Title: **Identifying the Enemy – Part II: Algorithms versus Human Analysts**

Suggested Tracks:
Information Operations/Assurance, C2 Modeling and Simulation

Authors:

Elliot Entin
Aptima Inc.,
12 Gill Street, Suite 1400
Woburn, MA 01801
Phone: 781-935-3966
Fax: 781-935-4385
e-mail: entin@aptima.com

Rebecca Grier
Aptima Inc.,
1726 M Street, N.W., Suite 900
Washington, DC 20036
Phone: (202) 842-1548
Fax: (202) 842-2630
e-mail: rgrier@aptima.com

Tyrone Jefferson
Aptima Inc.,
1726 M Street, N.W., Suite 900
Washington, DC 20036
Phone: (202) 842-1548
Fax: (202) 842-2630
e-mail: tjefferson@aptima.com

Georgiy M. Levchuk
Aptima Inc.,
12 Gill Street, Suite 1400
Woburn, MA 01801
Phone: 781-935-3966
Fax: 781-935-4385
e-mail: georgiy@aptima.com

Correspondence:

Elliot Entin
Aptima Inc.,
12 Gill Street, Suite 1400
Woburn, MA 01801
Phone: 781-935-3966
Fax: 781-935-4385
e-mail: entin@aptima.com

Extended Abstract

Motivation:

To successfully predict the actions of the adversary, identify high-value targets, and develop effective counteractions, the knowledge of the enemy organization, objectives, and the modus operandi are needed. Current approaches to analyze the threat are manual: the intelligence analysts have to deal with huge amounts of data, most of which is irrelevant to the analysis performed. Large information gaps, including missing data, deceptions, and errors, have to be dealt with, and analysts often fill the gaps with their experiences which might not be applicable to the problem they need to solve, thus resulting in *decision biases*. In addition, people tend to exhibit *confirmatory biases* when the first seemingly valid hypothesis is selected and further relied upon during the analysis. This issue is compounded by huge amounts of data and complexity of the problem people need to analyze, influencing what data is used and which is filtered out and never studied. All these factors negatively impact the ability of the intelligence team to recognize acting enemy and further results in decreased efficiency of counteractions and unintended consequences.

Currently, only a limited set of tools are available to intelligence operators to analyze, correlate and visualize the data. No tools with automated threat prediction and assessment capabilities that can reason from multi-source data and support the decisions about the enemy's command and control organization have been developed. In the past this was due to the inability to bring all data sources together for common analysis. As new tools and data collection techniques become available, the feasibility of new technologies to automate threat prediction is increasing.

