14th International Command & Control Research and Technology Symposium
C2 and Agility

Using Simulation as a Knowledge Discovery Tool in an Adversary C2 Network

Topic 6: Modeling and Simulation

Authors

Celestine A. Ntuen [1], O.A. Alabi[1,] Y. Seong[1] , and E. H. Park[1]
[1]Army Center for Human-Centric Command & Control Decision Making
Center for Human-Machine Studies
419 McNair Hall
North Carolina A&T State University
Greensboro, NC 27411

Point of Contact

Celestine A. Ntuen
Army Center for Human-Centric Command & Control Decision Making
The Institute for Human-Machine Studies
419 McNair Hall
North Carolina A&T State University
Greensboro, NC 27411
Phone: (+1) 336-334-7780; Fax: (+1) 336-334-7729
Email: Ntuen@ncat.edu

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Using Simulation as a Knowledge Discovery Tool in an Adversary C2 Network	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Center for Human-Centric Command & Control Decision Making,North Carolina A&T State University,419 McNair Hall,Greensboro,NC,27411**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
In Proceedings of the 14th International Command and Control Research and Technology Symposium (ICCRTS) was held Jun 15-17, 2009, in Washington, DC

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**52**	

Using Simulation as a Knowledge Discovery Tool in an Adversary C2 Network

Abstract

This paper discusses a discrete-event simulation model of an adversary social network using Micro Saint Simulation software. The purpose is for knowledge discovery from the many interactions and relationships among and between the adversary players in the Iraqi conflicts, especially on the attack targets, weapons used, and the motives of attack. The model developed to solve the problem is an Adversary Network Simulation (ANS). ANS is a rule-based driven simulation that reasons from the strategic rules used by the adversaries. The ANS results provide important information in understanding the adversary behaviors in terms of selecting targets for attacks and the methods used in the attacks. The results show that coalition forces were targeted 68% of the time, Police stations 12.8%, mosques, 10.2%, malls and markets; 5.5%, and other public places, 3.2%. Most of the attacks to the coalition forces were from Al-Zawahari army, al-Qaida, Islamic Fundamentals, and Foreign agents. It was also revealed that ethic fighting sponsored by rogue politicians led to attacks on the mosques.

1. Introduction

Military commanders in the most recent and continuing conflicts of fighting war against terrorism and insurgents are overburdened with conflicting command and control (C2) functions that searching for the real adversaries, their strategies and tactics, motives, and their sponsors is problematic. Nations at wars are often orchestrated by many reasons that may include ethnic conflicts, political wills, religious differences, and other socio-cultural causes. In addition, these wars occur in the urban and cosmopolitan corridors making the tractability of the adversaries difficult. Simply, it is not a force-on-force war of strength; it is a war of will, deception, concealment, and use of nontraditional strategies and weapons. The war scenario is often characterized the juxtapositions of cultural behaviors with social forces. Heightened by the ubiquity of complex network of information and communication technologies, the description of the battlefield remains vague and the enemy unknown; however, both the adversary and the friendly forces are likely to have the same access to information technology as a weapon of war. In fact modern wars and their battlefields have been described as “wicked”, “complex”, and “chaotic.”(Yolles, 2006).

An example of the above scenario is the current conflict in Iraq. Here, for the past ten years, both the civilian populations, coalition forces led by United States of America (USA) and sometimes unknown enemies are subject to myriads and different types of daily attacks. These attacks include, but are not limited to kidnapping, suicide bombing, improvised electronic device (IED) and mortars. Obviously, the commanders of the coalition forces have interests to know who the real adversaries are, their motives, strategies on the use of attack weapons, and the sources of financial supports. The answers to these concerns remain the necessity to monitor, control, regulate and influence the battlefield outcomes so as to shift the advantages of the conflicts to the friendly Iraqi and coalition forces. Many modeling techniques are required to help analyze these situations.

Unfortunately, the use of the classical deliberate military decision making and planning models to study the problem is inadequate for at least two reasons: (1) deliberate decision making models assume rational normative axioms with known states of nature; this is not the case when the adversaries are not known and hence difficult to guess any states of nature; and (2) deliberate decision making models are suitable to systems with cause-effect (input-output) descriptions (Taber, 1994). In these types of systems, at least, some information are known a priori; and, the unknown information are often assumed to follow some known probability distributions where the system is intentionally allowed to partially behave in uncertain modes. In the battlefield information described for the modern conflicts, the system behaviors are chaotic and the best known way to characterize the system is derived from the science of complex and adaptive systems (Adams and Ntuen, 2008).

In spite of the shortfalls in the deliberate decision making models and their analytical derivatives, there have been relentless efforts to model battlefield behaviors both descriptively and prescriptively. The reason is obvious: in order for the coalition forces (hereby referred to as blue force) to gain a decisive edge over the adversaries, the reliance on analytical predictive models cannot be ignored. It is therefore surmised that the collection and analysis of battlefield information will support the commanders to understand the evolving adversary dynamic behaviors. In this respect and similar to Wiig's (1993) concept, battlefield information can be organized to characterize a particular situation so as to derive a set of truths and beliefs, perspectives, judgments, expectations, and insights. The uses of constructive simulation models are the most favorite ways to study complex and chaotic systems such as modern battlefield environment. From the commander's perspective, simulation will in general provide some expected views on how to transform information into meaningful situation assessment and understanding. This understanding is the center of gravity of actionable knowledge in context of evolving actions and their probable consequences. The result of simulation modeling also allows the decision makers to make anticipative inferences which when combined with experiences and expertise can allow a partial visualization of causal relationships not previously known.

2. Anecdotal Past Studies

Heuer (1999) notes that gaining the edge over an adversary now relies more on the analytical, predictive and cognitive abilities that can be brought to bear on the analysis of information. He also notes the challenges of model representation that may include such cognitive issues as:

• The mind is poorly "wired" to deal effectively with many forms of uncertainty that surround complex, indeterminate intelligence issues and the "fog" associated with denial and deception operations;

• Increased awareness of cognitive and other "unmotivated" biases, such as the tendency to see information confirming an already-held judgment more vividly than one sees "disconfirming" information, does little by itself to help analysts deal effectively with uncertainty;

• Tools and techniques that gear the analyst's mind to apply higher levels of critical thinking can substantially improve analysis on complex issues for which information is incomplete, ambiguous, contradictory, and often deliberately

distorted. Key examples of such intellectual devices include techniques for structuring information, challenging assumptions, and exploring alternative interpretations.

To understand the dynamics and interactions of multivariate and multifaceted information in the battlefield, social network theories have surfaced as the most flexible modeling approach. Social network analysis can be regarded as a tool, a theory, or a method that helps to explain interrelationships between actors in a system, such as individuals, groups, team members, organizations, and countries (Perez & Kedia, 2002). The actors in a social network analysis (SNA) consist of different entities with clearly defined characteristics that can be shared between and among the entities as individuals or groups within the network structure. SNA is usually used to predict similarity between attitudes and behaviors (Burt, 1992). Moreover, network analysis can be used to understand the flow of personal influence and power an individual or groups in a social system (Valente, 1995).

From the many paradigms of social network theory, it is observed that a network analysis can focus on four elements: the characteristics of the network (i.e., characteristics with respect to the form versus the relationships), the types of actors in the network (i.e., central versus peripheral positions and active versus passive roles), the scope of the network (i.e., international versus domestic networks), and the type of diffusion network (e.g., structural equivalence versus cohesive ways to diffuse information in the network). Many social network analyses and simulation adopt this philosophy. Some examples are: (a) WESTT (Workload, Error, Situational Awareness, Time and Teamwork) which is a software tool developed for visualizing, measuring and modeling C2 and team activity (Houghton et al, 2005); (b) Senturion, a simulation model that analyzes the political dynamics within local, domestic, and international contexts and predicts how the policy positions of competing interests will evolve over time (Abdollahian & Alsharabati, 2003); and (c) Dynamic network analysis (DNA) which is centered on the collection, analysis, understanding and prediction of dynamic relations and the impact of such dynamics on individual and group behavior(Carley, 2003).

3. Theoretical Representation

Consider a situation in Iraq. A set of targets has been attacked. These targets may consist be a mosque, kidnapping, a social gathering, market place, or a political building. The intelligent analysts (IAs) will have to determine the adversary groups responsible for the attack. There are many possible suspects: Al-Qaeda, Al-Sadi Militia, Islamic radicals, Rogue Politicians, and Foreign mercenaries. In addition, the IAs will have to determine the likely motives, for example, unemployment, dissent of foreign incursion and occupation, ethnic conflicts, and so on. There may be a need to know the organizations that support the adversaries financially. This is known as a knowledge discovery (KD) problem whose information can be represented in the form of a network because of the characteristics of the adversaries and the common activities they are engaged. Figure 1 is a hypothetical adversary network representation used to depict the above scenario.

