Evaluation of Organizational Designs with Network-Centric Philosophy

Celestine A. Ntuen, Ph.D
Distinguished University Professor
The Army Center for Human-Centric C2 Decision Making
ntuen@ncat.edu
http://gandalf.ncat.edu/ihms
+1-336-334-7780 (X531): phone
+1-336-334-7729: fax

Kim Gwang-Myung and Eui H. Park; co-authors

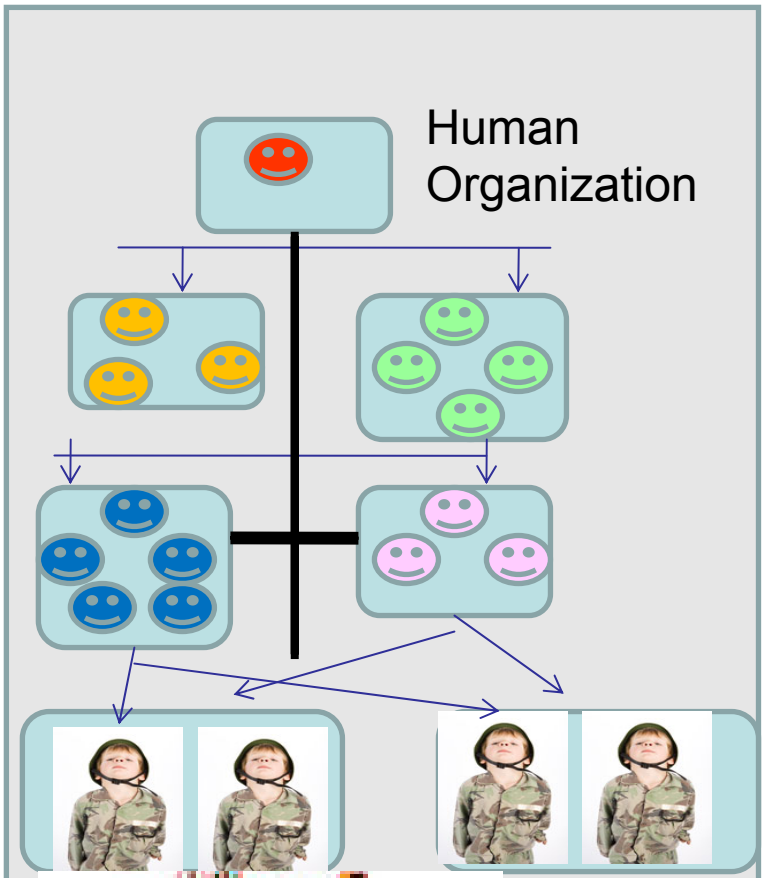
This project is supported by ARO grant #W911NF-04-2-0052 under Battle Center of Excellence initiative. The opinions presented here are not those from ARO, and are solely those of the authors.

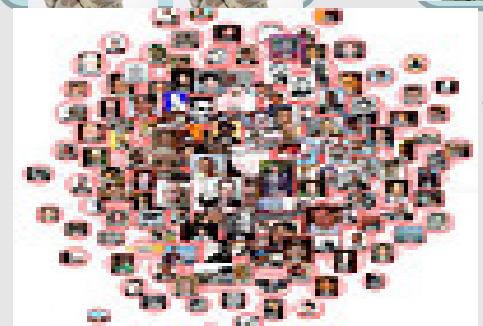
Presentation Outline

1. Introduction: A network view of organizations
2. Vulnerability of C2 networks
3. Selected types of organizational designs
4. Evaluation metrics and their heuristics
5. Computational model
6. Results and Summary