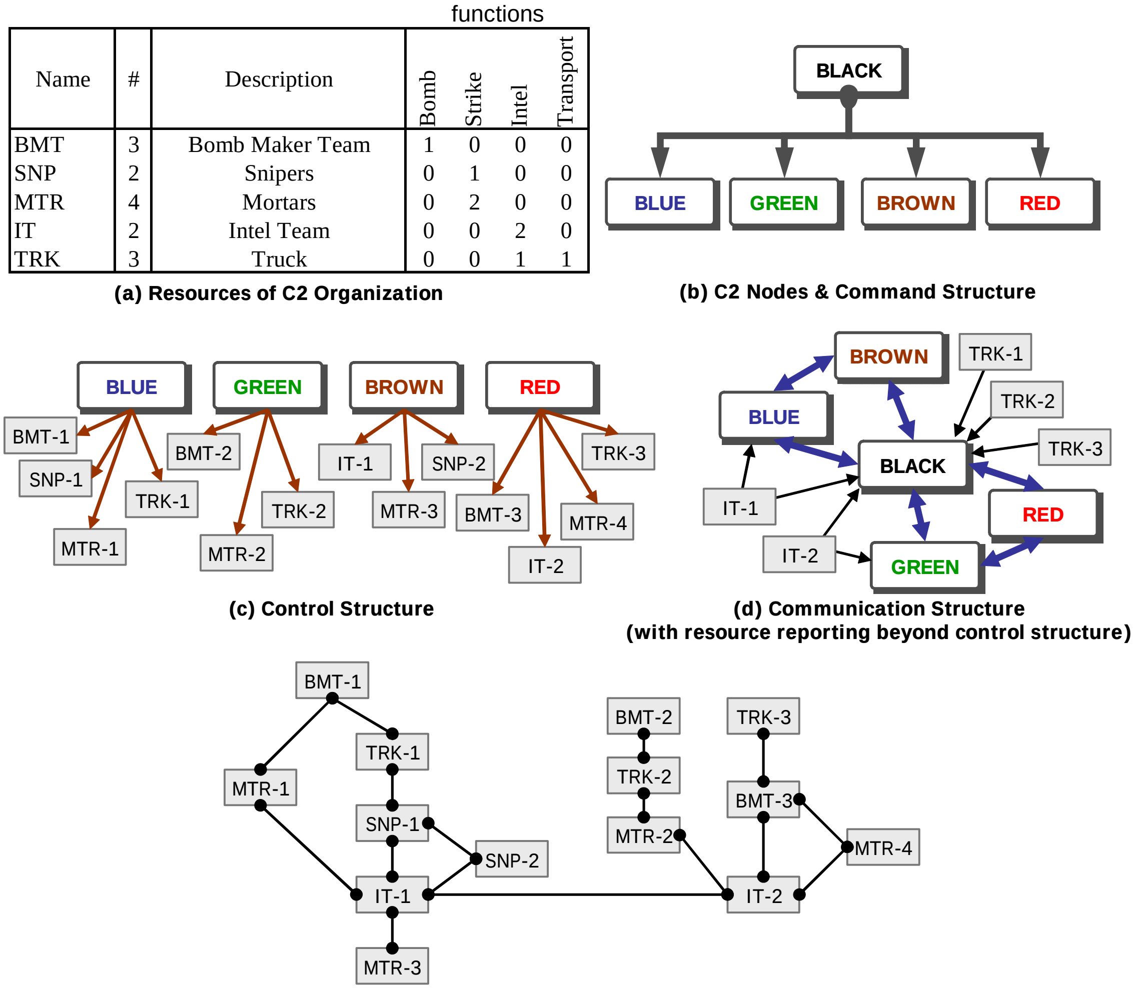
Problem:

This paper is part II of 2-paper submission describing a DARPA-sponsored project to develop and validate the NetSTAR technology for automated threat identification. In this paper, we describe how our identification of adversarial organizations stem from our analysis of command and control (C2) organizations and our analysis of what a model/algorithm must accomplish to identify and describe an adversarial organization. We then summarize the human table-top experimentation and concomitant comparison of the accuracy of adversarial organization discovery obtained by a team of human analysts versus the automated C2 identification process.

The threat analysis is based on understanding the decision-making processes in the general C2 organization. While C2 organizations are designed to manage personnel and resources to accomplish the mission requiring their collective skills. However, C2 organizations are not limited to one type of organization and such organizations are common to both friendly and adversary domains. Given specific functions and principles of individuals together with the structural form in which they are organized, a myriad of different potential organizations can be constructed. All of them are based on the underlying C2 principles. Moreover, organizational research findings indicate that there is no single "best" approach to (or philosophy of) command and control, thus many organizational constructs are possible.

C2 refers to procedures used to effectively organize and direct armed forces to accomplish a mission. The *command* function is oftentimes referred to as an art of an individual to set the initial conditions and providing the overall intent for mission execution. The *control* is referred to as those structures and processes devised by command to enable it and to manage risk and other entities in the organization. The commander in a C2 organization issues instructions to subordinates, makes suggestions to commanders of adjacent units, and makes requests from and reports to supporting units and superiors. He develops and maintains situational awareness of his area of operations through reports presented by other people or by electronic systems (Coakley, 1991). The basic premise of C2 organizations is the ability to distribute the responsibilities among its elements and coordinate these seemingly independent entities for joint operations to achieve objectives. The fundamental need for communications significantly constrains the options for C2 making the communications infrastructure a critical feature of a C2 system. However, describing the communications links and nodes of a fighting force does not suffice to explain, understand, or predict successes and failures in C2 organizations. We need to be able to represent, model, and identify the functions and objectives of the individual elements of the C2 organization.