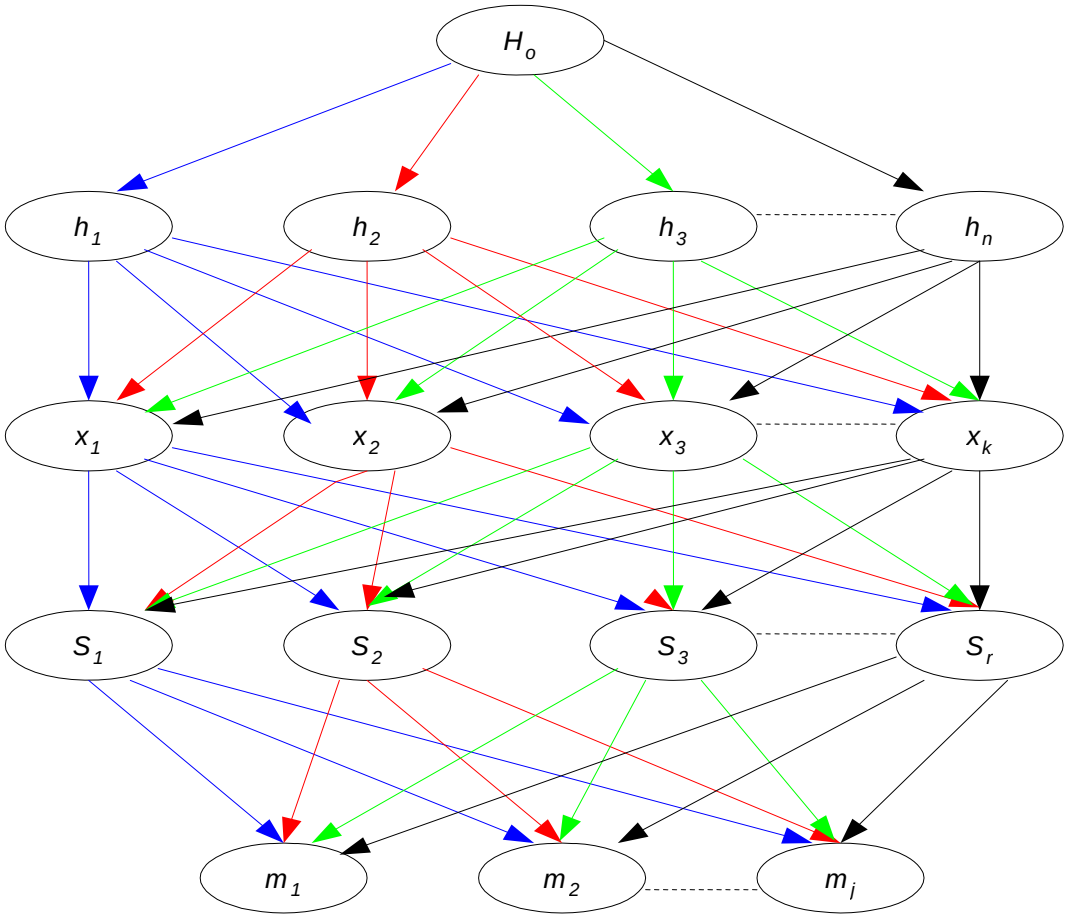


Figure 1. An example adversary network information representation

In Figure 1, the topmost node, H_o represents a space of composite hypotheses that maps a vector of likely targets to be attacked to a vector of adversaries. The variable h_i is a subset of H_o and may represent hypothesized lists of the adversaries involved in a given attack. The variables X_i may represent a perceived motive vector for the operation focus, while S_i may represent the influence path such as people or nations providing financial and weapon support to the adversaries).

From modeling and simulation (M&S) perspective, the interests of the Intelligent Analyst community may be one or all of the following:

a. What are the most likely targets by the adversaries?
b. What are the risks associated with these targets?
c. Which adversary tends to show dominant behaviors?
d. What are the common motives of the adversaries?

ANS predictive modeling is designed to provide answers to the above speculative questions that are of interests to the command decision making. ANS is an evolution from the sense making simulation model developed earlier (Ntuen and Alabi, 2006).

ANS can also determine the types of actors in the network and the power structure through influence metrics. ANS use the relationship between the centralities of all nodes to reveal much about the overall network structure (Krebs, 2003), such as: (1) who do adversaries seek information and knowledge from; (2) who do they share their information and knowledge with; (3) who is financing them; (4) how do they select targets for attack; and (5) why use the weapons such as IED on different instances and kidnapping in another? These kinds of information can enable the commanders to visualize and understand the many relationships that can either facilitate or impede knowledge creation and sharing in the battlespace.

4. ANS Implementation with Micro Saint

Micro Saint is a network-based simulation language developed from knowledge of human performance and cognitive information processing. It is a task network modeling, in which activities are represented in a diagram as nodes, and the arrows between the nodes represent the sequence in which the activities are performed (Hood, Laughery, and Dahl, 1993). Each activity, whether it is a human activity or a system activity, is defined using the same method. This minimizes the complexity of the user interface and eliminates the need for programming blocks specific to an application. Figure 2 shows a generic task network representation by Micro Saint for ANS. Although the identifier "task" has connotations of human activity, it is not restricted to such.

Tasks represent the lowest level in the model have specific parameters (timing information, conditions for execution, beginning and ending effects). Thus, in order to

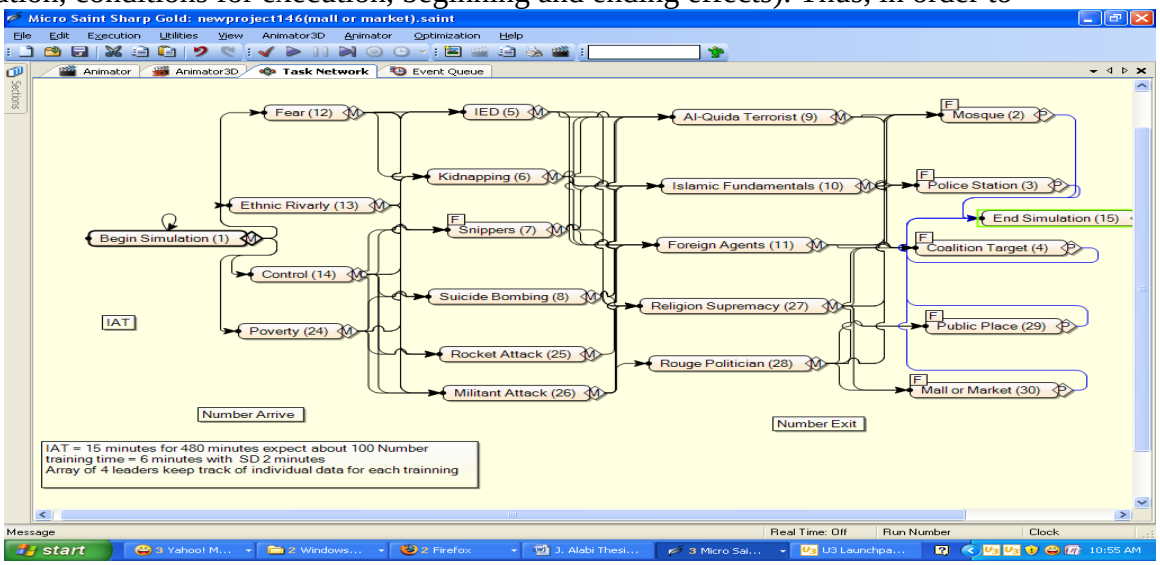


Figure 2. The Micro Saint networks for ANA

use Micro Saint, the system of interest must be decomposed into a network of relational hierarchies, with tagged conditions for triggering events, states, or activities. Micro Saint

uses a standard window "point and click" approach to define the network objects. Users must enter the conditions that control the branching when there is more than one following task. Micro Saint provides the following decision types to ensure that all real-world situations may be represented in the model:

Probabilistic – The following task conditions are evaluated and the next tasks to execute are determined by the relative probabilities of all tasks listed. Probabilistic decisions allow only one of the following tasks to execute.

Multiple – The following task conditions are evaluated and all of the tasks whose conditions evaluate to nonzero will execute.

Tactical – The following task conditions are evaluated and the next task to execute is the task whose condition evaluates to the highest value.

5. Performance Evaluation

The simulation begins with an appropriate network representation and parameter definitions as shown in Figure 2. The simulation chooses one or more targets to be attacked. The target information uses the Target Selection Rules (TSR) to map the information from Attack Resource Rules (ARR). Here, the model selects the types of weapons, e.g., IED, Kidnapping, Suicide Bombing, or a Sniper attack. The type of weapon is then associated with the adversaries such as Al-Qaida, Islamic–Fundamentalist, militants, and so on. Following this, the model attempts to map the adversaries to the sponsors using the derived matrix multiplication rules. The performance evaluation of ANS uses heuristic-based rule and assumptions that attempt to replicate the adversary intents and behaviors. The rules are:

1. **Adversary Relationship Rules (ARR)**
   a. Equally weighted adversary power (defined in terms of a reward sharing behavior) with equal probability assignment.
   b. Unequal adversary power using random probability assignment.
2. **Target Selection Rules (TSR)**
   a. Targets with the most human casualties.
   b. Targets with the most cultural and religious values (e.g. holy mosques)
   c. Targets with the most political values (e.g. ethnic killings and kidnappings)
   d. Targets with the most military significant (e.g. coalition forces)
   e. Targets with most economic values (e.g. oil wells)
3. **Attack Resource Rules (ARER)**
   a. Use the most available weapon (select at random)
   b. Use the cheapest weapon with the likelihood of more effect; high priority e.g. IED, and so on.
   c. Use weapon of mass destruction (low priority in this model)
4. **Motive Selection Rules (MSR)**
   a. Disgrace of foreign coalition troops
   b. Distortion and blackmail for economic gain
   c. Unemployment

d. Religious sentiment
e. Neighbor influence to control religion
f. Ethnic influence to control political power

In the simulation, resources represent anything that has a restricted capacity. Resources are represented by terrorism sponsors: Al-Qaida, Al-Zawahari army, Party of God, and so on. Another class of resource is the attack method. For example, an attack can be realized by the use of IED, kidnapping, or suicide bombing. The capacities of these resources are assumed to be infinite and their selection rules are probabilistic.

A single or multiple events can occur in the network. Thus, any attack is considered an event. An event is assumed to change the behavior of one or several entities in the simulation. For instance, a suicide bombing of a mosque or market place can lead to a change of state of the world which the entities exist.

The mental model of Figure 1 is converted into information network flows with multiple decision nodes and branches by Micro Saint Software. According to Micro Saint Software tool, in other to simulate task execution times as realistically as possible, Micro Saint randomly generates the execution times for each task using a probability distribution. When a time distribution for a task is selected, Micro Saint uses the distribution to generate random execution times that occur in the pattern predicted by the distribution. A probability distribution defines how frequently a particular value is likely to occur in a set of observations. Micro Saint provides twenty basic and advanced probability distributions for your use.

6. Simulation Results

6.1 Variance Reduction Simulation Trials

Warm up conditions were initiated by simulating the network without any rule using the traditional network information flow in Micro Saint with the input data randomly initialized. Ten different simulation experiments were conducted and the average results calculated on daily event basis (1440 minutes). The dependent variable was the number of deaths inflicted on the network by the adversaries using the available methods of attacks. The experiments were performed to reduce variations and to determine the best number of runs to minimize result variations and obtain stability. Table 1 shows one of the several matrixes used in the variance reduction study.

6.2 Discovering Relationships

Knowledge discovery (KD) in a network of complex battlespace of asymmetric adversaries is important to the commander and the battle staffs. KD is defined by Fayyad, Piatetsky-Shapiro, and Smyth (1996) as ``the non-trivial extraction of implicit, unknown, and potentially useful information from data.” Under computational conventions, the knowledge discovery process takes the raw results from data mining (the process of extracting trends or patterns from data) and carefully and accurately transforms them into useful and understandable information. This information is not typically retrievable by standard techniques but is uncovered through the use of simulation and artificial intelligence techniques. While machine discovery relies solely on an autonomous approach to information discovery, KD typically combines automated approaches with

human interaction to assure accurate, useful, and understandable results. For an instance, to the human, understanding a situation means that we have a grasp of the relevance knowledge spectra about the situation for decisions and actions (Ntuen, 2009).