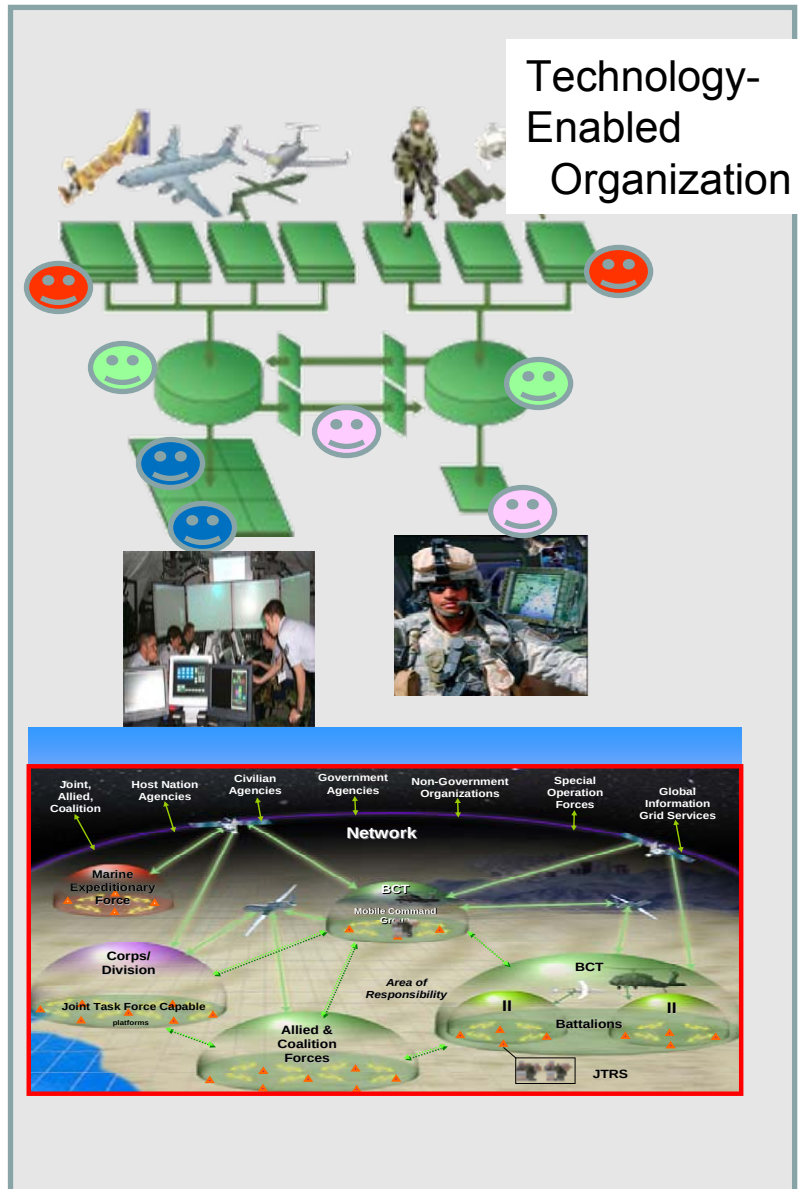
NORTH CAROLINA A&T STATE UNIVERSITY

A Network View of Organizations





Social Network



The Center for Human-Machine Studies

Some Characteristics of Network-centric Organizations

* Focused on expanding number of people / organizations reached
* Focused on expanding capacity of network to perform
* More attention paid to information sharing
* Values and rewards sharing of information
* Values social contact between staffs of partner organizations
* Values coordinated action over "leadership"
* Distributed power structure
* Power is pushed to the edge of the network
* Leverages and shares resources with partners
* Values cooperation, collaboration, redundancy and interaction.

A Brief on Network-Centric Organizations

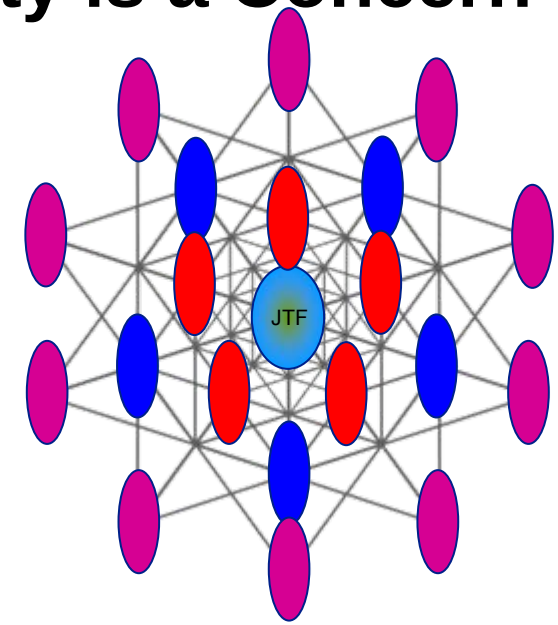
Technology has driving human social organizations to the information age:

