecasts of future adversary support for their missions (Figure 8) by evaluating the changes in the social environment that may make it more or less conducive to particular missions. This resource support may come in the form of new recruits or as a result of local attitudes. In the case of attitudes, the support may be more passive in that locals do not trust authorities or fear reprisal for providing information on insurgent activities.

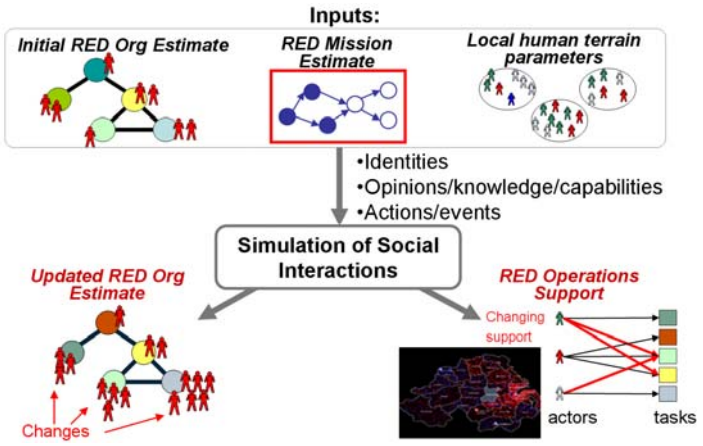


Figure 8: Resource Criticality Forecasting using Social Interaction Simulation

The **C2 Simulation** model is based on *resource-mission scheduling algorithms* to forecast when the mission tasks will be performed by the adversaries, and what alternative resources they might use. The scheduling algorithms are based on organizational performance simulation technology Aptima has developed (Levchuk et al., 2002; Levchuk et al., 2005; Lowell and Levchuk, 2006; Meirina et al., 2006). Our empirically validated algorithms for designing C2 structures and simulations for military human organizations have evolved into Aptima’s Models of Organizations, Systems and Technologies (MOST) tool. MOST is an interactive environment for analyzing the performance and designs of human organizations for specific missions or sets of missions. MOST scheduling algorithms employ heuristic resource-constrained task-to-agent scheduling, which incorporate normative models of synthetic agents and teams (Levchuk et al., 2002; Lowell and Levchuk, 2006; Levchuk et al., 2006). The synthetic agents utilize the design of priority rules to model human stochastic preferences for task selection and resource allocation. Individual task execution is modeled by accounting for human workload constraints and the impact of workload, experience, and learning on task execution accuracy. Team processes are modeled using agent interactions in the form of communication, including (i) decision/action, (ii) command, (iii) information request/transfer, and (iv) task execution synchronization. The organizational structures (information transfer and command responsibility) serve as a medium for this communication.

The **Criticality Assessment** model utilizes the inputs from C2 simulator to come up with criticality scores for RED actors (*who* can execute RED operations) as well as geo-spatial areas and facilities (*where* RED operations can be executed). To identify the critical resources in the adversarial organization, we need to compute the impact of disrupting or influencing a member of this organization

or places where they want to conduct operations on the operations and objectives of the adversaries. This impact calculation cannot be based on knowledge of the organization alone, as the same organization might have different bottlenecks and resource utilization when it conducts their missions differently. That is, since RED may change what actors are performing its operations and where operations may occur, BLUE wants to make sure that only least effective possibilities (if any) to perform its mission are left to the adversaries. In addition, since the data about the adversaries has large information gaps, we cannot rely on a single estimate of the enemy’s capabilities, organizational connections, and missions.

As the result, we use the outcomes of behavior prediction as the estimates of RED mission and organization and the outcomes of resource support analysis as forecasts of future support for RED activities in the area. These are then fed into C2 simulation to generate multiple possible policies (what to do, where, and by who) of RED executing its mission. The resulting mission schedules are then used to compute resource criticality scores (Figure 9).

