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

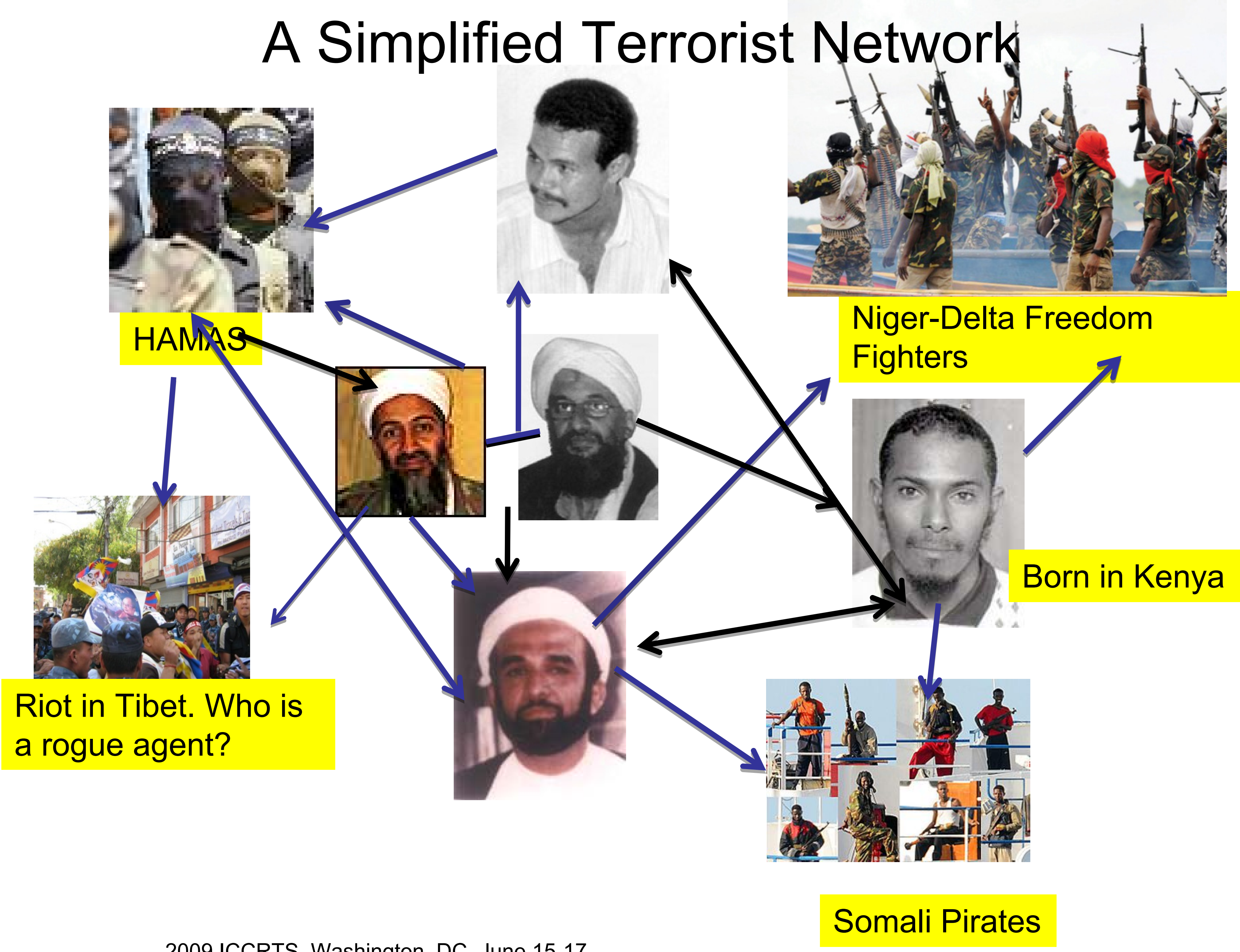
1. INTRODUCTION: Adversary Network
2. SOCIAL NETWORK CHARACTERISTICS
3. A MODEL OF ADVESARY NETWORK
4. KNOWLEDGE DISCOVERY IN AN ADVERSARY NET
5. SOURCE OF DATA
6. EXPERIMENTS
7. RESULTS
8. SUMMARY & CONCLUSIONS