As illustrated in Fig. 1 we describe a *C2 organization* as a collection of C2 nodes and resources connected via command, control, communication, and task structures. The roles, responsibilities, and relationships among C2 nodes and resources constrain how the organization is able to operate. **C2 nodes** are entities with information–processing, decision–making, and operational capabilities that can control the necessary units and resources to execute mission tasks, provided that such an execution does not violate the concomitant capability thresholds. C2 node can represent a single commander, liaison officer, system operator, or a command cell with its staff. A set of physical platforms and assets, C2 nodes, and/or personnel can be aggregated to form a **resource** (e.g., squad, platoon, weapons system, etc.). A resource is considered a physical asset of an organization that provides resource capabilities and is used to execute tasks. The level of aggregation depends on the problem at hand. For example, in cordon and search missions executed by a company–size forces, we can consider the squads as resources. The roles and responsibilities of the C2 nodes and resources identify possible operational and tactical policies: decisions they can make and actions they can perform.



			functions			
Name	#	Description	Bomb	Strike	Intel	Transport
BMT	3	Bomb Maker Team	1	0	0	0
SNP	2	Snipers	0	1	0	0
MTR	4	Mortars	0	2	0	0
IT	2	Intel Team	0	0	2	0
TRK	3	Truck	0	0	1	1

(a) Resources of C2 Organization

(b) C2 Nodes & Command Structure

(c) Control Structure

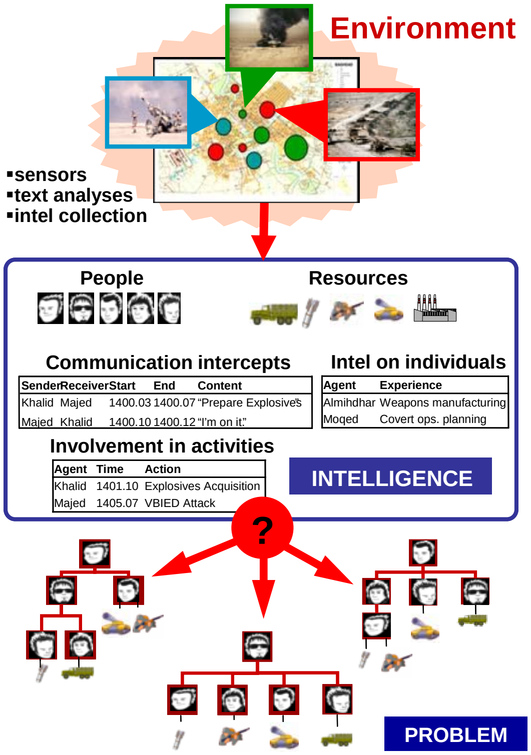
(d) Communication Structure (with resource reporting beyond control structure)

(e) Task Structure (example)

Figure 1: Example of C2 Organization

Command structure, represented as a network with directed links, defines superior–subordinate relationships among C2 nodes of the organization, thus specifying who can send commands to whom. **Communication structure** is a network between the decision makers of the organization, that defines “who can talk to whom”, the information flow in the C2 organization, the communication resources that decision-makers can use (communication channels), as well as the security of the communication channels. A **control structure** is an assignment of resources to C2 nodes, and specifies which commanders can send tasking orders to what assets. A **task structure** is a network among resources, where each link corresponds to operations jointly executed by these resources.