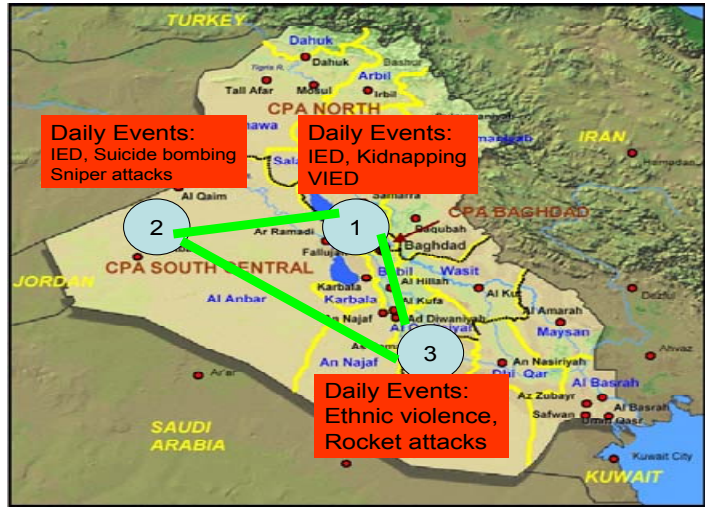
- The World has become a network of networks, filled with actors who behave in increasingly interconnected ways and with wide-reaching and rapid consequences.
- Complexity has evolved as a result of complicated seamless interactions.

A Brief on Network-Centric Organizations

- Information is the weapon for competitive advantage
  - Universal need-to-share
  - Changes in organizational structure
  - Adaptation to environmental changes
- Creates vulnerabilities:
  - Different scales and layers of organizational design
  - Speed of information flow

In the Military Domain, C2 Network Vulnerability is a Concern





1. Physical attacks on the command nodes; e.g., daily attack in tactical C2 elements in Iraq regions—leading to node agitations and instabilities.
2. Cyber attacks on information technology nodes:
   (a) Network failures and insecurities; (b) malicious “viruses”
3. Informational attacks through insertion of press propaganda.

The Center for Human-Machine Studies

In the Military Domain, C2 Network Vulnerability is a Concern

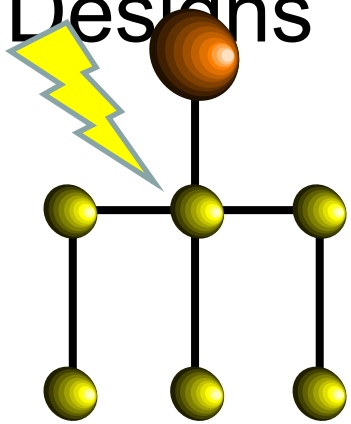
Current measures of network vulnerability consider:

1. hardware failures and reliability parameters.
2. dependability measures which assess availability and ease of maintenance
3. anecdotal use of subjective trust measures

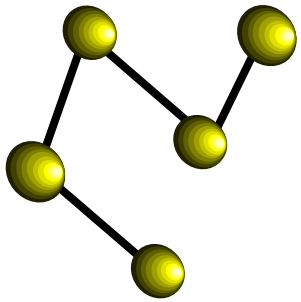
Must be considered:

1. Events that may likely destabilize the C2 nodes and elements.
2. Organization design and information flow structure.
3. Latent events (fog of war) such as deceptions and “worms” that crawl into the cyber network.

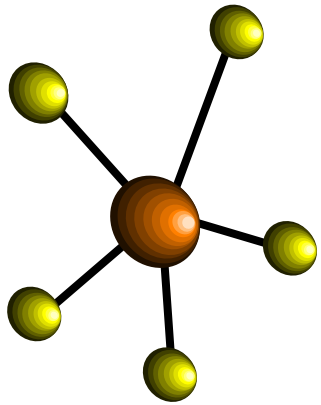
Selected Types of Organization Designs



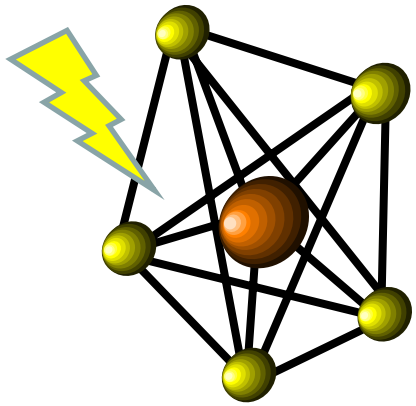
Standard Hierarchy (one Boss)