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

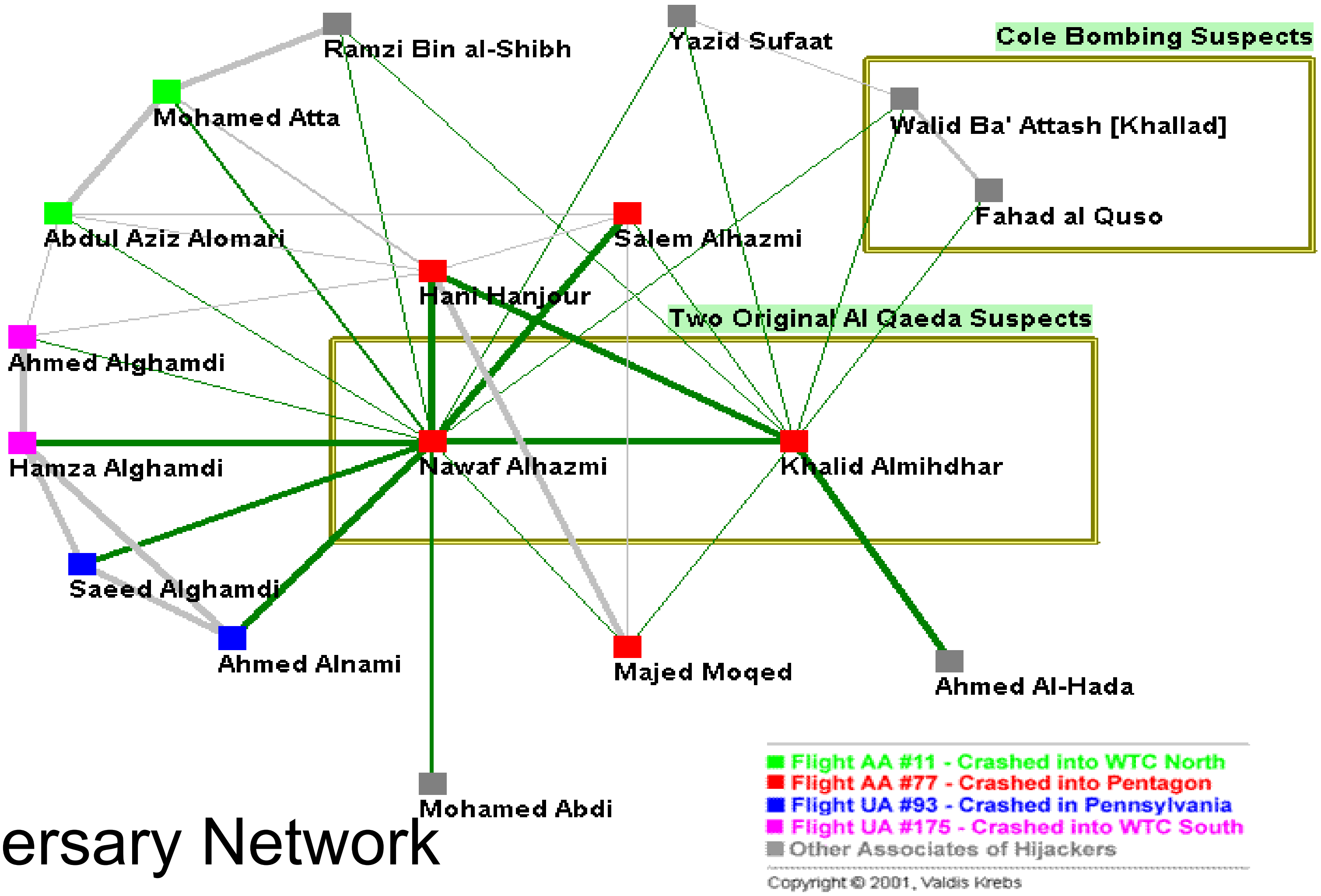
Niger-Delta Freedom Fighters

Born in Kenya

Riot in Tibet. Who is a rogue agent?

Somali Pirates

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


Ramzi Bin al-Shibh
Yazid Sufaat
Cole Bombing Suspects
Mohamed Atta
Walid Ba' Attash [Khallad]
Fahad al Quso
Abdul Aziz Alomari
Salem Alhazmi
Hani Hanjour
Two Original Al Qaeda Suspects
Ahmed Alghamdi
Hamza Alghamdi
Nawaf Alhazmi
Khalid Almihdhar
Saeed Alghamdi
Ahmed Alnami
Majed Moqed
Ahmed Al-Hada
Mohamed Abdi
🟩 Flight AA #11 - Crashed into WTC North
🟥 Flight AA #77 - Crashed into Pentagon
🟦 Flight UA #93 - Crashed in Pennsylvania
🟪 Flight UA #175 - Crashed into WTC South
⬛ Other Associates of Hijackers
Copyright © 2001, Valdis Krebs

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

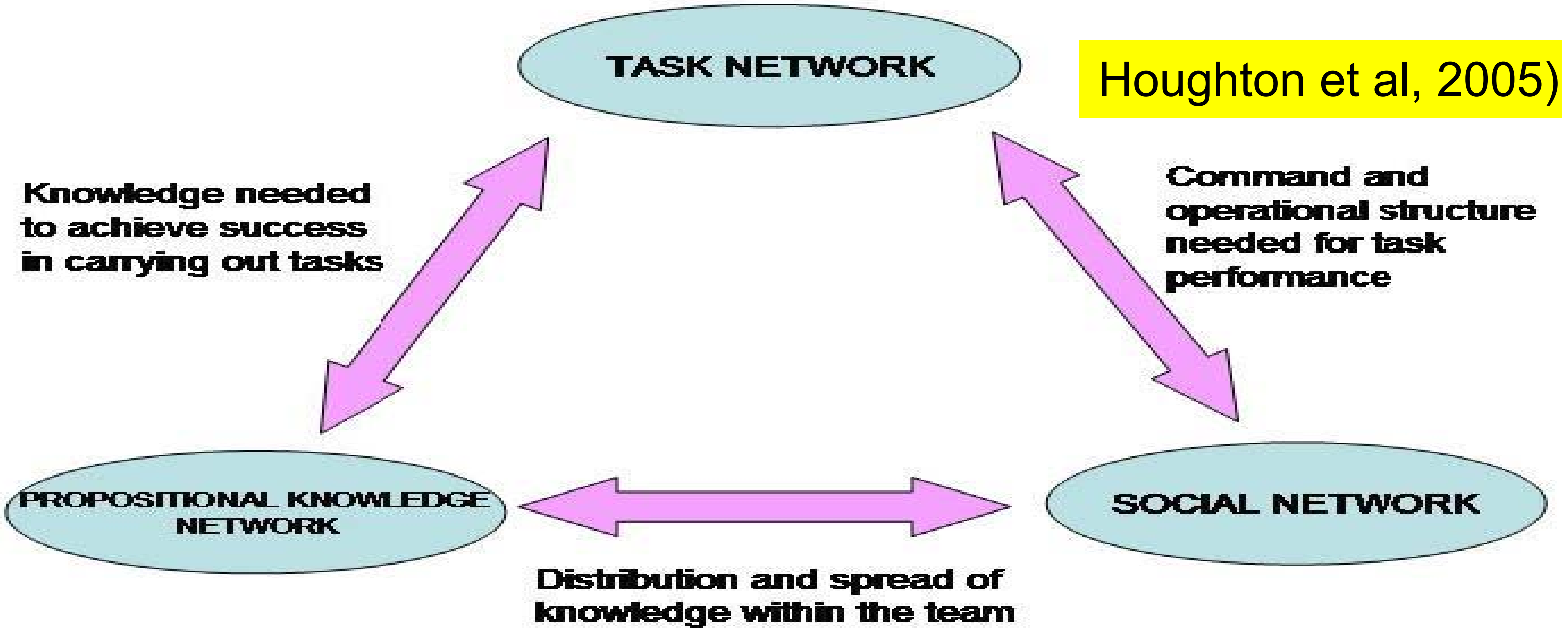
- Social network analysis (SNA): a method that helps explain interrelationships between actors.
- The actors in SNA consist of individuals or other groups in the organization.
- SNA contacts can be formal alliances, cooperatives, interlocking directorates, intergovernmental relationships, supplier/customer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