In Fig. 1 we depicted an example of an enemy command and control military team consisting of 5 command elements and 14 units/resources. The commanders of this organization make decisions to manage assigned resources in a cooperative manner to achieve team objectives. Commanders are executing mission tasks and prosecuting the desired targets via allocating their resources (military assets and weapons) and synchronizing their mission task execution and target engagements. Fig. 1.also describes the set of resources – military units and assets controlled by commanders. The assets include bomb making teams, sniper teams, mortar units, intelligence and reconnaissance teams, and trucks. This figure shows as well the *functional* or *resource capabilities* (Levchuk *et al*., 2002) of the units and resources in terms of bomb making, strike and small-arms attack, intelligence and monitoring, and transportation. The authority structure among the 5 commanders is a flat hierarchy (see Fig. 1.b) with a single commander (“BLACK”) being a main commanders of enemy forces. The assignment of assets and units to commanders (Fig. 1.c) determines the control structure of the C2 organization. Note that in the hypothetical example of Fig. 1 the main commander (“BLACK”) does not control any resources directly. The communication structure (who can talk to whom) of the organization is depicted in Fig. 1.d along with the direction of unit reporting observed events (information flow) beyond the control structure (we assume that units controlled by commanders also report their observations to these commanders). A partial task structure – a network between resources – is shown in Fig. 1.e. The task structure is due to the joint task execution by resources; therefore, it evolves throughout mission execution and depends on how the commanders manage their resources to assign and execute tasks.



Sender	Receiver	Start	End	Content
Khalid	Majed	1400.03	1400.07	“Prepare Explosives”
Majed	Khalid	1400.10	1400.12	“I’m on it.”

Agent	Experience
Almihdhar	Weapons manufacturing
Moqed	Covert ops. planning

Agent	Time	Action
Khalid	1401.10	Explosives Acquisition
Majed	1405.07	VBIED Attack

Figure 2: Organization detection problem

The meaning of organizational discovery is the ability to **recognize** the C2, communication, and task structures of the organization. However, the challenge is that most of the time we cannot observe the elements of the structures of the organization. Instead, we can obtain the intelligence due to the actions and activities of the organization. The specific actions depend on the structure of enemy C2 organization and are derived from the goals of the team. Before we outline our methodology to relate the observations to the structural elements, we discuss the structure of the observation data available from intelligence gathering sources.

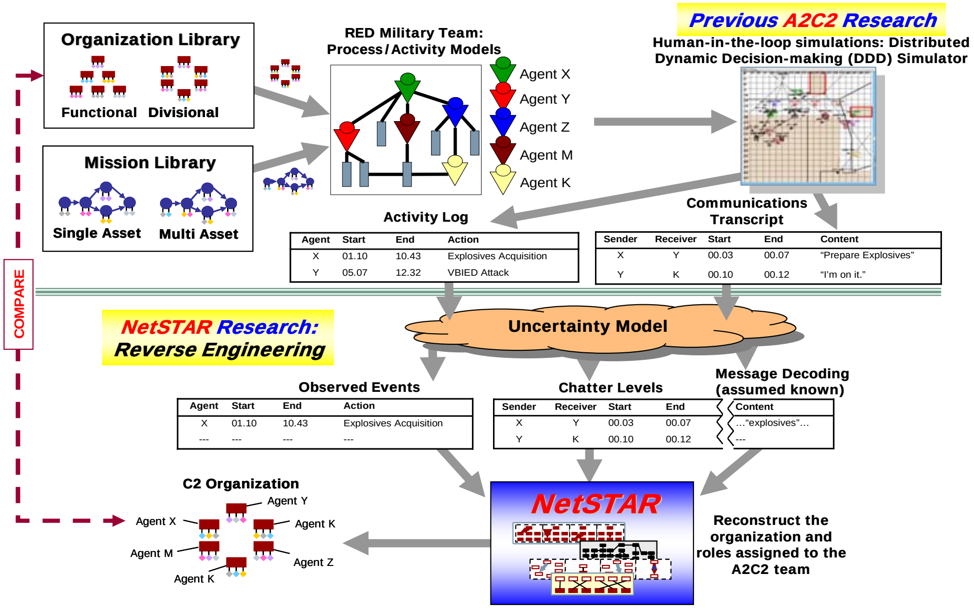
For threat analysis, we assume that the intelligence (observations, or data) given to us includes the set of tracked (monitored) individuals whose positions in the organization we need to determine, the resources of the enemy (including physical military, economic, and political resources), information about individuals (such as attributes of the individuals and resources – e.g., expertise of individuals, training, background, affiliation, family ties, roles and responsibilities, etc.), and information about transactions that involves these entities – communications among individuals (including some knowledge of its content), involvement in activities (such as individuals committing the same crime, or meeting among each other, or performing financial or business transactions, or using the resources in covert or open operations). The outcome of threat analysis is the prediction of the adversary's organization – that is, the roles and responsibilities of individuals, and their command, communication, control, and information networks (see Fig. 2).