Table 1: An Example of Targets Attack with Association to Sponsors

SPONSORS\TARGET	MOSQUE	POLICE STATION	COALITION FORCES	PUBLIC PLACES	MALL ATTACK
AL ZAWAHARI ARMY	**0.4**	**0.05**	**0.25**	**0.05**	**0.05**
FOREIGN ARMY	**0.15**	**0.25**	**0.15**	**0.25**	**0.25**
ROUGE POLITICIAN	**0.05**	**0.05**	**0.05**	**0.05**	**0.05**
ISLAMIC FUNDAMENTALIST	**0.25**	**0.3**	**0.15**	**0.3**	**0.3**
AL QUIDA	**0.15**	**0.35**	**0.4**	**0.35**	**0.35**

For knowledge discovery using the simulations results, cluster and correlation analyses were used to discover the relationships in the ANS. Figure 3 below shows the superimposed cluster tree obtained. In the upper part, foreign agents and politicians share the same distance and can be reasoned that the foreign agents are paid for or invited by the rogue agents. The correlation between the politicians and foreign agents using the profile

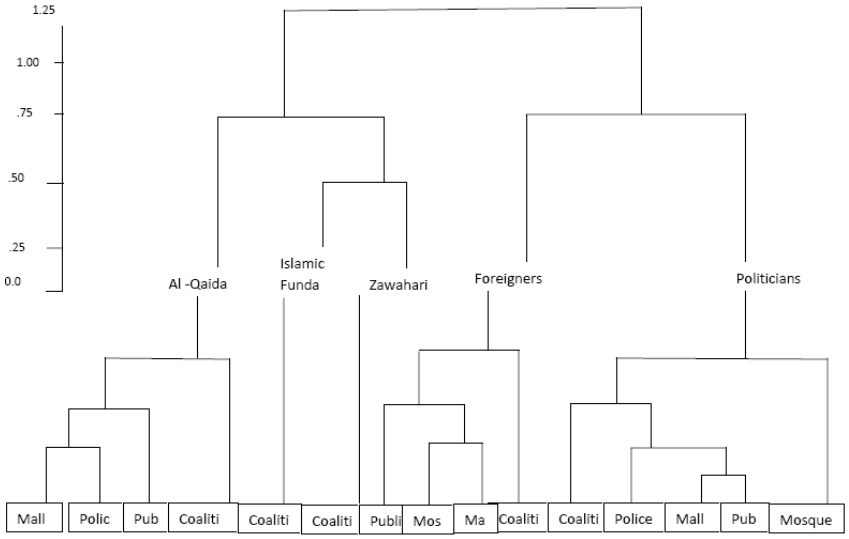


Figure 3. A hierarchical cluster tree of the sponsors and targets.

of attacks was 0.68 (p = 0.003). The part of the diagram on the left side shows that Al-Qaida, Islamic Fundamentals, and Al-Zahwari Army belong to the same cluster with the following correlation values: Al-Qaida and Islamic Fundamentals, 0.83 (p = 0.001), Al-Qaida and Al-Zahwari Army, -0.745 (p = 0.018), and Islamic Fundamentals and Al-Zahwari Army, 0.61 (p = 0.003). From the relationships, Al-Qaida, Islamic Fundamentals and Islamic Fundamentals and Al-Zahwari Army are close by their religious philosophy; Al-Qaida and Al-Zahwari Army are in competition for control, hence the negative correlation; Bboth the Islamic Fundamentals and Al-Zahwari Army share the same distance metric in the cluster. As analyzed by the percentage of attack, most of the attacks on the mosques were by the politicians and very few by the foreign agents or fighters. Generally, the coalition forces were the most targeted by all adversaries. Public places were the most targets by the foreign fighters and Al-Qaida. The police headquarters were frequently attacked by Al-Qaida and sponsors of the politicians.

6. Conclusion

The paper presents the summary of results for combining data mining, simulation modeling, and sensemaking for aiding the intelligent analysis. The paper is a combination of proof-of-concept (POC) and practice in a laboratory setting that uses experienced battlestaff for information analysis. As a POC, the paper seeks to show how integrative modeling can be used to support information fusion in a complex system. In this case, we use simulation to capture the uncertainties and complex information interaction in a battle system. Then a statistical classification technique is used to reveal how information is related from the simulation outputs. The sensemaking process becomes relevance to the decision maker who can now visualize the information linkages and patterns. For application, the results of the POC is built into an on-going experimentation to calibrate sensemaking performance metrics for different contexts and intelligent analysts, see, e.g., Ntuen (2009)

The results of the ANS model is specific and domain dependent as different contexts and information may generate different patterns of information fusion. The ANS provides important information in understanding the adversary behaviors in terms of selecting targets for attacks and the methods used in the attacks. It shows that the coalition forces is targeted 68% of the time, Police stations,12.8%, mosques,10.2%, malls and markets,5.5%, and other public places,3.2%. Most of the attacks to the coalition forces were from Al-Zawahari army, al-Qaida, Islamic Fundamentals, and Foreign agents. It was also revealed that ethic fighting sponsored by rogue politicians led to attacks on the mosques through suicide bombing. Two things can be attributed to this: first the belief of “going to heaven”, and second, the fact that people attending mosques are rarely check for weapons. The Police stations were attacked mostly by mortars, suicide bombing, and rocket propelled grenades. There were occasional attacks by IEDs and snipers. The coalition forces suffered attacks by rocket propelled grenades and mortars. There was some use of IEDs and snipers, but far less use of suicide bombing. These strategies by the adversaries have to do with the securities at the Police stations and the coalition force headquarters. It is believed that delivering weapons remotely will also protect the adversaries and lead to unexpected deaths on the targets. Suicide bombing were used often on malls and market places. Again, suicide bombers have free access to these places. There were some attacks recorded by snipers, kidnapping, and infrequent

use of IEDs. Other public places also were targets of suicide bombers, kidnapping and snipers. IEDs were used sporadically, but not as a preferred weapon of attack.

The ASN simulation is developed as a proof of concept model for understanding the adversary behaviors in modern battlefields. The conflict in Iraq is used as the domain. While the results obtained are useful in validating these adversary behaviors and strategies, the model is not robust and encompassing to address many strategic problems associated with network-centric battlefield command and control system, including the intangibles of cultural cognition. More studies are needed for this purpose.

ACKNOWLEDGMENT:

This project is supported by Army Research Office (ARO) Grant # W911NF-04-2-0052 under Battle Center of Excellence initiative. Dr. Celestine Ntuen is the project PI. The opinions presented in this report are not those of ARO and are solely those of the authors.

References

Abdollahian, Mark and Carole Alsharabati. (2003). "*Modeling the Strategic Effects of Risk and Perceptions in Linkage Politics*." Rationality and Society. Winter. Available at http://rss.sagepub.com/.

Adams, K. and Ntuen, C.A. (2008). The Advantages and Disadvantages of the Use of Social Network Analysis in the Analysis of Wicked Problems. The Eighth Annual Symposium on Human Interaction With Complex Systems (HICS), Norfolk, VA, April 3-4.

Burt, R.S. (1992). The social structure of competition. In N. Nohria & R. G Eccles (Eds). *Networks and organizations: Structure, form, and action* (pp. 57-91). Boston, MA: Harvard Business School Press.

Carley, Kathleen M. (2003). "Dynamic Network Analysis" in Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers, *Human Factors, National Research Council*, National Research Council. Pp 133-145.

Fayyad, U.M., Piatetsky-Shapiro, G., and Smyth, P (1996). . From Data Mining To knowledge Discovery: An Overview. In Advances in Knowledge Discovery and Data Mining, eds. U.M. Fayyad, G. Piatetsky-Shapiro, P. Smyth, and R. Uthurusamy, AAAI Press/The MIT Press, Menlo Park, CA., 1, pp. 1-34.

Heuer, Richards J. Jr. (1999). Psychology of IntelligenceAnalysis. Center for the Study of Intelligence.

Hood, L., Laughery, K.R., and Dahl, S. (1993). *Proceedings of the 1993 Winter Simulation Conference* (G.W. Evans, M.Mollaghasemi, E.C. Russel, and W.E. Biles, eds), Los Angeles, CA, 218-222.

Houghton et. Al. (2005). WESTT (Workload, Error, Situational Awareness, Time and Teamwork): An Analytical prototyping software tool for C_2. Paper submitted for *10th International Command and Control Research & Technolog.y*

Ntuen, C.A. (2009). Sensemaking as a naturalistic knowledge discovery model. Naturalistic Decision Making and Computers Conference, London, (June).

Perez, L. M., & Dedia, B. L. (2002). An historical evolution of network analysis and its impact on strategic management thinking. *Unpublished paper* #31492.

Krebs, V.E (2003). Website for Inflow, a software-based SNA tool. Includes a good range of articles on SNA as well as Inflow product information. http://www.orgnet.com/.

Ntuen, C.A. and Alabi, O. (2006). Simulating sensemaking process with MicroSaint. Proc. International Command & Control Research Technology (ICCRTS). Devere University Arms, Cambridge, UK.

Valente, T.W. (1995). Network models of the diffusion of innovations. Cresskill, NJ: Hampton Press, Inc.

Wiig, Karl M. (1993). Knowledge Management Foundations: Thinking about thinking – How people and organizations create, represent, and use knowledge. Arlington, TX: Schema Press pp. 87-99.

Taber, C.S. (1994). The policy arguer: The architecture of an expert system. Social Science Computer Review, 12(1), 1-25.

Yolles, M.A. (2006). Organizations as Complex Systems: An Introduction to Knowledge Cybernetics. Greenwich, Connecticut: Information Age Publishing.

USING SIMULATION AS A KNOWLEDGE DISCOVERY TOOL IN AN ADVESARY C2 NETWORK

Celestine A. Ntuen, Ph.D,
Distinguished University Professor
O.A. Alabi, Y. Seong, and Eui H. Park, Ph.D
The Army Center for Human-Centric C2 Decision Making
ntuen@ncat.edu
+1-336-334-7780 (X531): phone
+1-336-334-7729: fax

This project is supported by ARO grant #W911NF-04-2-0052 under Battle Center of Excellence initiative. The opinions presented here are not those from ARO, and are solely those of the authors.