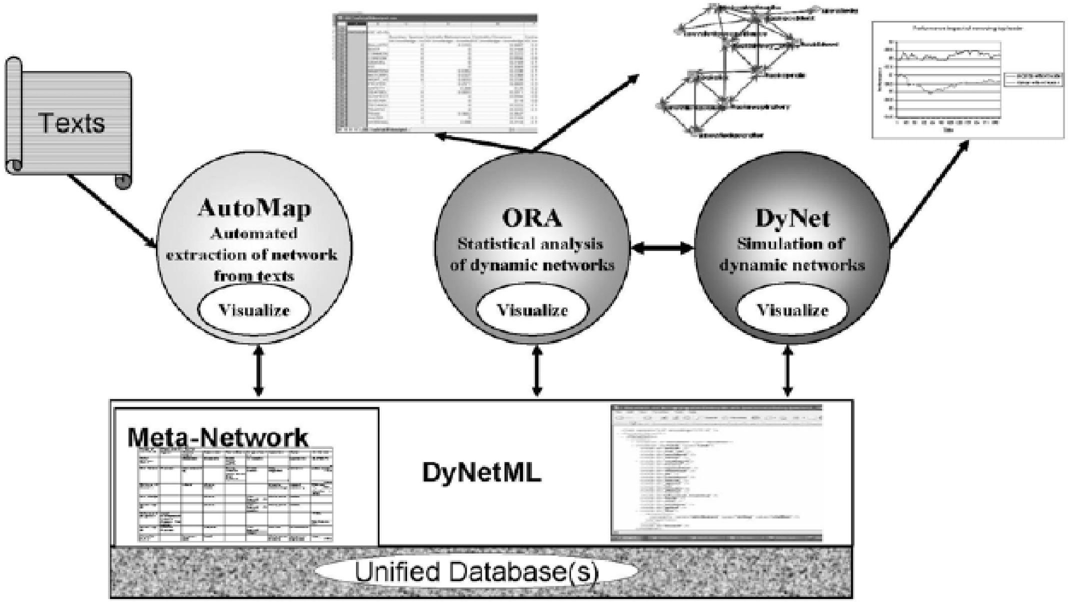

TASK NETWORK
Knowledge needed to achieve success in carrying out tasks
Command and operational structure needed for task performance
PROPOSITIONAL KNOWLEDGE NETWORK
SOCIAL NETWORK
Distribution and spread of knowledge within the team

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.



Texts

AutoMap
Automated extraction of network from texts
Visualize

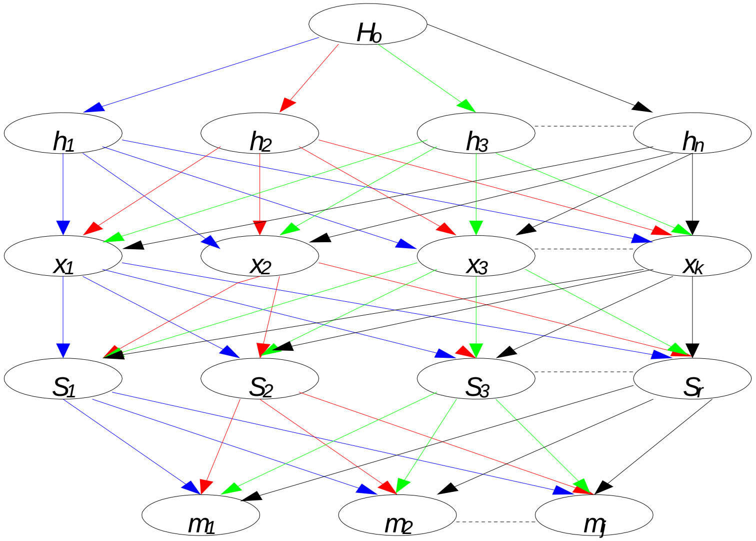
ORA
Statistical analysis of dynamic networks
Visualize

DyNet
Simulation of dynamic networks
Visualize

Meta-Network

DyNetML

Unified Database(s)



- 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?