Method:

Model

The NetSTAR system, a hybrid model-based structure and process identification methodology, was developed to automate the identification of the acting organizational networks and facilitate validation of network hypotheses developed by information operations analysts during adversary analyses (Levchuk et al., 2005, 2006). NetSTAR performs network state/pattern recognition from multi-source uncertain data based on probabilistic attributed graph matching principles. The outcome of this process is finding the mapping between nodes of the observed graph and library graphs and rank-orders the library graphs in terms of their likelihood (probability that the observed data was generated by the library network). The node mapping corresponds to finding the roles of the observed nodes (actors, individuals, cells, resources) and mapping the command, control, communication, information and task networks of the enemy organization.

The graph matching problem has many complicating aspects. First, there exist many mappings from individuals/actors to command nodes (there are N*M mappings from N actors to M command nodes). Second, we need to explore many different hypotheses about enemy organization – that is, many organizational structures. Third, even if the organization is known, we still need to determine what goals/mission it has, and how far along this organization is in finishing the mission. Other issues, such as transcribing the communications to identify the content, constructing feasible organization and mission representations, and determining the most efficient intervention strategies must be addressed.



Activity Log

Agent	Start	End	Action
X	01.10	10.43	Explosives Acquisition
Y	05.07	12.32	VBIED Attack

Communications Transcript

Sender	Receiver	Start	End	Content
X	Y	00.03	00.07	"Prepare Explosives"
Y	K	00.10	00.12	"I'm on it."

Observed Events

Agent	Start	End	Action
X	01.10	10.43	Explosives Acquisition
---	---	---	---

Chatter Levels

Sender	Receiver	Start	End
X	Y	00.03	00.07
Y	K	00.10	00.12

Message Decoding (assumed known)

Content
…"explosives"…

Figure 3: NetSTAR Project Workflow

The NetSTAR's automated C2 identification process is aimed at reducing the complexity of organizational discovery. This allows analysts to focus on information most essential for decision making and explore in detail only a limited number of most likely hypotheses. To assess the decision aids capability and evaluate whether the solutions produced can significantly increase capabilities to make inferences regarding enemy command structures and explore how discovered information can be used by friendly forces to disrupt adversarial activities.

Our evaluation method schematisized in Fig. 3 leverages many years of model-based human-in-loop (HIL) experimentation cycles executed for the Adaptive Architectures for Command and Control (A2C2) research program (Diedrich et al., 2003; Entin et al, 2003; Kleinman et al, 2003; and Levchuk et al, 2003). This work studied the ability to use models to develop optimized military organizational structures for different missions and to encourage organizational adaptation. The A2C2 program included iterative cycles of experimentation to evaluate and validate the modeling approaches. These experiments have been conducted using Distributed Dynamic Decisionmaking (DDD) virtual environment (Kleinman, Young, and Higgins, 1996). DDD is a distributed real-time simulation platform implementing a complex synthetic team task that includes many of the behaviors at the core of almost any C2 team: assessing the situation, planning response actions, gathering information, sharing and transferring information, allocating resources to accomplish tasks, coordinating actions, and sharing or transferring resources. Successive DDD generations have demonstrated the paradigm's flexibility in reflecting different domains and scenarios to study realistic and complex team decision-making. An outcome of A2C2 program that directly feeds our validation work has been the creation of DDD-based scenarios and organizational structures. The A2C2 experiments have catalogued a diverse set of outcomes from HIL runs for various teams, organizations, and mission conditions.