Presentation Outline

1. INTRODUCTION: Adversary Network
2. SOCIAL NETWORK CHARACTERISTICS
3. A MODEL OF ADVESARY NETWORK
4. KNOWLEDGE DISCOVERY IN AN ADVERSARY NET
5. SOURCE OF DATA
6. EXPERIMENTS
7. RESULTS
8. SUMMARY & CONCLUSIONS

Adversary Network

- Terrorist Cells Activist Group
- Street Gang Militia Insurgency

Could be caused by:
Political, Economic, Social
Religious, Nation-Nation, Ethnic Groups
Military/Dictatorship

A Simplified Terrorist Network

HAMAS

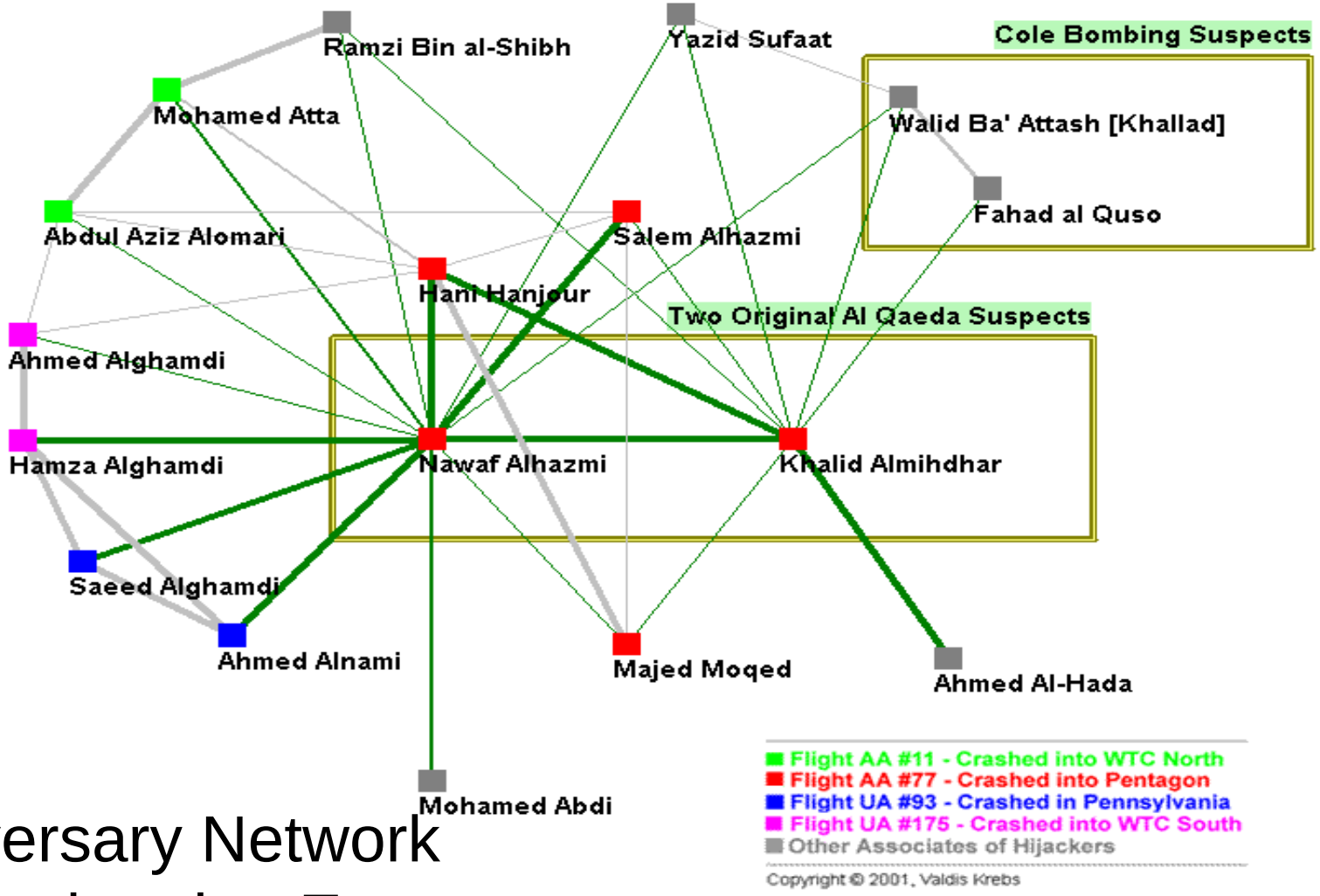
Niger-Delta Freedom Fighters

Born in Kenya

Riot in Tibet. Who is a rogue agent?

Somali Pirates

Valdis Krebs: www.orget.com/tnet.html (June 2, 2009)



Adversary Network Associated to Events

Figure 2 - All nodes within 1 step [direct link] of original suspects

SOME PROBLEMS

- ✓Creates complex social networks
  - ✓Adversaries –adaptive, evolving, learning, migrating, recruiting
  - ✓Techniques and practices are sophisticated---use technology wisely, adopt low cost investment with maximum payoff—chaos, pandemonium, etc.

SOME PROBLEMS

- ✓Leadership
  - ✓Controlled
  - ✓Loyalty/ affinity/ coercion/
- ✓Organization
  - ✓No specific structure
  - ✓Spread-activation nets
  - ✓Religious-based

CHALLENGES TO MILITARY C2

Intelligence Collection and Analysis
Sensemaking/Decision Making
Security Protection to High State Targets
Tracking, Recognizance, and Targeting
Predictability of the Adversary Intentions

Modeling and knowledge representation problem
Mathematically intractable

===> Simulation provides an alternative

ADVERSARY NETWORKS HAVE SOCIAL NETWORK CHARACTERISTICS

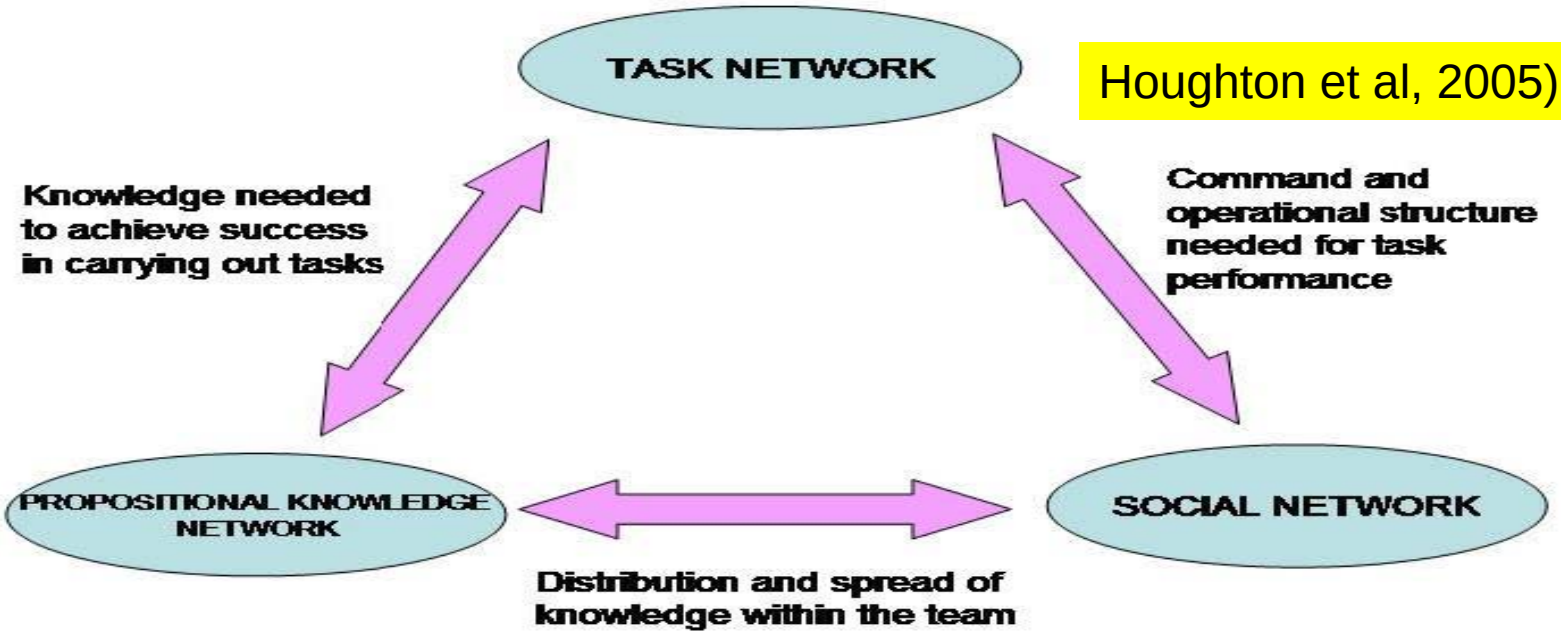
- Social network analysis (SNA): a method that helps explain interrelationships between actors.
- The actors in SNA consist of individuals or other groups in the organization.
- SNA contacts can be formal alliances, cooperatives, interlocking directorates, intergovernmental relationships, supplier/customer relationships, and joint ventures

- Network structure is used to predict similarity between attitudes and behaviors
- Network analysis can help focus on the types of actors in the network.
- SNA is also the mapping and measuring of relationships and flows between people, groups, organizations, computers or other information/knowledge processing entities

- Social network theory provides the following information:
  - It provides the metric on how people interact and share common information characteristics.
  - It can be used to help explain forces and influences that determine how groups are formed.
  - It allows researchers to determine the metrics that glue groups together

- Social Network background
  - Valente (1995) explained that a “network is the pattern of friendship, advice, communication, or support that exists among members of a social system
  - Burt (1983, 1987), has studied different network models of diffusion and noted that social contagion occurs when people use one another in a network to manage the uncertainty of innovation

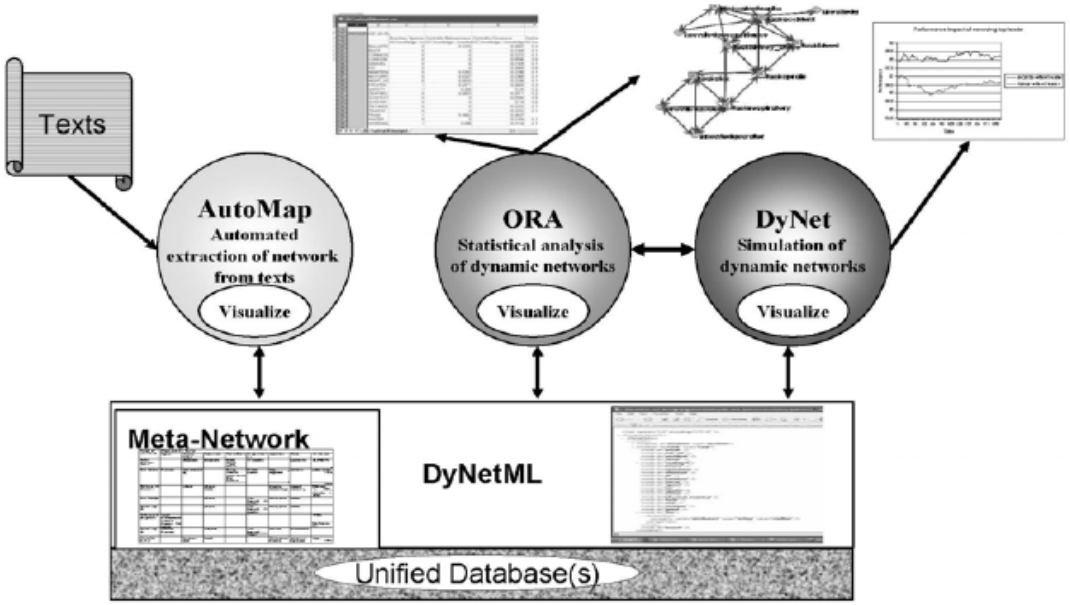
- Social Network modeling approaches
  - WESTT (Workload, Error, Situational Awareness, Time and Teamwork)
  - WESTT represents a team activity at the system level in which both humans and the technology interact with each other