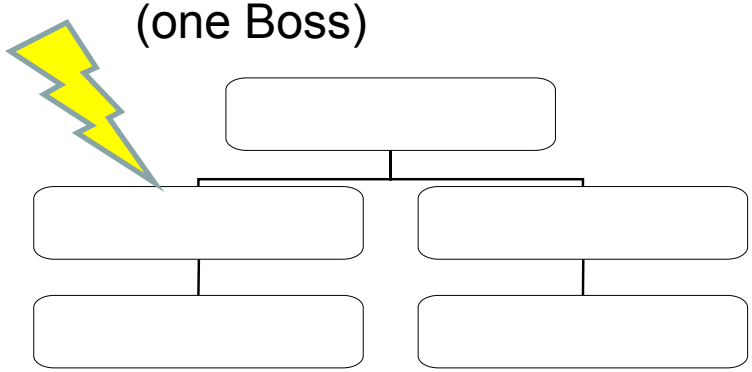
Chain Network



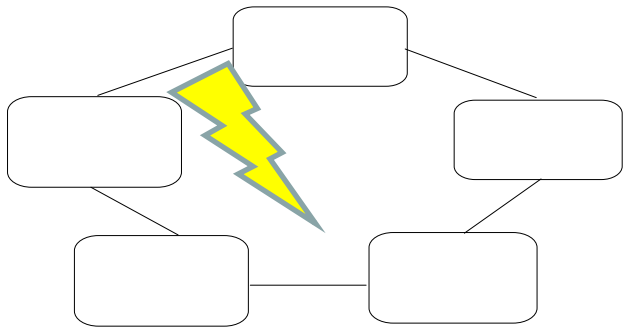
Hub & Spoke



All-Channel



Dual authority



Circle Network design

Considered for the study

Bolman & Deal, 2003

Evaluation Metric for Organization Design Comparison

Assumptions:

1. **An organization is driven by communication and information flows.**
2. **Information can be lost, degraded, misplaced, ‘ damaged’, etc.**
3. **The “boss” defines the context of the organization ‘self- informaton’ to the subordinates.**
4. **Surprisal or self entropy can be used to measure information lost in the system.**
5. **Higher entropy measure indicates the likehood of organization network vulnerability.**

Vulnerability as a Function of Information Surprisal.

- Shannon (1948) defined the term information entropy as a measure of randomness or "disorder" in a system.
- It tells us how much uncertainty there is.
- In 1961 Myron Tribus used the term surprisal to describe the "unpredictability of a single digit or letter" in a word.
- This assertion by Tribus was however an extension of Shannon's concept of information event or "entropy event" measured by $U = -\log_2 P$; where U is the measure of information content and P is the probability of event happening.
- Given a specific event occurrence, if all messages are certain, i.e., P is certain (P=1) for all events, then U =0

Vulnerability as a Function of Information Surprisal.

These are our assertions:

a). The decision of agents in an organization to attend to messages of instructions depend on the value of the message to the agent and the processing complexity involved. Although certain organizational designs may coerce the agent or allow freedom to choose, self perception of information value can best be described by its surprisal.

b). Given a one boss, e.g., the subordinate agent prefers to keep the amount of information or instruction from the boss uniform per instruction time and context.

Vulnerability as a Function of Information Surprisal.

These are our assertions:

c). Given that an agent in the organization interacts with several other agents through formal relationship, the agent would prefer information of higher value with less uncertainty.

d). We are not concerned with the level of uncertainty or entropy in the organization; rather, we seek to measure the information content processed by each node or agent in the network.

Evaluation Metric for Organization Design Comparison

(1)

Given this information, we can determine the level of node agitation defined by the intensity vector q_i defined in equation (1).

$$q_i = \left\{ \frac{\sum_{J=1}^{NE(i)} W_{ij} \; R_{ij}}{\sum^{NE(i)} W_{ij}} \right.$$

The probability p_i and the intensity q_i for the network is combined by using a sigmoid threshold function to realize the overall strength of the agitation. This is defined by equation (2).