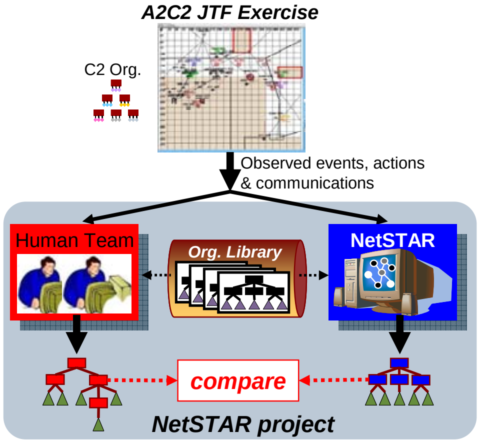


Figure 4: NetSTAR Validation

A HIL DDD run includes a team of participants playing roles of commanders in a predefined command and control team and performing the mission tasks in the DDD virtual environment using kinetic and non-kinetic assets/resources. Of particular interest to our validation work are A2C2 experiments with Joint Task Force (JTF) organizations, which explored the range of possibilities to assign the command and control relationships, resource ownership, and individual responsibilities among commanders. Under the A2C2 program, we have tested both traditional and non-traditional C2 structures, thus providing rich data for the validation experimentation. For each HIL run from an A2C2 experiment, the data logs have been captured which include task execution logs (who does what, where, and when) and the communication interactions among team players. The latter information has been coded into distinct categories corresponding to several types of formal and informal interactions in a C2 organization. This data was directly used by our validation process graphically outlined in Fig. 4 with the addition of the uncertainty model component that can take the task execution and communication logs from real experiment runs and make the data noisy – that is, introduce deceptive events (false alarms), create missing data (misdetection), and add noise and errors to other data elements. In the validation experiment, this noisy observation data is presented to both human analyst team and automated C2 identification model that must reconstruct the acting enemy C2 organization. The outcomes of human analyst team and automated identification model were then compared (see Fig. 4) to judge the benefits of the proposed automated NetSTAR process in both identification accuracy and time required to identify (or manpower needs).

Human Experiment

Participants - Nine two-person teams drawn from officers attending the Naval Postgraduate School served as subjects.

Independent variables and Design - Two independent variables were examined: organization type and fogging level (i.e., percentage of errors). Organization type was operationalized as varying organizational structures along a continuum, ranging from functional to divisional organizations. Following Diedrich et al. (2003) the functional organizational structure was organized such that each commander specialized in one or two aspects of a mission such as Strike or Air Warfare, where the specific assets controlled were distributed across multiple platforms (ships). In contrast, in the divisional organizational structure, each commander had control over a single multifunctional platform that was able to process a variety of functional tasks in a given location. An intermediate, or hybrid, organizational structure was a type of organization in which some commanders controlled assets functionally and other commanders comprising the team controlled assets divisionally. Stimuli data representing three types of organizations were presented to the participants: Functional, Divisional and a Hybrid. For the experiment, the hybrid organizational structure was derived from a divisional structure where four commander controlled assets divisionally and two controlled assets functionally.

The second independent variable, fogging level, referred to the amount of noise or error injected into the tables and illustrations describing an organizational structure. Using a specific algorithm three levels of fogging were produced: one with 10% noise or errors, one with 30% noise or errors, and one with 50% noise or errors.

Procedure - Teams came to the lab for 2 two-hour sessions. During each one hour trial, participants were provided one stimulus data set and 7 hypothesis organizational structures. An observer was assigned to watch a team, record which of the data sheets the team used, how they used these sheets, in addition to recording time stamps. When the team had selected a hypothesis organizational structure, the observer recorded the time (this was the working time dependent variable) and provided the Participant Response Form to collect the remaining dependent variables. Participants had 50 minutes to select the correct hypothesis organizational structure and get as far in the commander, leader, and asset mapping as possible. At the start of the trial, participants were told they had 45 minutes to select an organization. If they had not indicated a hypothesis organization by that time, the observer asked them to make their best guess and to begin filling out the mappings. Throughout the trial the amount of time left was indicated by the observer. After teams completed the first trial, the observed data set and participant response sheets were gathered. Participants were then provided a different observed data set and the process was repeated. During most sessions two or three teams were working in the lab simultaneously.

Results and Discussion:

In order to properly evaluate the NetSTAR process, we needed to answer the following two questions:

(1) Is it possible to judge the impact of *uncertainty* on the quality of the organization identification solution?

(2) Is it possible to judge the impact of *problem domain* and *complexity* on the quality of the organization identification solution?