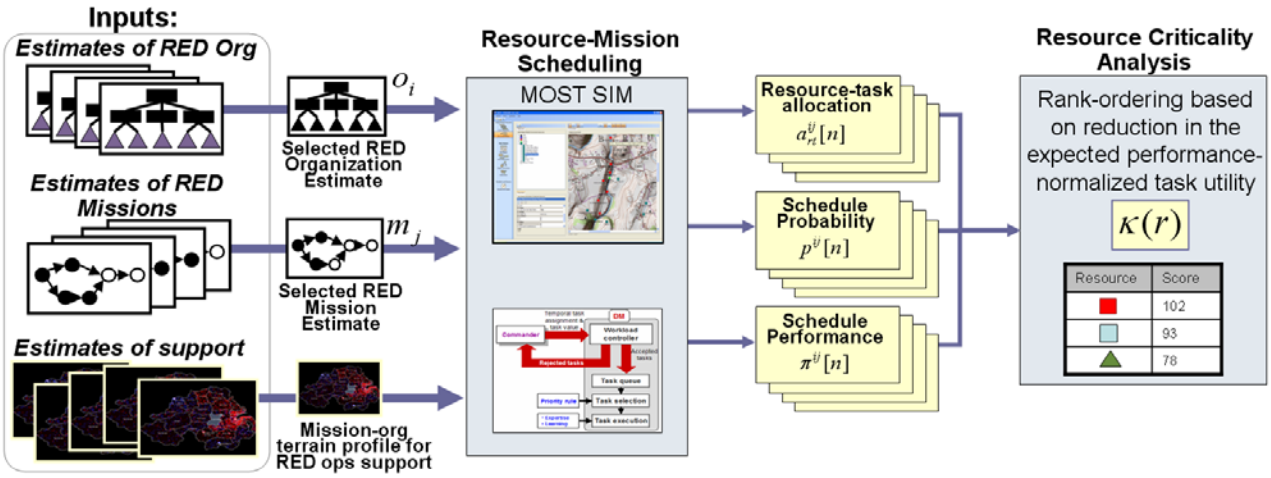


Figure 9: Resource Criticality Analysis Process

Formally, the input to the C2 simulation component is a set of most likely organizations $O = \{o_1,...,o_{|O|}\}$ and missions $M = \{m_1,...,m_{|M|}\}$, together with the probabilities of their occurrence p_i^O, p_j^M. From the mission identification step we also receive the estimate of the mission’s state $\hat{S}_j = \| s_t^j \|_{t \in m_j}$. Then, for each pair of organization and mission $< o_i, m_j >$, we conduct Monte-Carlo simulations to generate a set of predicted adversarial mission execution schedules using MOST scheduling algorithms. The mission input into MOST is a set of tasks $t \in m_j$, for which the estimated state is equal to $s_t^j = 0$ - i.e., the tasks which, according to the mission state estimate, have not been executed. The outcome of these simulations is a set of schedules and corresponding allocation of resources from the hypothesized organization o_i to the tasks of mission m_j. That is, for each task $t \in m_j$, we obtain a matrix $a_{rt}^{ij}[n], r \in o_i, t \in m_j$, which specifies the *allocation of resources to this task* ($a_{rt}^{ij}[n] = 1$ if the resource $r \in o_i$ is allocated to task $t \in m_j$ in the mission schedule n). During the simulation, we also calculate the *probability* $p^{ij}[n]$ that a mission execution schedule produced by schedule (Monte-Carlo run) n might occur in a real world situation. This probability is based on stochastic prioritization parameters of task and resource selection used in the MOST simulation. In addition, we calculate the *performance* score for each schedule $\pi^{ij}[n]$. Various metrics can be used to compose the performance score, including task accuracy and timeliness, temporal reward, safety of operations, resource utilization,

communication delays, etc. Currently, we use the *gain measure* (Levchuk et al., 2003) to calculate effectiveness of mission performance.

We calculate *criticality of a resource* r (where resource denotes RED actor or facility/area) as the **reduction in the expected performance-normalized task utility** for the adversaries:

$\kappa(r) = \sum_{ij} p_i^O p_j^M \sum_n p^{ij}[n] \frac{u_n^{ij}(r)}{\pi^{ij}[n]}$, where $u_n^{ij}(r)$ is the static resource utility loss of r to RED organization i executing mission j using schedule n. The expected value of the normalized utility provides an efficient rank-ordering between different adversarial resources. Calculation of task utility can be done based on the assumption that a task failure will entail the failure of all succeeding tasks in the RED mission.