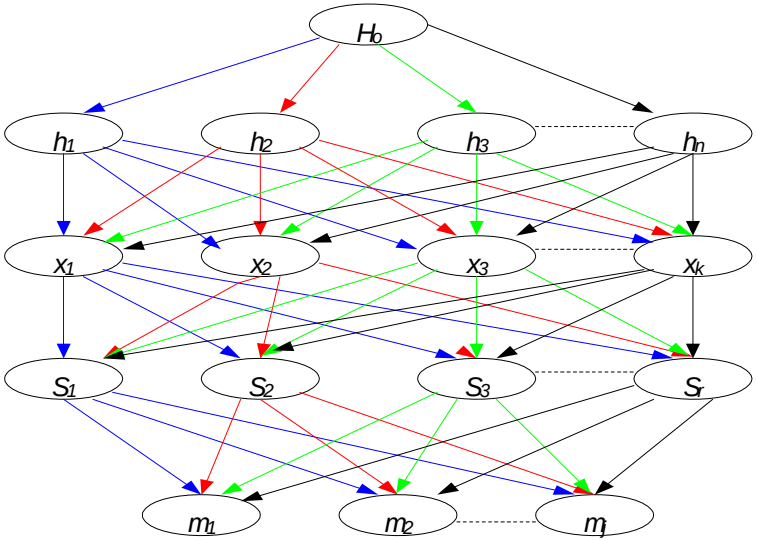


Houghton et al, 2005).

- Senturion is a simulation model that analyzes the political dynamics within local, domestic, and international contexts and predicts how the policy positions of competing interests will evolve over time (Abdollahian & Alsharabati, 2003).
  - The set of rules used by Senturion synthesize several classes of political science and microeconomic theories into a real-world decision-making tool for researchers and practitioners

- Dynamic network analysis (DNA) is a social network model centered on the collection, analysis, understanding and prediction of dynamic relations (such as who talks to whom) and the impact of such dynamics on individual and group behavior (Carley, 2003)
- DNA has several distinctive hallmarks:
  - The web of affiliations connects not just agents, but agents and other entities such as knowledge, tasks and organizations.
-





- A model of an adversary network requires various interacting factors that may include:
  - Intention expressed by target (h)
  - Adversary agents (x)
  - Motive for attack (m)
  - Possible sponsor (s)
- The information is required by friendly forces in other to plan and develop courses of action required to deter unwanted adversary behaviors

KNOWLEDGE DISCOVERY (KD) IN AN ADVESARY NETWORK

- KD is a non-trivial extraction of implicit, unknown, and potentially useful information from data (Fayyad, Piatetsky-Shapiro, & Smyth, 1996)
- Naturalistic KD (Ntuen 2009): Combines field observation and experience to interpret a situation of interest. When an on-going information does not fit into the existing mental model of the expert, further information is explored, selected, and mentally tested for the situation.
  - Sensemaking
  - Information foraging
  - Information fusion

SIMULATION AS A KNOWLEDGE DISCOVERY TOOL

From modeling and simulation, the intelligent analyst can explore many state-spaces of information analysis required for knowledge discovery:

For examples:

- Who are the adversary agents? Their cliques? Organization culture? Sponsor?
- What are the targets of interest to the adversaries? Why?
- What are their traditional and non-conventional intents/objectives?
- How do the recruit? From what cohort population?
- Which adversary tends to show dominant behaviors? Why?
- What are the adversary motives?

SIMULATION AS A KNOWLEDGE DISCOVERY TOOL

From modeling and simulation, the intelligent analyst can explore many state-spaces of information analysis required for knowledge discovery:

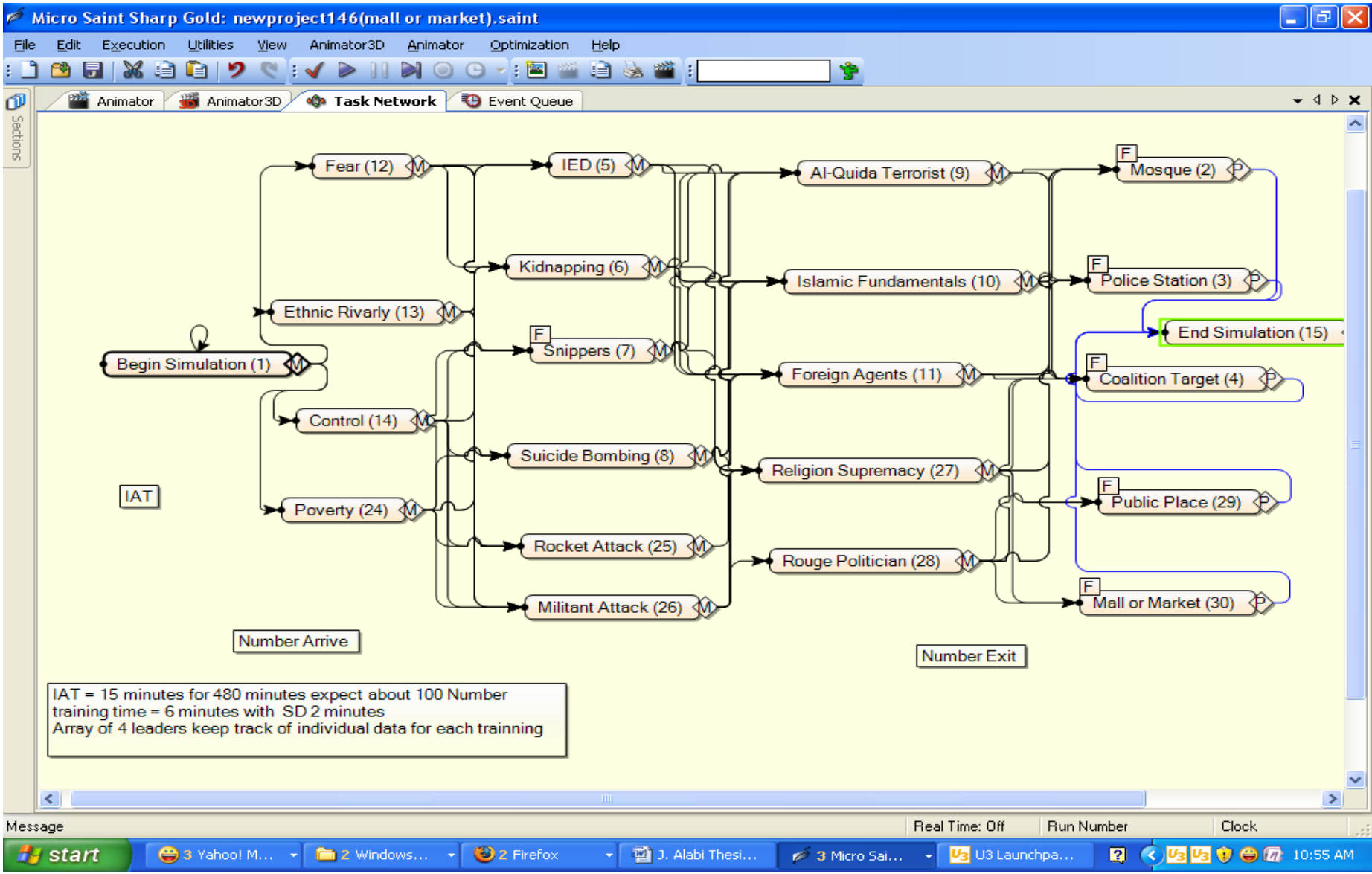
For examples:

- Who are the adversary agents? Their cliques? Organization culture? Sponsor?
- What are the targets of interest to the adversaries? Why?
- What are their traditional and non-conventional intents/objectives?
- How do the recruit? From what cohort population?
- Which adversary tends to show dominant behaviors? Why?
- What are the adversary motives?

The simulation model is based on cognitive representation of social information linkages between the adversary players and the dimensions of attack orchestrated in asymmetric battlefield environments

- Micro Saint is a network-based simulation language developed from knowledge of human performance and cognitive information processing.
- It is a task network modeling, in which activities are represented in a diagram as nodes, and the arrows between the nodes represent the sequence in which the activities are performed (Hood, Laughery, and Dahl, 1993).
- Each activity, whether it is a human activity or a system activity, is defined using the same method.

Sample Micro Saint networks for ASN



Source of Data

- Department of Defense website, icasualties.org and Brookings Institution website
  - Types of casualties
  - Suspected/claimed advesaries
  - Targets and locations
  - Time of incidence
  - Claims and motives

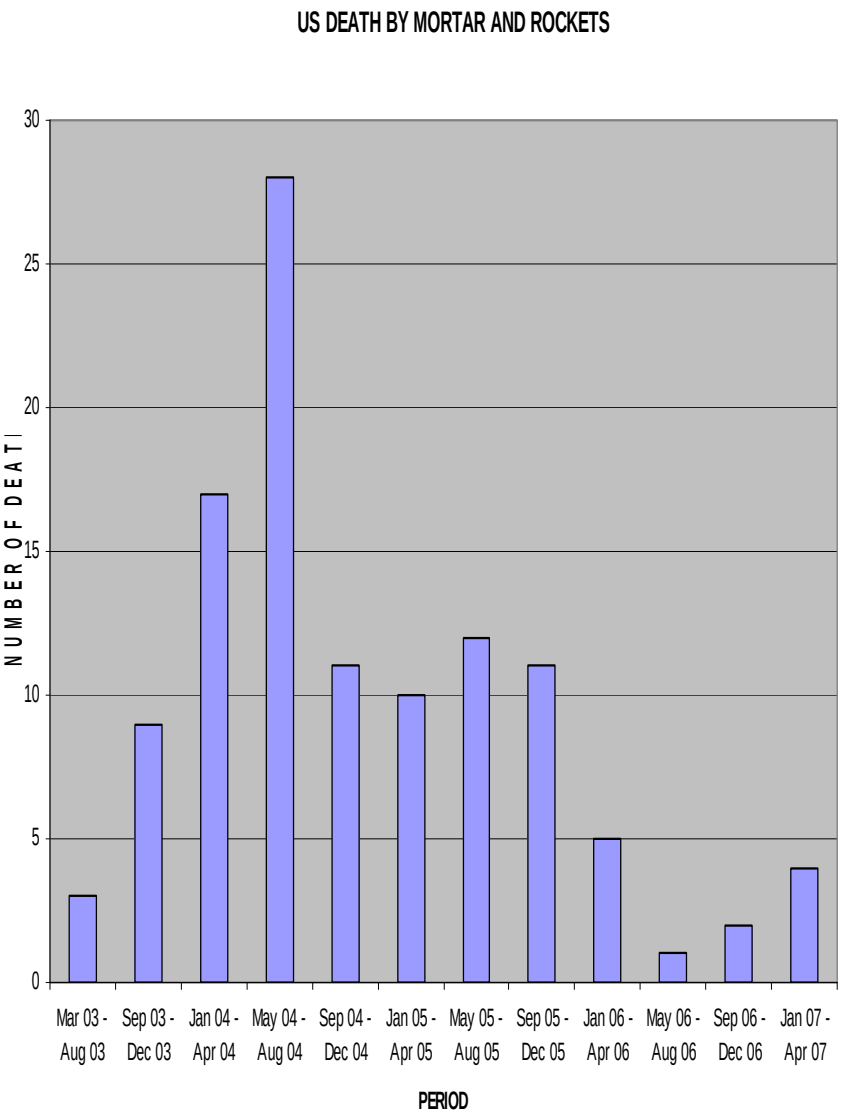
Source of Data: *Events and Fatality Statistics for 3/2003-2/2007*