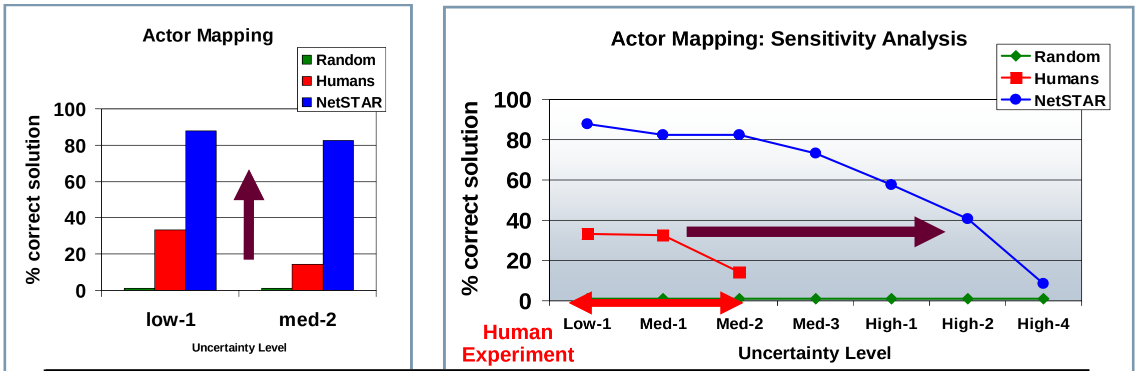
To address the first question, our study included exploring various levels of uncertainty and the corresponding parameters (probability of false alarm, misdetection, and errors). To address the second question, we conducted comparisons according to the type of organization that needs to be recognized. Different information is needed to recognize different types of organizations. In our pilot studies, we found that when the low-noise commander-to-subordinate intercepts can be obtained, a functional organization, where a single commander controls resources of the same type distinct from other commanders, is easier to recognize than a divisional organization, where each commander controls a variety of resources but thus has similar capabilities to other commanders. The divisional organization is more complex than the functional in terms of resource control, but can be easily recognized given the low-noise data of commanders' activity locations, since commanders' geographic responsibilities in divisional organization are distinct. Both functional and divisional organizations have elements that are encountered in today's command and control teams, and thus a study of such "hybrid" teams was essential to explore how difficult it is for human analysts to use multiple types of information for C2 discovery.

The NetSTAR project has showed that the automated threat identification algorithm outperformed unaided human analysts providing at least 2.5 times more accurate mapping between observed actors and their correct roles in the organization as depicted in Fig. 5. The NetSTAR algorithm also provided a robust solution being able to correctly identify 70% of actor-role mapping for 50% noise condition, whereas unaided human could only correctly map 12%.

Examining the human results some interesting findings came to light. It was noted that during the first experimental trial, all of the teams took the time to review most of the information presented to them (for both the hypothesized and observed stimuli data). After their initial experience, however, teams became increasingly less methodical and less thorough with each subsequent trial, to the point where teams would seek out and examine only one or two pieces of information that pertained to their observed organizational structure and then went about comparing these data to the hypothesized organizational structures. Once they had made a selection, as to which of the hypothesized organizational structure they thought was most similar to the observed data structure, teams would then attempt to determine the hierarchy for all of the Commanders, Platform Leaders, and Assets present in the data.

To elaborate, after their initial trial, teams developed a schema for how they would go about solving the problem. Schemas can be useful, as they "streamline" the processes of decision make in high workload complex situations. But, schemas are prone to a user's heuristics and biases because they tend to limit the type and amount of information decision makers attend to, thusly limiting or impairing decision quality. Frequently, human decision makers use schemas and heuristics to lessen their cognitive load and expedite task completion. The problem with this approach is that it can lead to particularly erroneous decisions, or lengthen decision time because insufficient information is present for users to make an informed choice.

An outcome of this heuristic strategy observed in our study is that after some teams selected a hypothesized organization structure, they seemed to disregard it and instead attempted to form their hierarchy mappings solely from the observed stimuli data. By relying on the stimuli data which is also noisy, this greatly increased their chances of making errors in their organizational mappings.