To define RED’s mission performance score $\pi^{ij}[n]$ and resource utility $u_n^{ij}(r)$, we assumed in use-case that individual task values $v(t)$ are defined as reward to RED succeeding in task t, and used the *gain measure* (Levchuk et al., 2003) to calculate the performance score $\pi^{ij}[n] = \frac{1}{T}\sum_t \delta_n^{ij}(t) v(t)\left(T - s_n^{ij}(t)\right)$, where T is the end time of the RED mission, $\delta_n^{ij}(t) = 1$ if task t is successful (=0 otherwise), and $s_n^{ij}(t)$ is the start time of task t for schedule n. The gain measure allows to trade-off the timeliness of task execution and achieved value/reward (the larger it is, the faster is RED achieving the highest aggregated reward from task executions). We can then calculate the resource utility loss to RED as $u_n^{ij}(r) = \frac{1}{T}\sum_{t \in \Omega_n^{ij}(r)} \delta_n^{ij}(t) v(t)\left(T - s_n^{ij}(t)\right)$, where $\Omega_n^{ij}(r)$ is the set of tasks that involve resource r together with their successors.

The estimate of probability $p^{ij}[n]$ for schedule n of organization i executing mission j was computed using a softmax criterion $p^{ij}[n] = \frac{e^{\pi^{ij}[n]}}{\sum_m e^{\pi^{ij}[m]}}$.

Example of Identifying Critical Adversarial Resources

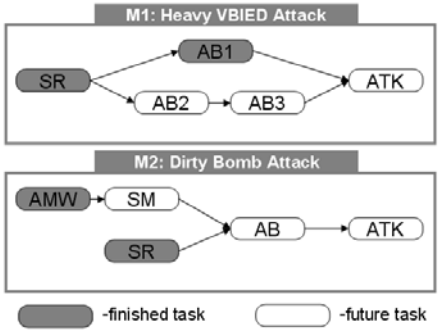
With described dataset, we have conducted three types of analysis:

- **RED behavior recognition:** We have used behavior recognition algorithms to identify RED mission structure and resource and actor networks (Levchuk and Chopra, 2005; Levchuk, Levchuk, and Pattipati, 2006; Levchuk et al., 2007, 2008). We have achieved over 70% accuracy for the data with large missing information (>50% missing events).
- **Forecasting resource support to RED operations:** The support forecasting algorithms used in BESTNET are based on an agent-based implementation of social identity and social influence theories (Grier, et al., 2008). We used a proportional representation of a region’s population to simulate the propagation of changes to opinions and identity affiliations in response to events and actions.
- **Assessing criticality of RED resources:** We developed forecasts of the future adversarial operations and involvement of hostile actors and resources. Using this knowledge, we have computed the criticality scores of RED resources (members of hostile organization and areas where RED may perform their actions) that have aligned well with the actual involvement of those resources in future hostile activities.

In this paper, we describe an example of criticality assessment process conducted with BESTNET. In Figure 10 we show example of predictions of RED organization and mission identification updated with resource/task support forecasts are shown. Two possible mission patterns have been identified (probability of mission M1 is 0.7 and probability of M2 is 0.3, see Figure 10(a)), and the states of these missions (which operations RED has completed and which ones it plans to do next) have been estimated (Figure 10(b)). Only a single organization (Alternative 4) has matched the observed data (Figure 10(c)). We will identify the critical resources of the RED organization in this situation. We constructed a set of simulations of future task execution by RED actors. In Figure 11, we illustrated examples of RED mission execution forecasts as Gantt-chart schedules for the predicted missions and organizations. These schedules all resulted in the same mission gain scores.