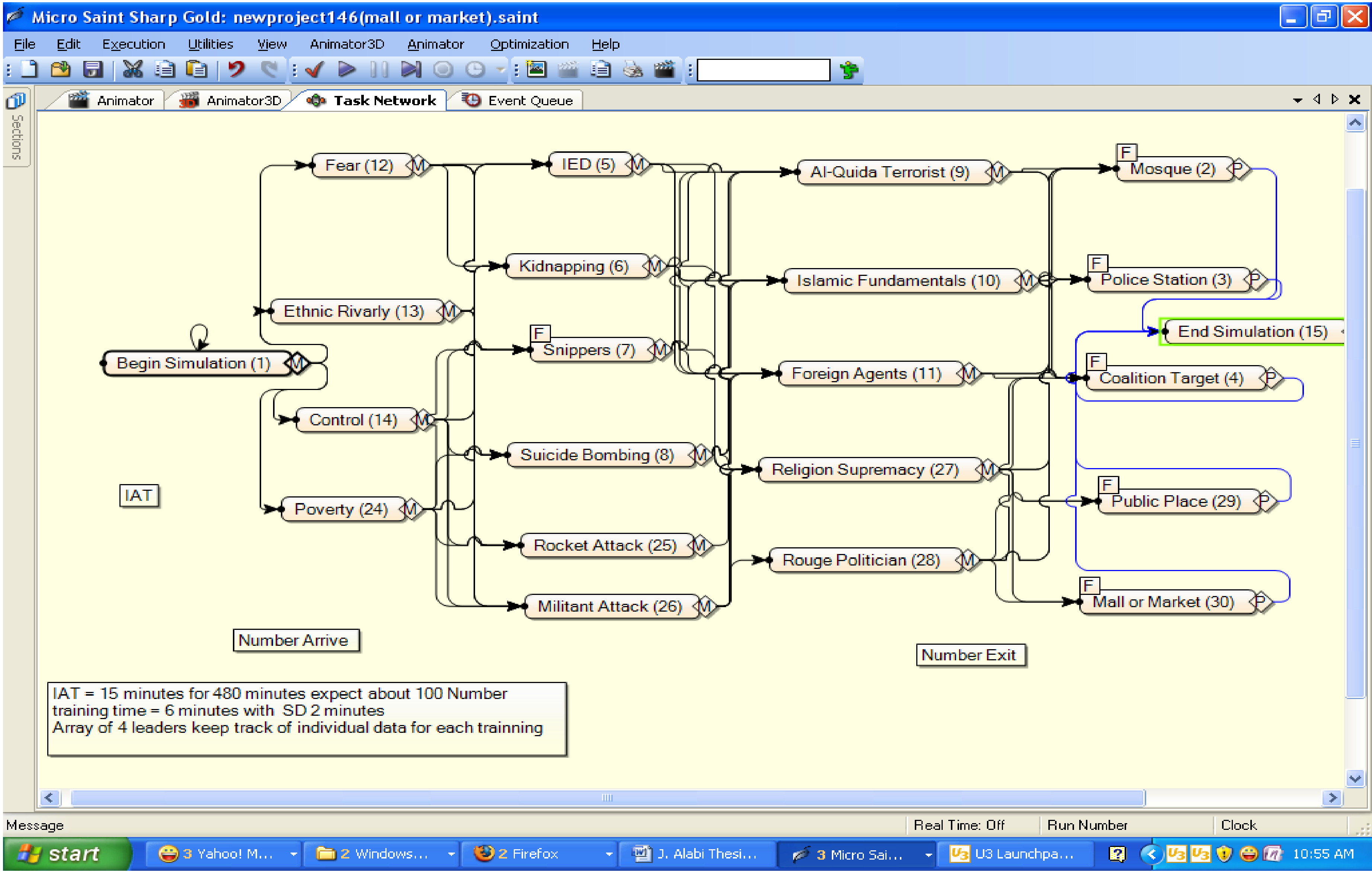
The simulation model is based on cognitive representation of social information linkages between the adversary players and the dimensions of attack orchestrated in asymmetric battlefield environments

❑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



IAT = 15 minutes for 480 minutes expect about 100 Number
training time = 6 minutes with SD 2 minutes
Array of 4 leaders keep track of individual data for each trainning

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

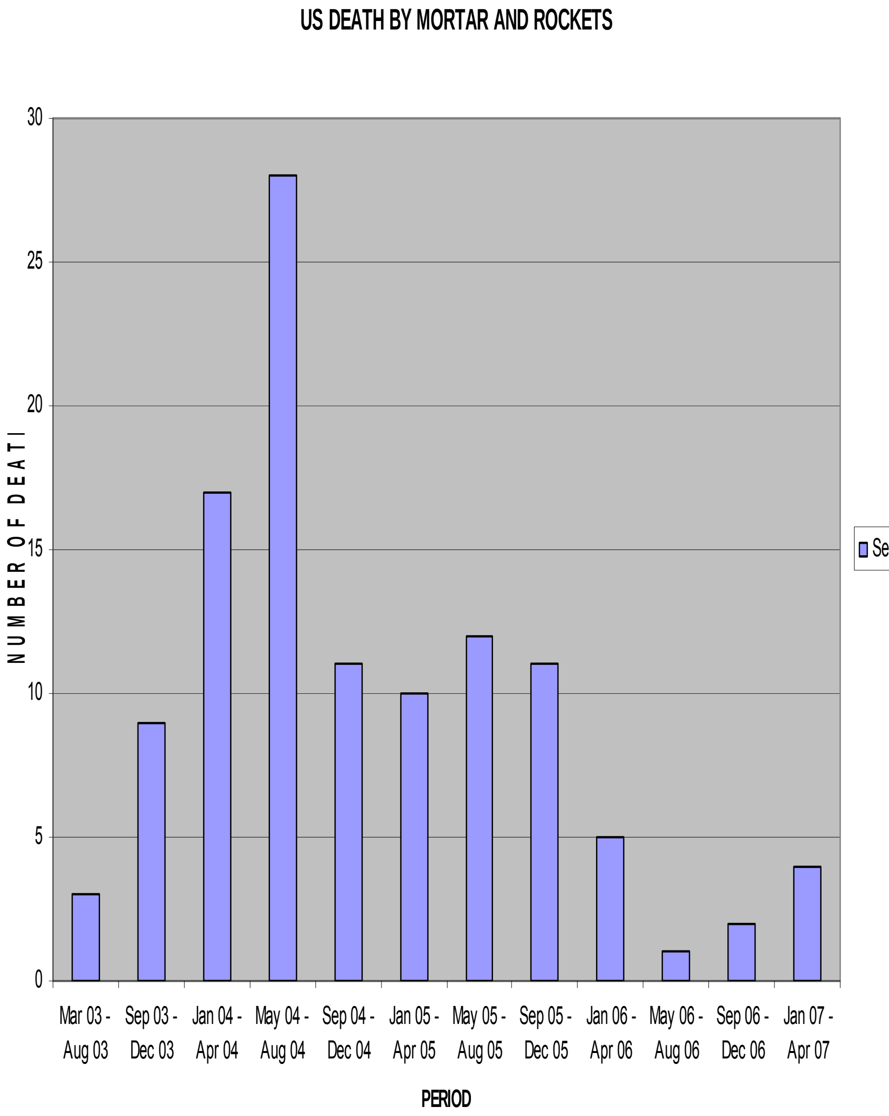
Source of Data: *Events and Fatality Statistics for 3/2003-2/2007*