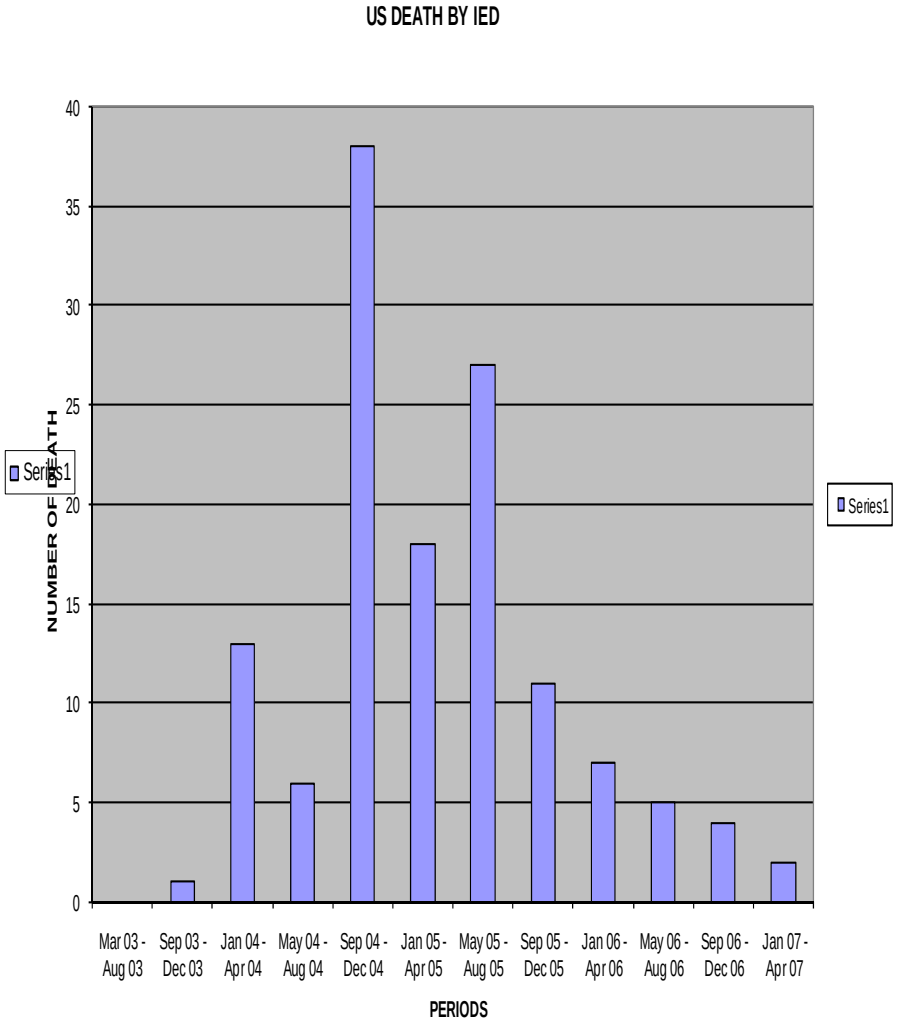
Method Used (Number of Occurrence)		IED	Kidnapping	Sniper Attack	Suicide Bombing	Mortar	Rocket Propelled Grenade
	Min	0.005	2.56	2.99	4.03	1.71	1.45
	Max	18.7	9.44	7.57	15.74	18.46	14.99
	Mean	4.27	5.91	4.99	9.67	9.77	9.79
	STD	3.44	1.55	0.99	3.01	3.2	3.07
	Distribution Assumption	**Normal**	**Normal**	**Exponential**	**Normal**	**Log Normal**	**Exponential**
	K – S Value	**0.49**	**0.22**	**0.14**	**0.43**	**0.46**	**0.44**
Fatalities (Deaths)	Min	11	1	1	1	11	1
	Max	191	10	20	32	28	17
	Mean	105.8		7.95	3.64	9.416	6.58
	STD	56.8		6.1	2.14	7.57	5.36
	Distribution Assumption	**Normal**	**Normal**	**Exponential**	**Normal**	**Lognormal**	**Exponential**
	K – S Value	**0.17**	**0.53**	**0.92**	**0.31**	**0.4**	**0.84**

An Example of Event –Target Mapping By Attack Methods to Area of Interests (1)/ By Suspected Sponsors (2)

EVENT \ TARGET (1)	MOSQUE	POLICE STATION	COALITION TARGET	PUBLIC PLACES	MALL OR MARKET
IED	0.15	0.1	0.3	0.15	0.15
KIDNAPPING	0.3	0.1	0.05	0.3	0.3
SNIPPER	0.15	0.15	0.15	0.05	0.05
ROCKET ATTACK	0.05	0.15	0.15	0.05	0.05
SUCIDE BOMBER	0.05	0.3	0.15	0.3	0.3
MILITANT ATTACK	0.3	0.2	0.2	0.15	0.15

SPONSORS\TARGET (2)	MOSQUE	POLICE STATION	COALITION TARGETS	PUBLIC PLACES	MALL ATTACK
AL ZAWAHARI ARMY	0.4	0.05	0.25	0.05	0.05
FOREIGN ARMY	0.15	0.25	0.15	0.25	0.25
ROUGE POLITICIAN	0.05	0.05	0.05	0.05	0.05
ISLAMIC FUNDAMENTALIST	0.25	0.3	0.15	0.3	0.3
AL QUIDA	0.15	0.35	0.4	0.35	0.35


US DEATH BY MORTAR AND ROCKETS
NUMBER OF DEATH
30
25
20
15
10
5
0
Mar 03 - Aug 03
Sep 03 - Dec 03
Jan 04 - Apr 04
May 04 - Aug 04
Sep 04 - Dec 04
Jan 05 - Apr 05
May 05 - Aug 05
Sep 05 - Dec 05
Jan 06 - Apr 06
May 06 - Aug 06
Sep 06 - Dec 06
Jan 07 - Apr 07
PERIOD


US DEATH BY IED
NUMBER OF DEATH
40
35
30
25
20
15
10
5
0
Mar 03 - Aug 03
Sep 03 - Dec 03
Jan 04 - Apr 04
May 04 - Aug 04
Sep 04 - Dec 04
Jan 05 - Apr 05
May 05 - Aug 05
Sep 05 - Dec 05
Jan 06 - Apr 06
May 06 - Aug 06
Sep 06 - Dec 06
Jan 07 - Apr 07
PERIODS
Series1

Experimental Design

- The ASN simulation consists of the mapping of targets (M), attack methods (N), a set of adversaries (A), and motivation variables (P).
- Dimensionally, the simulation space is M * N * A * P design. The complexity of the network is determined by the number of elements in M, N, A, and P respectively.
- If M = 2, N = 3, A = 2, and P = 2, there are 24 possible experimental trials by Micro Saint software.
- The mappings are also realized through probabilistic decision nodes.
- The minimum number of experiment equal to 1 (assume M = 1, N = 1, A = 1, P = 1).
- The expected number of experiments depends on the user's input and can be constrained by $1 \leq NE \leq \#E$ where, #E = M * N * A * P, and at least one M, N, A, or P has elements greater than 1.

CONTROL RULES

Rule 1: Adversary Relationship Rules (ARR)

a. Equally weighted adversary power (defined in terms of a reward sharing behavior) with equal probability assignment.

b. Unequal adversary power using random probability assignment.

Rule 2: Target Selection Rules (TSR)

a. Targets with the most human casualties.

b. Targets with the most cultural and religious values (e.g. holy mosques)

c. Targets with the most political values (e.g. ethnic killings and kidnappings)

d. Targets with the most military significant (e.g. coalition f forces)

e. Targets with most economic values (e.g. oil wells)

CONTROL RULES

Rule 3: Attack Resource Rules (ARER)

a. Use the most available weapon (select at random)
b. Use the cheapest weapon with the likelihood of more effect; high priority e.g. IED, and so on.
c. Use weapon of mass destruction (low priority in this model)

Rule 4: Motive Selection Rules (MSR)

a. Disgrace of foreign coalition troops
b. Distortion and blackmail for economic gain
c. Unemployment