Mission	Probability
M1: Heavy VBIED Attack	.7
M2: Dirty Bomb Attack	.3
M3: Hostage Taking	0
M4: Contaminate Water Supply	0
M5: Site Attack and Mining	0

(a) Mission Predictions

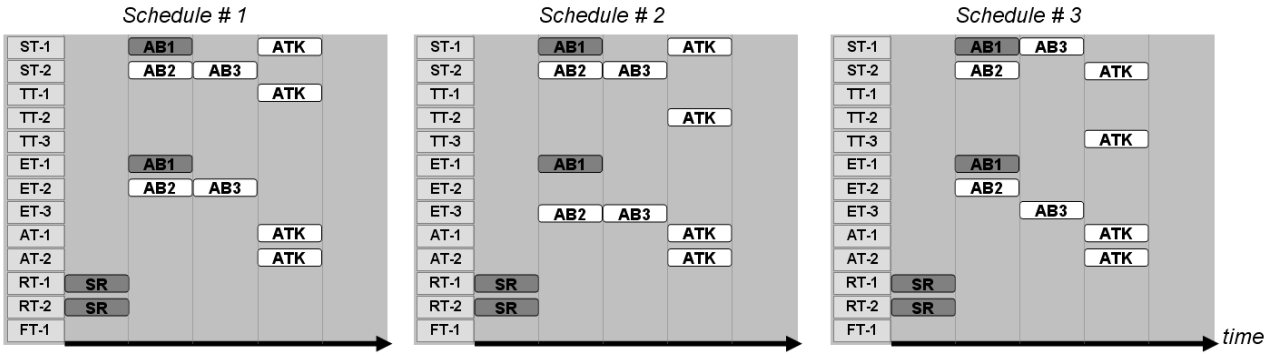


(b) Estimates of Mission State

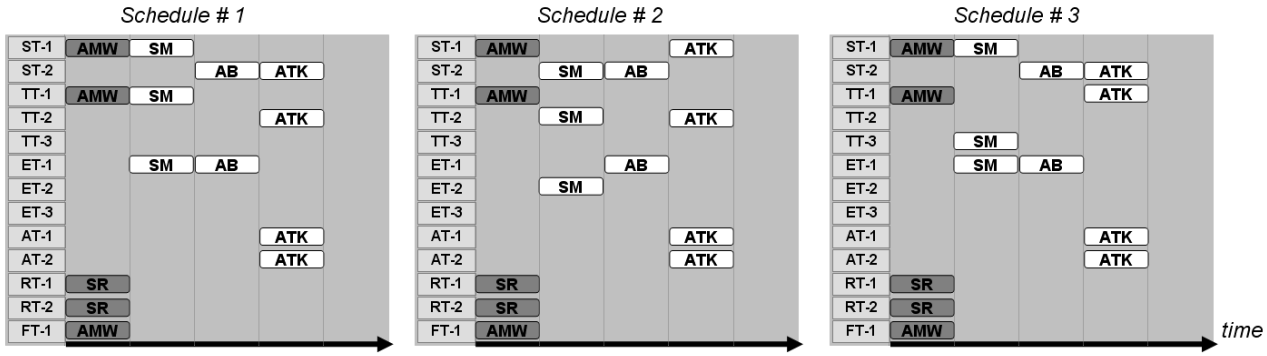
Mission	Probability
Alternative 1	0
Alternative 2	0
Alternative 3	0
Alternative 4	1

(c) Organization Predictions

Figure 10: Example of RED Predictions



(a) Alternative Schedules for Prediction 1: *Organization=4, Mission=M1*



(b) Alternative Schedules for Prediction 2: *Organization=4, Mission=M2*

Figure 11: Examples of Simulated RED Schedules for two Predictions from Dataset

	Resource utility loss for prediction 1			Normalized Expected Task	Resource utility loss for prediction 2			Normalized Expected Task	Total Normalized
Actors	Schedule # 1	Schedule # 2	Schedule # 3	Utility for Prediction 1	Schedule # 1	Schedule # 2	Schedule # 3	Utility for Prediction 2	Expected Task Utility
ST-2	6	6	1	0.333333333	3	6	3	0.285714286	0.319047619
ET-2	6	0	6	0.307692308	0	6	0	0.142857143	0.258241758
ST-1	1	1	6	0.205128205	6	1	6	0.30952381	0.236446886
ET-3	0	6	0	0.153846154	0	0	0	0	0.107692308
ET-1	0	0	0	0	6	3	6	0.357142857	0.107142857
AT-1	1	1	1	0.076923077	1	1	1	0.071428571	0.075274725
AT-2	1	1	1	0.076923077	1	1	1	0.071428571	0.075274725
TT-1	1	0	0	0.025641026	6	0	1	0.166666667	0.067948718
TT-2	0	1	0	0.025641026	1	6	0	0.166666667	0.067948718
TT-3	0	0	1	0.025641026	0	0	6	0.142857143	0.060805861
RT-1	0	0	0	0	0	0	0	0	0
RT-2	0	0	0	0	0	0	0	0	0
FT-1	0	0	0	0	0	0	0	0	0