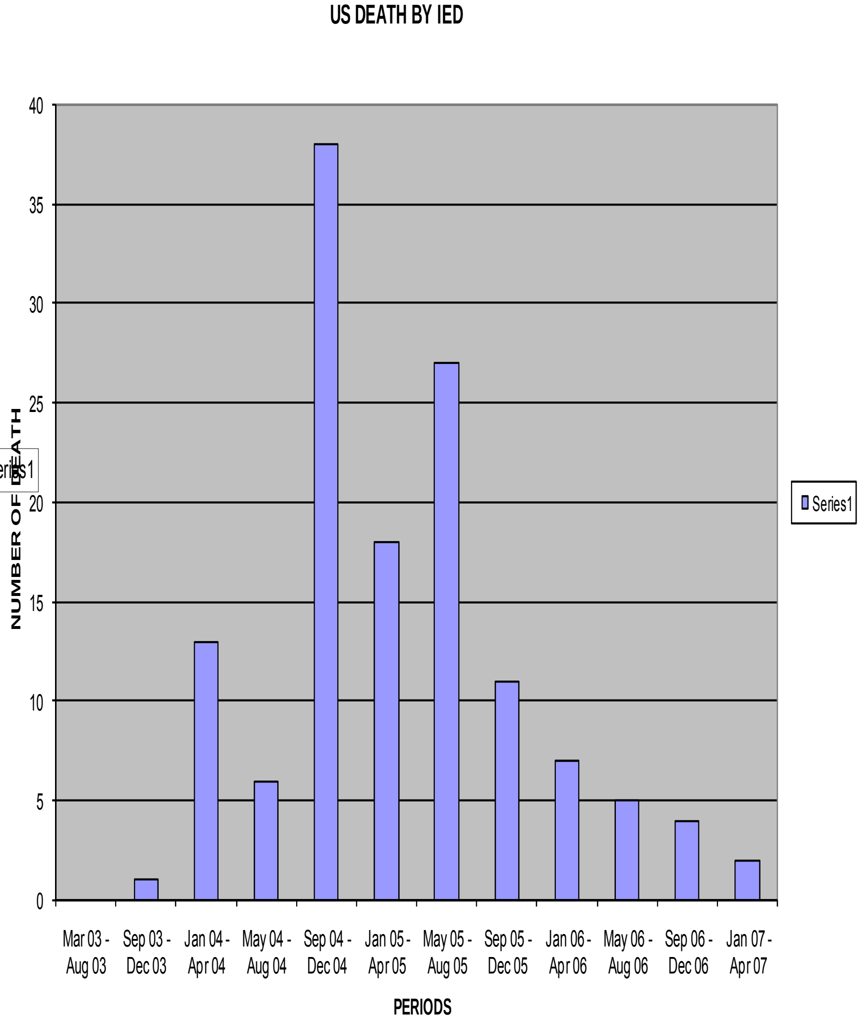
Method Used		IED	Kidnapping	Sniper Attack	Suicide Bombing	Mortar	Rocket Propelled Grenade
(Number of Occurrence)	Min	0.005	2.56	2.99	4.03	1.71	1.45
	Max	18.7	9.44	7.57	15.74	18.46	14.99
	Mean	4.27	5.91	4.99	9.67	9.77	9.79
	STD	3.44	1.55	0.99	3.01	3.2	3.07
	Distribution Assumption	**Normal**	**Normal**	**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 DEATI
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
Series1


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 ≤ NE ≤ #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