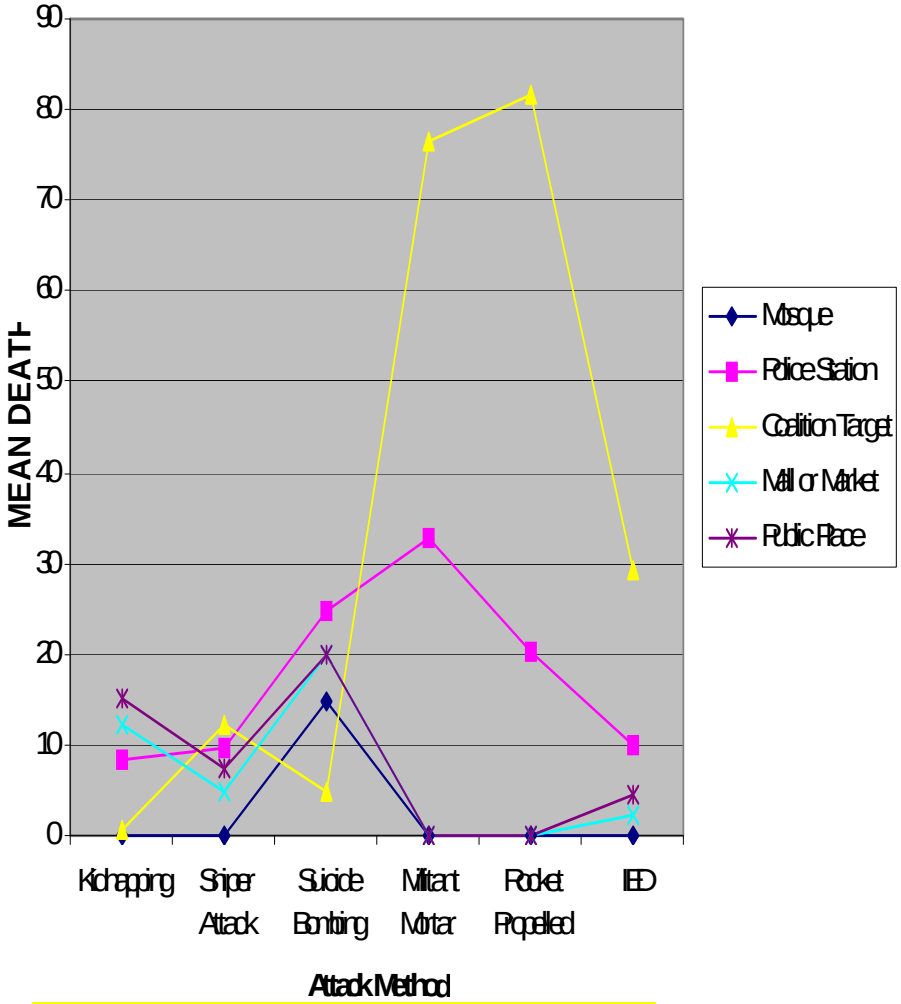
Variance Reduction Simulation Trials

Warm up conditions were initiated by simulating the network without any rule using the traditional network information flow in Micro Saint with the input data randomly initialized.

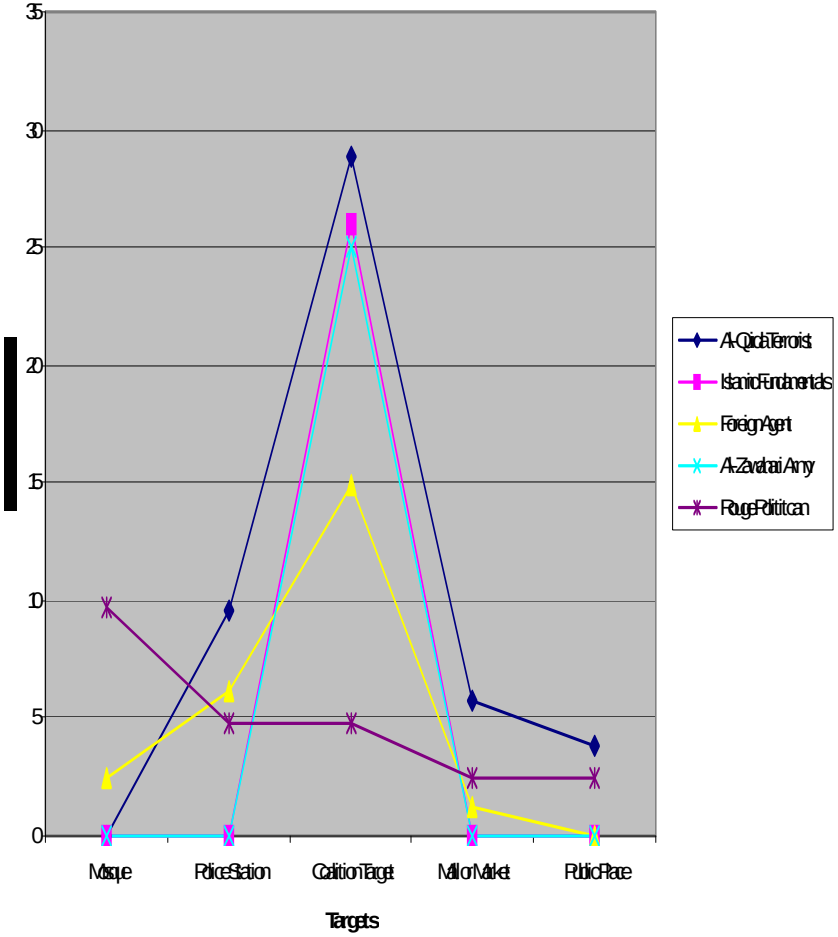
Ten different simulation experiments were conducted and the average results calculated on daily event basis (1440 minutes).

The dependent variable is the number of deaths inflicted on the network by the adversaries using the available methods of attacks. The experiments were performed to reduce variations and to determine the best number of runs to minimize result variations and obtain stability.

Results and Analysis: Rule 1-Equally weighted



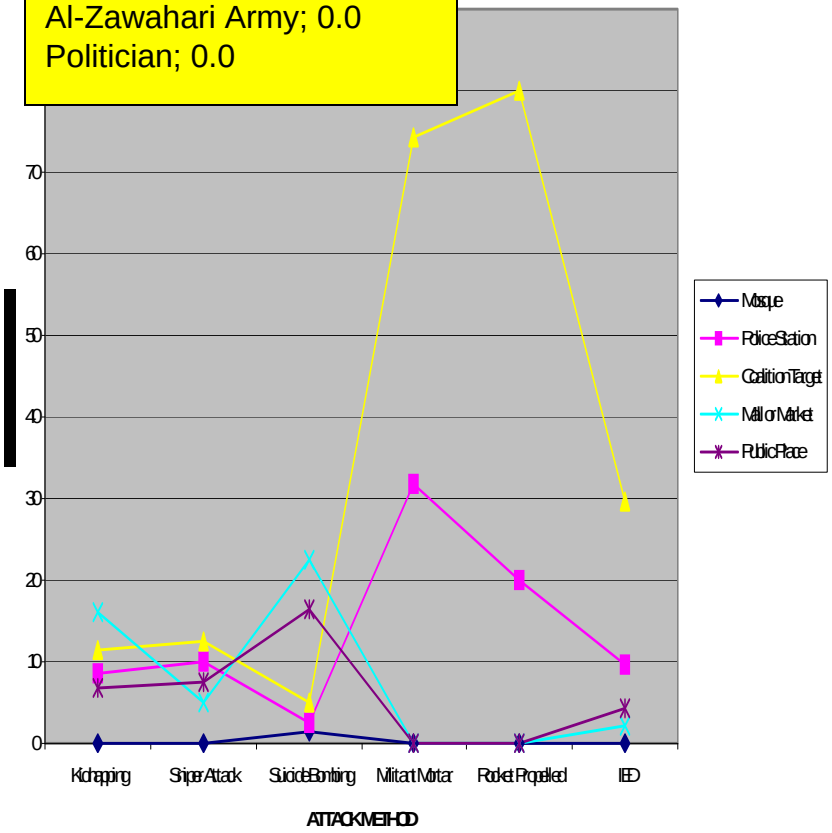
Attack Method & Targets



Sponsors & Targets

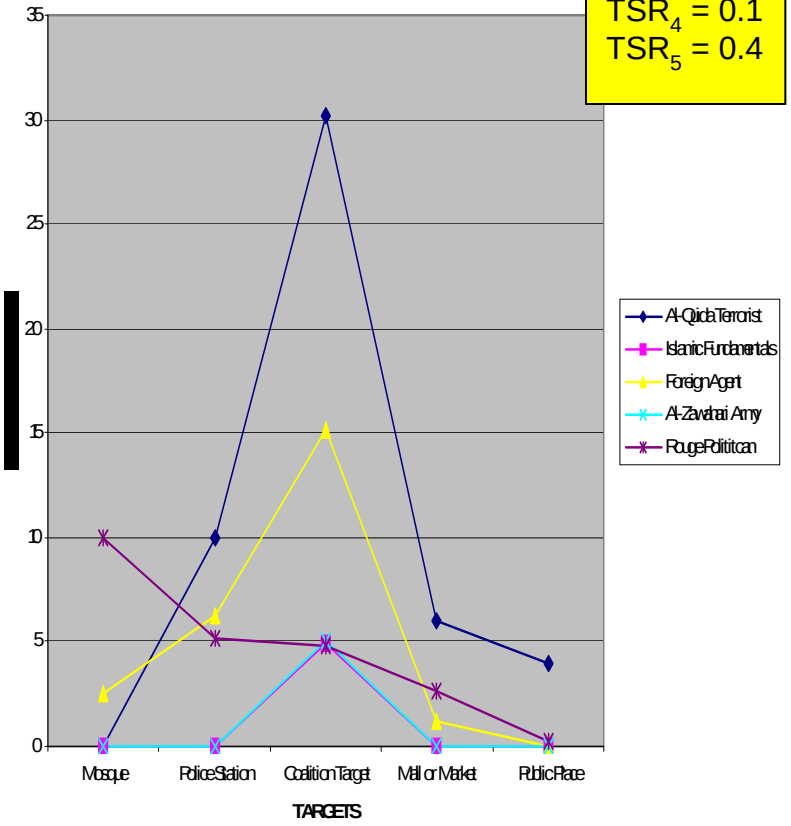
Results and Analysis: Rule 2-UnEqually weighted

Al- Quida; 0.5
Islamic fundamental; 0.3
Foreign Agents; 0.2
Al-Zawahari Army; 0.0
Politician; 0.0