Figure 12: Example of Resource Criticality Score Computation using Expected Normalized Task Utility

Figure 12 shows how the resource criticality score is computed based on computing task utility reduction for each forecasted schedule. The last column in Figure 12 shows the final criticality scores. We can see that the RED actor Support Team-2 scores the highest. We can also see that this result matches the fact that this team participates in all forecasted alternative mission execution policies for RED and is involved in early stages of its operations so that its disruption will degrade RED’s performance the most and thus would provide the highest benefit to BLUE. We conclude that BESTNET algorithms produce the resource criticality scores that meaningfully measure the forecasted involvement of RED actors and other environment resources in the future RED operations. Thus, BESTNET promises to provide a solid decision support capability to operations planners, intelligence collection, and analysts.

Conclusions and Future Research

In this paper, we have presented an approach that combines probabilistic identification technology with socio-cultural influence models and resource utilization forecasting models to generate the estimates of most critical actors of the adversarial organization. We have developed a synthetic dataset that resembles possible real-world scenario of adversarial activities. For this simulated scenario, as well as for other randomly generated behavior patterns, BESTNET achieved high accuracy in identifying the adversarial actors, their roles and organizational relationships, the mission they have been executing, and forecasting future support to hostile actions can change over time, actions adversaries may do, and actors who will participate in the future operations. BESTNET model produced the criticality scores of RED resources (members of hostile organization and areas where RED may perform their actions) that have been highly correlated with the actual involvement of those resources in future hostile activities. As the result, BESTNET products are reliable and traceable to the data and assumptions made by the models, and will enable the users of this tool to conduct a range of adversarial analyses and explorations of their own possible actions.

The solution outlined in this paper is a one-pass framework based on estimation, simulation, and forecasting algorithms. Our current research is focused on validating the criticality assessment in empirical studies and developing feedback mechanisms to make a close-loop iterative online solution for adversarial assessment. Future research will include development of algorithms for controlling and disrupting the adversarial mission and organization, and integrating these algorithms with recognition and forecasting methods.

Acknowledgement:

This work was supported by AFRL Contract # FA8750-08-C-0175. The authors would like to thank AFRL customers – Peter Rocci, RIED, and John Taylor, AFMC ESC/XR, for providing us with valuable feedback on the conceptual framework, simulated data generation, and results.

References:

Grande, D., G. Levchuk, W. Stacy, and M. Kruger, “Identification of Adversarial Activities: Profiling Latent Uses of Facilities from Structural Data and Real-time Intelligence”, *Proceedings of the 13th International Command and Control Research and Technology Symposium*, 2008.

Grier, R., Skarin, B., Lubyansky, A., & Wolpert, L. “Implementing the Cultural Dimension into a Command and Control System,” *Proceedings of GMU C4I Center-AFCEA Symposium*, 2008

Levchuk, G., Y. Levchuk, and K. Pattipati, “Identifying Command, Control and Communication Networks from Interactions and Activities Observations”, *Command and Control Research and Technology Symposium*, 2006, San Diego, CA.

Levchuk, G., Yu, F., Meirina, C., Singh, S., Levchuk, Y., Pattipati, K., Willett, P., & Kelton, K. (2007). Learning from the Enemy: Approaches to Identifying and Modeling the Hidden Enemy Organization. In A. Kott (Ed.). *Information warfare and organizational decision-making*. Norwood MA: Artech House.

Levchuk, G., D. Grande, K. Pattipati, Y. Levchuk, A. Kott ”Mission Plan Recognition: Developing Smart Automated Opposing Forces for Battlefield Simulations and Intelligence Analyses,” *Proceedings of the 13th International Command and Control Research and Technology Symposium*, June, 2008

Levchuk, G., D. Lea, and K. Pattipati, “Recognition of Coordinated Adversarial Behaviors from Multi-Source Information”, *Proceedings of SPIE Defense and Security Symposium*, Volume 6943, Orlando, FL, 2008