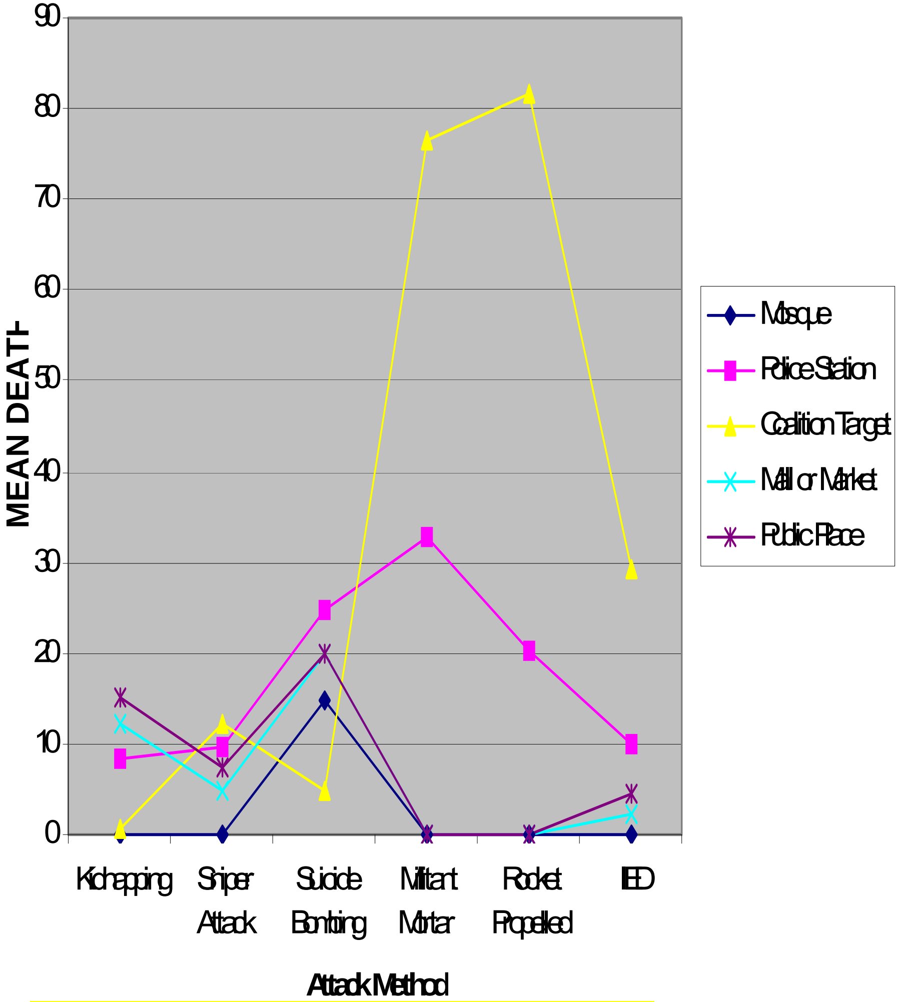
Variance Reduction Simulation Trials

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.

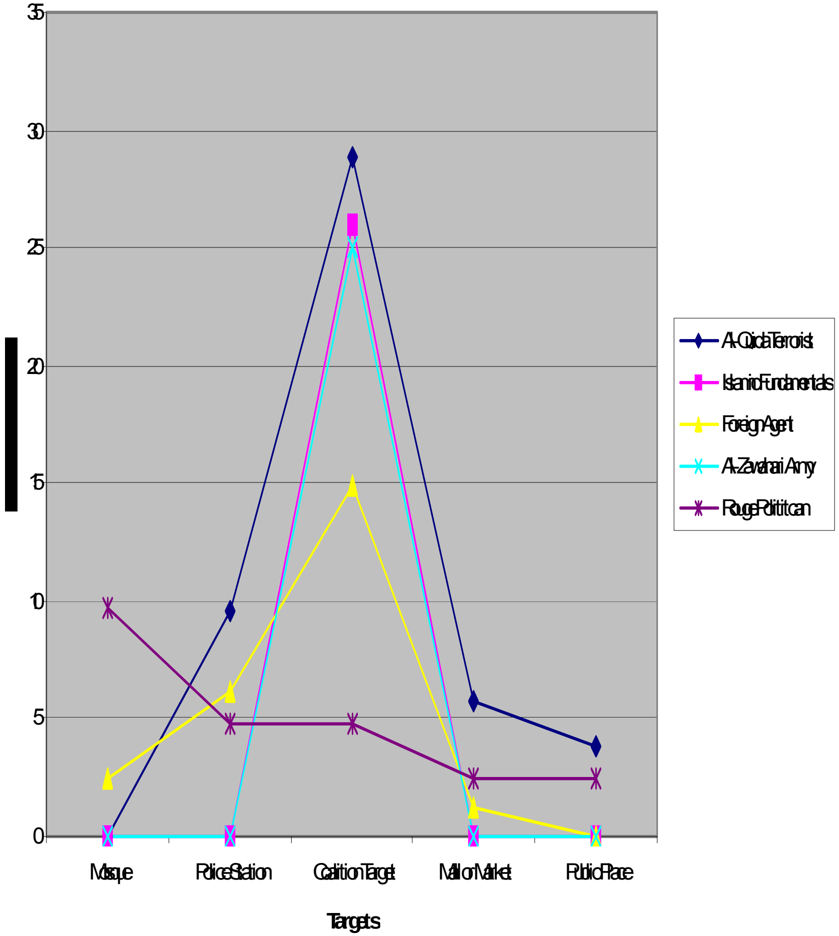
Ten different simulation experiments were conducted and the average results calculated on daily event basis (1440 minutes).