Uncertainty Level	Low-1	Med-1	Med-2	Med-3	High-1	High-2	High-4
% missing data	10	30	40	50	55	60	70
% deceptions/errors	10	20	30	30	30	35	45
SNR = true messages/deceptive messages	9	3.5	2	1.6666667	1.5	1.1428571	0.6666667

NetSTAR provides >2.5X better detection than human analysts under same uncertainty level

NetSTAR achieves same performance as human analysts under 3X uncertainty level

Figure 5: Sensitivity to Uncertainty and Comparison of NetSTAR Algorithm to Human Performance

(Random = results of random identification; NetSTAR = results of automated algorithm identification; Humans = results of threat identification by human analysts during table-top experiment)

Additionally, there were many instances when participants were observed only looking for information that supported the hypothesized organizations that they felt best matched the observed data. There were very few instances when teams sought to disprove their selection, and many examples of teams clearly ignoring or discounting information that suggested they had chosen the incorrect organizational structure. For example, participants would say that a piece of evidence that went against their hypothesis was just an example of an error in the data. This is an example of a heuristics bias called the *confirmation bias* - the tendency to search for or interpret information in a way that confirms one's preconceptions (Kahneman and Tversky, 1979).

Conclusion

In conclusion, the study demonstrated that human decision makers are capable of working with “noisy” observed data and discerning from a set of hypothesized organizational structures the organizational structure that produced the observed data, and to do so well above chance. We also observed the inherent limitations of human decision makers: decision biases, difficulty handling large data amounts, difficulty analyzing organizational networks with high network complexity. However the knowledge of how human operators performed data filtering and were able to abstract from limited set of data to sometimes come up with correct results was beneficial. We may be able to utilize similar data reduction strategies in the automated tool to improve our ability to scale the solution to real domain problems. Also, by studying the way intelligence analysts solve problems helps us develop NetSTAR-based threat assessment decision support tools that will be usable and trusted by the analysts.

References.

Coakley, T.P., (1991). *C3I: Issues of Command and Control*, Washington, D.C.: National Defense University, 1991, pp. 43–52.

Diedrich, F.J., Entin, E.E., Hutchins, S.G., Hocevar, S.P., Rubineau & MacMillan, J. (2003). When do organizations need to change (Part I)? Coping with incongruence. *Proceedings of the 2003 Command and Control Research and Technology Symposium*, Washington, DC.

Entin, E. E., Diedrich, F.J., Kleinman, D.L., Kemple, W.G., Hocevar, S.P., Rubineau, B., & MacMillan, J. (2003). When do organizations need to change (Part II)? Incongruence in action. *Proceedings of the 2003 Command and Control Research and Technology Symposium*, Washington, DC.

Entin, E. E., Weil, S.A., Kleinman, D.L., Hutchins, S.G., Hocevar, S.P., Kemple, W.G., Serfaty, D. (2004). Inducing Adaptation in Organizations: Concept and Experiment Design *Proceedings of the 2004 Command and Control Research and Technology Symposium,* San Diego, CA.

Kahneman, D. and Tversky, A (1979). 'Prospect Theory: An Analysis of Decision Under Risk'. *Econometrica*, 47 263-291.

Kleinman, D.L, Levchuk, G.M, Hutchins, S.G., and Kemple W.G., (2003). "Scenario Design for the Empirical Testing of Organizational Congruence", *Proceedings of the 2003 International Command and Control Research and Technology Symposium*, Washington, DC, June.

Kleinman, D.L., Young, P., and Higgins, G.S., (1996). "The DDD-III: A Tool for Empirical Research in Adaptive Organizations", *Proceedings of the 1996 Command and Control Research and Technology Symposium*, Monterey, CA, June.

Levchuk, G.M and Chopra K., (2005). "NetSTAR: Identification of Network Structure, Tasks, Activities, and Roles from Communications", *Proceedings of the 10th International Command and Control Research and Technology Symposium,* McLean, VA, June.

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

Levchuk, G.M., Levchuk, Y.N., Luo, J., Pattipati, K.R., and Kleinman, D.L., (2002). "Normative Design of Organizations - Part I: Mission Planning", *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, Vol. 32, No. 3, May, pp. 346-359.