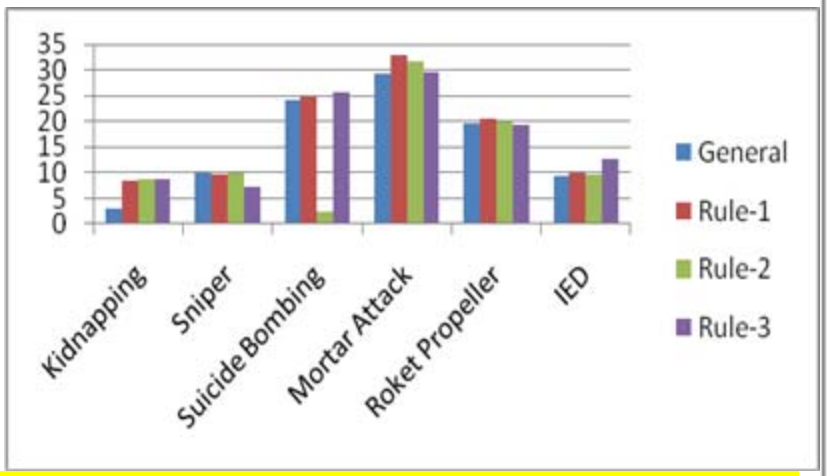
Attack Method & Targets

$TSR_1 = 0.0$
$TSR_2 = 0.2$
$TSR_3 = 0.3$
$TSR_4 = 0.1$
$TSR_5 = 0.4$

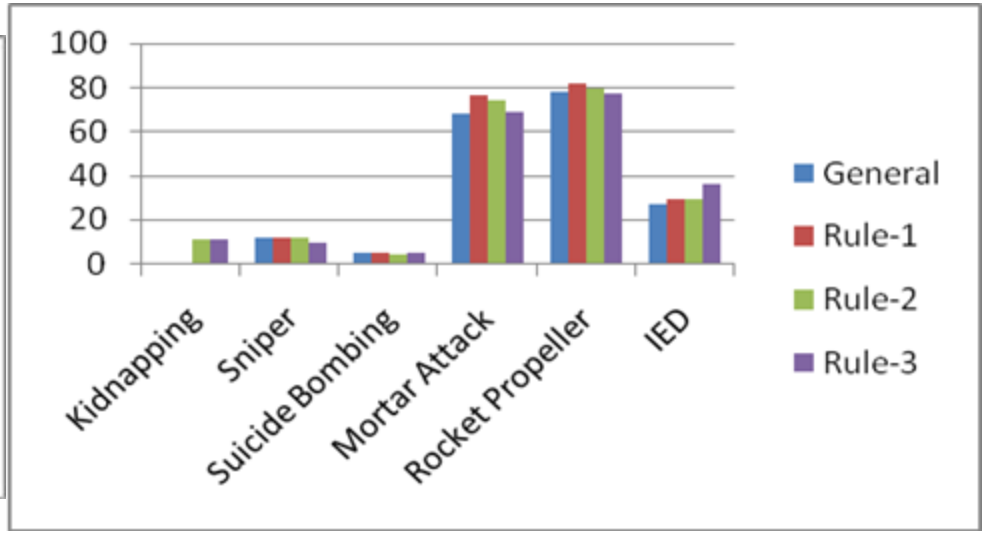


Sponsors & Targets

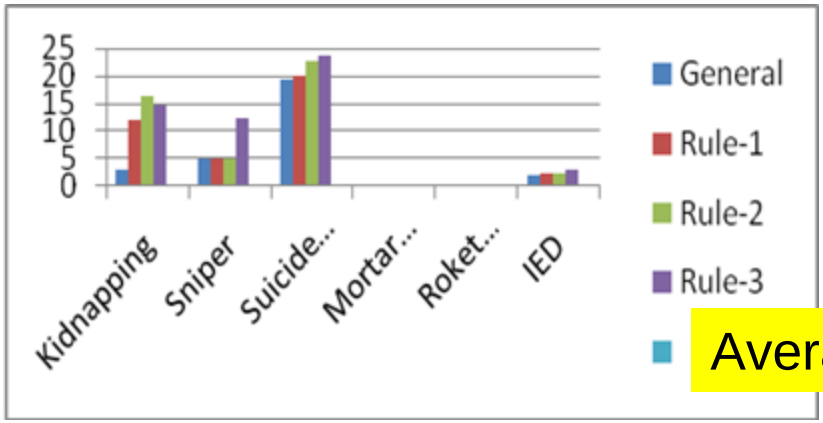
KNOWLEDGE DISCOVERY ANALYSIS—Insightful Statistics



Average death & attack on police



Average death & attack on coalition forces



Average death & attack on malls and markets

KNOWLEDGE DISCOVERY ANALYSIS—Insightful Statistics

	Mosques	Police Stations	Coalition Forces	Mall and Market	Public Place
General	30.70083	24.65116	23.4122	17.61905	25.79991
Rule - 1	31.5054	27.44186	25.05311	23.33333	26.36323
Rule - 2	3.091256	21.24031	25.93217	27.38095	19.73862
Rule - 3	34.70252	26.66667	25.60252	31.66667	28.09824
Total	**100%**	**100%**	**100%**	**100%**	**100%**

Percentage of rules used in each target by the ASN

KNOWLEDGE DISCOVERY ANALYSIS—Insightful Statistics

Advesaries	Mosque	Police Stations	Coalition Forces	Mall & Markets	Public places	Total
Al-Qaida	0	20	60	12	8	100
Al-Zawahari	0	0	100	0	0	100
Rouge Politicians	40	20	20	12	8	100
Islamic Fundamental	0	0	100	0	0	100
Foreign agents	11	24	60	5	0	0

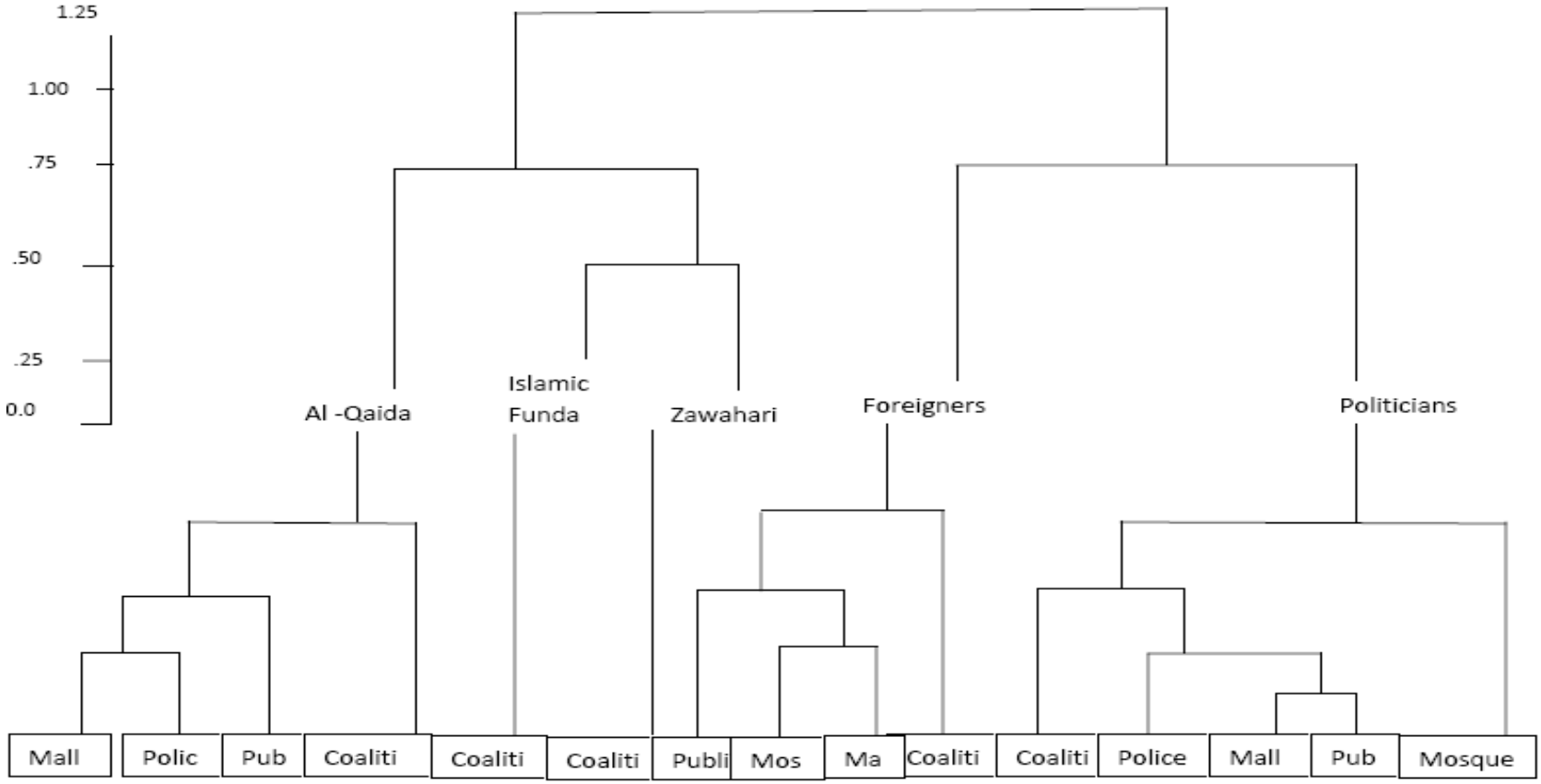
Percentage of targets attacked by each adversary in the network

KNOWLEDGE DISCOVERY ANALYSIS—Insightful Statistics

Weapons of attack	Mosque	Police Stations	Coalition Forces	Mall & Markets	Public places
Kidnapping	0	0	0	9.4	31.9
Sniper	0	11.1	6.7	15.6	17
Suicide bombing	69	26.7	2.6	60	42.6
Mortars	0	32.2	35.75	0	0
Rocket propelled	0	22.2	40	0	0
IED	0	11.1	13.9	6.25	8.5

Percentage of weapon used on targets

KNOWLEDGE DISCOVERY ANALYSIS—Insightful Statistics



A hierarchical cluster tree of the sponsors and targets.

KNOWLEDGE DISCOVERY ANALYSIS—Insightful Statistics

Politicians vs Foreign agents: 0.68 (p = 0.003)

Al-Qaida, Islamic Fundamentals, & Al-Zahwari Army belong to the same cluster:

Al-Qaida vs Islamic Fundamentaliss: 0.83 (p = 0.001)

Al-Qaida vs Al-Zahwari : -0.745 (p = 0.018)==➔ competition to control

Al-Zahwari vs. Islamic Fundamentalists: 0.61 (p = 0.003)—same distance metric

Coalition forces most attacked

Public places attacked by Al-Qaida and foreign agents

Police headquarters attacked frequently by Al-Qaida & sponsored politicians

Correlation Analysis.

SUMMARY AND CONCLUSIONS

- The ANS provides important information in understanding the adversary behaviors in terms of selecting targets for attacks and the methods used in the attacks.
- It shows that the coalition forces is targeted 68% of the time, Police stations,12.8%, mosques,10.2%, malls and markets,5.5%, and other public places,3.2%.
- Most of the attacks to the coalition forces were from Al-Zawahari army, al-Qaida, Islamic Fundamentals, and Foreign agents.
- It was also revealed that ethic fighting sponsored by rogue politicians led to attacks on the mosques through suicide bombing.

SUMMARY AND CONCLUSIONS

- The Police stations were attacked mostly by mortars, suicide bombing, and rocket propelled grenades. There were occasional attacks by IEDs and snipers.
- The coalition forces suffered attacks by rocket propelled grenades and mortars. There was some use of IEDs and snipers, but far less use of suicide bombing. These strategies by the adversaries have to do with the securities at the Police stations and the coalition force headquarters. It is believed that delivering weapons remotely will also protect the adversaries and lead to unexpected deaths on the targets.

SUMMARY AND CONCLUSIONS

- The ANS simulation is developed as a proof of concept model for understanding the adversary behaviors in modern battlefields.
- By using the current anecdotal results, investigate the effectiveness of using more rules that capture the behaviors of the adversaries and their strategies in the use of weapons and selection of targets.