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

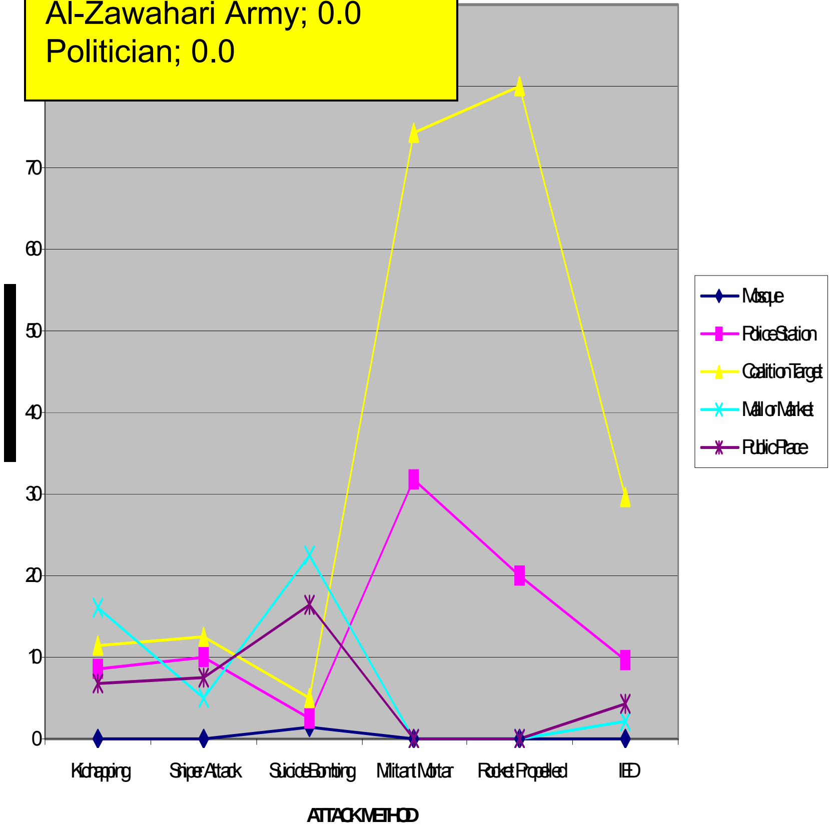


[redacted]

Sponsors & Targets

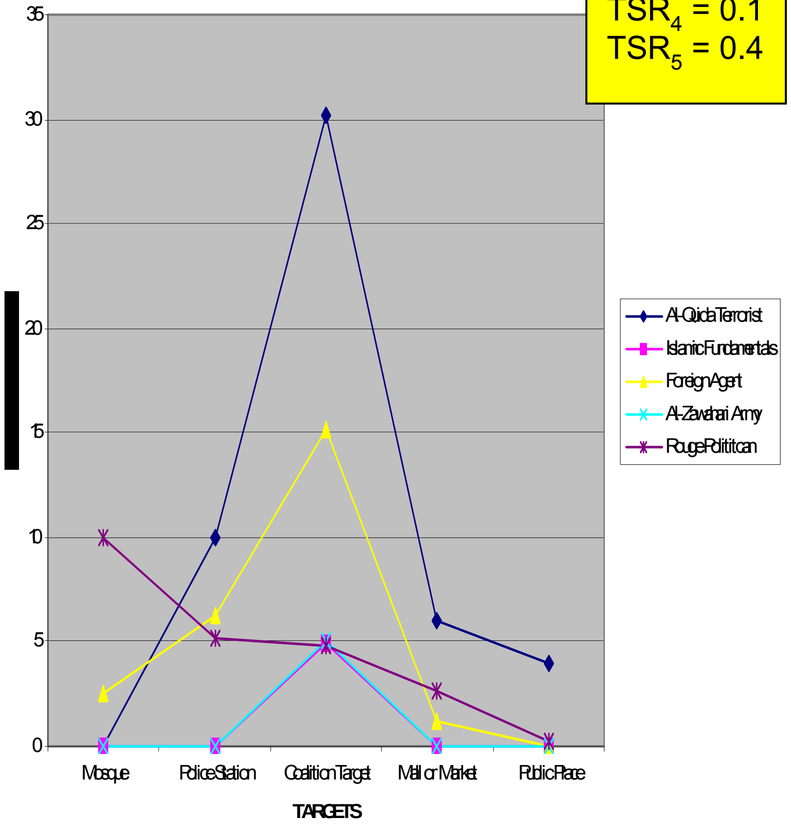
Results and Analysis: Rule 2-UnEqually weighted

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



Attack Method & Targets

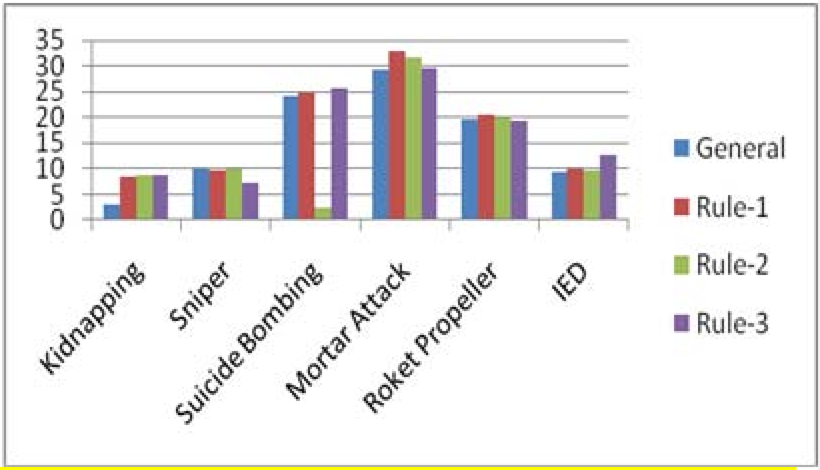
TSR_1 = 0.0
TSR_2 = 0.2
TSR_3 = 0.3
TSR_4 = 0.1
TSR_5 = 0.4



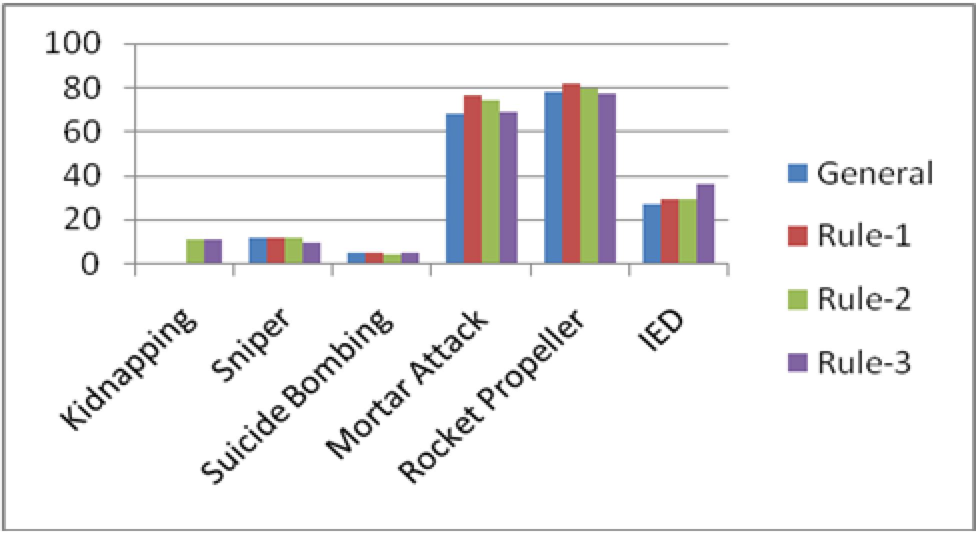
Sponsors & Targets

The Center for Human-Machine Studies

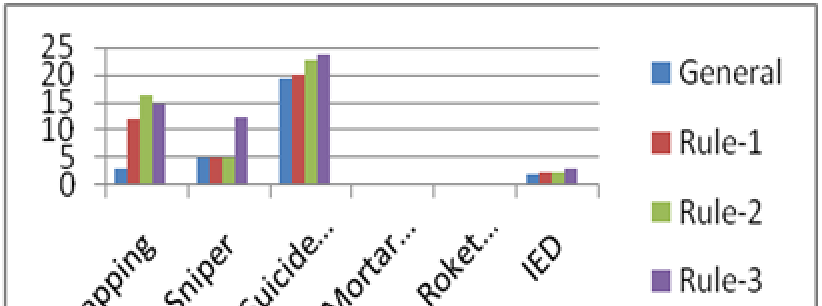
KNOWLEDGE DISCOVERY ANALYSIS—Insightful Statistics



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

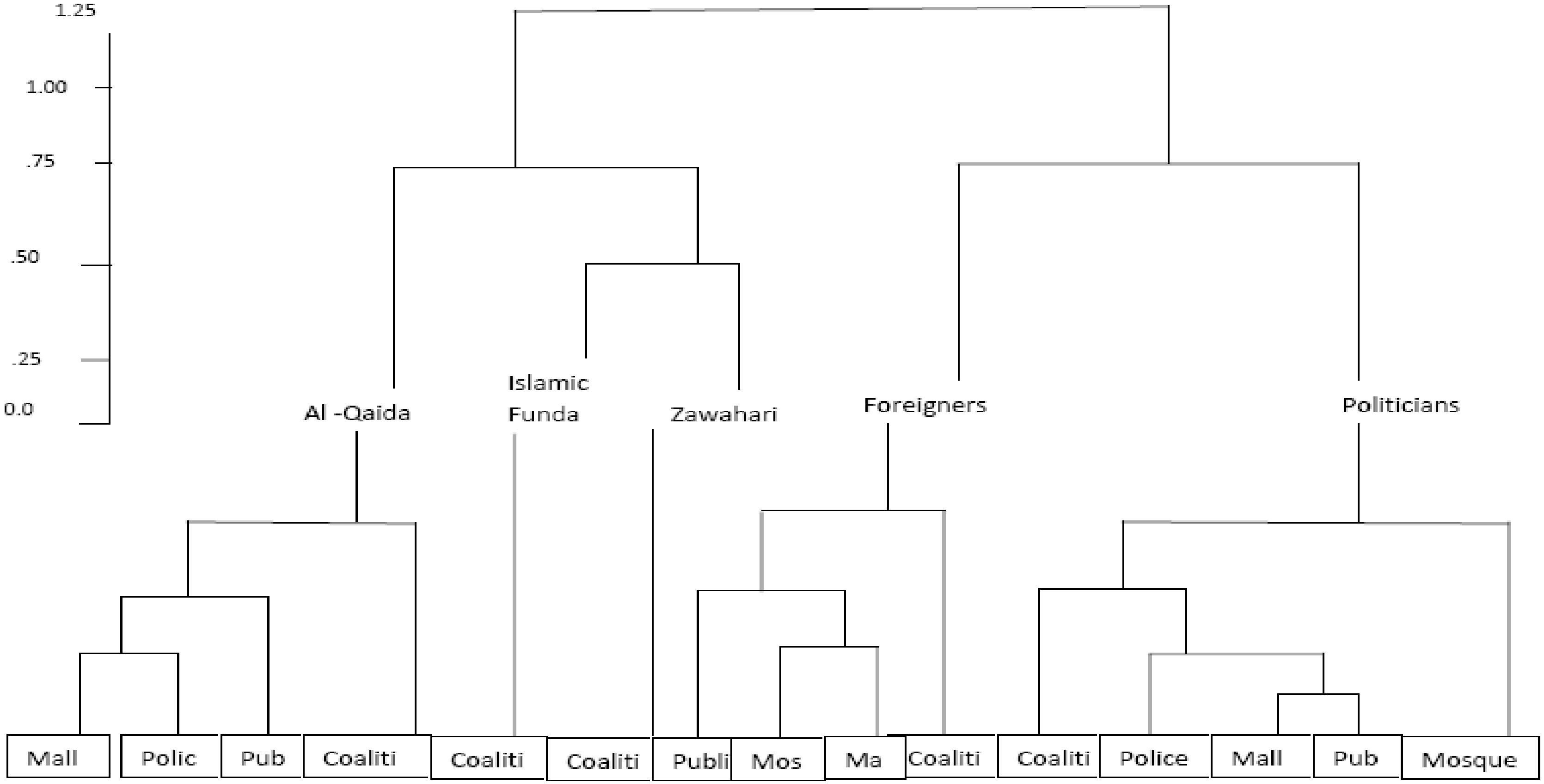
Percentage of targets attacked by each adversary in the network

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.