$$a_i = (1 + e^{-q_i * p_i})^{-1} \qquad (2)$$

The Center for Human-Machine Studies

Evaluation Metric for Organization Design Comparison

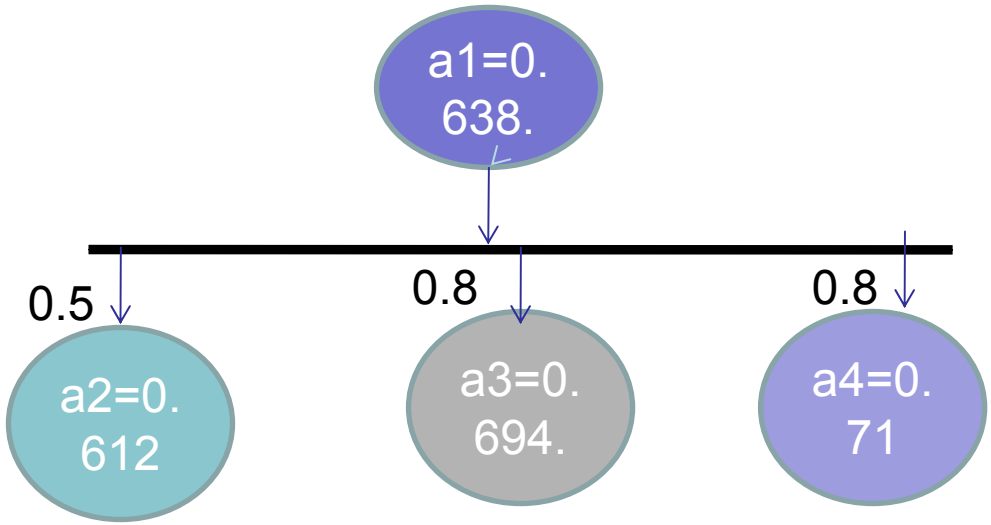
One Boss Analysis

We scale all the influence or authority scores such that their sum =1 (in probability sense). Then, we calculate the edge weights in the network by

$$e_{ij} = a_i * a_j * b^*_{ij} \quad (3)$$

where e_{ij} is the edge weight between parent i and child j; b^*_{ij} is scaled probabilistic influence. We then calculate the average network weight, W by

$$W = (1/N)\sum_{i=1}^{N}\sum_{j=2}^{n(i)} eij$$



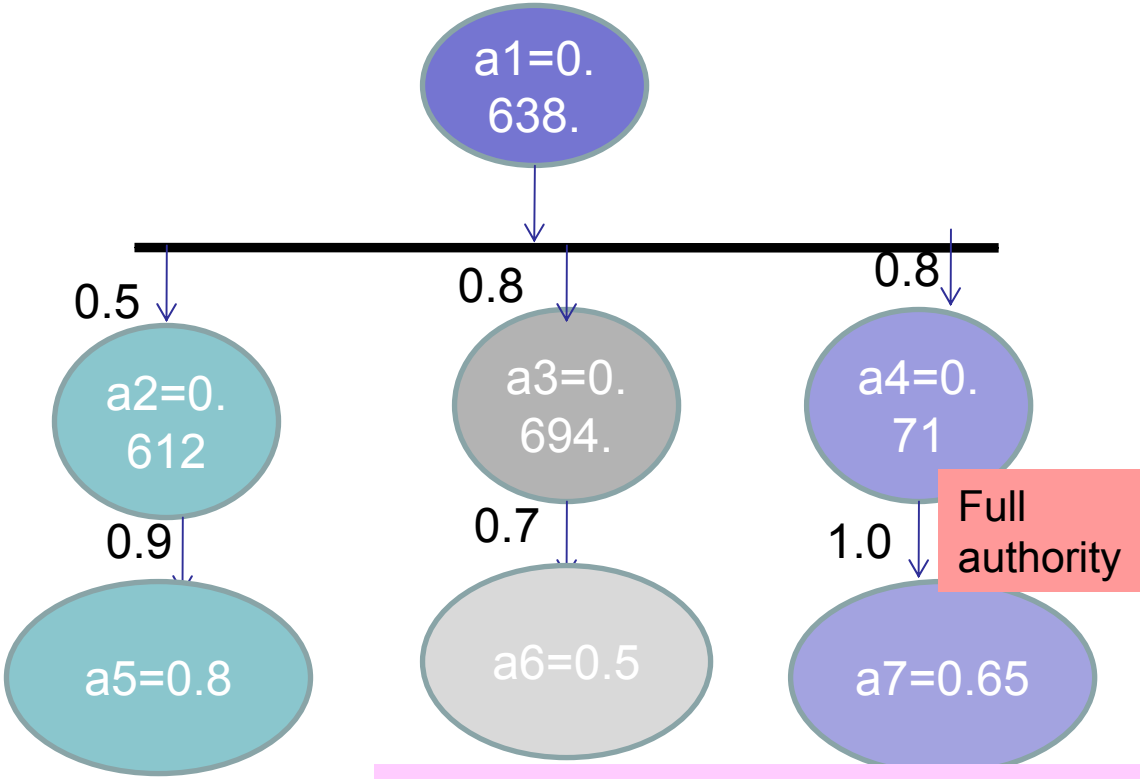
	1	2	3	4
1		0.5	0.8	0.8
2				
3				
4				

Information surprisal score, h_k $= \log_2\left(1/W\right)$

Evaluation Metric for Organization Design Comparison

Dual Authority

- Needs to account for percentage of authority retained by immediate boss. E.g., in the diagram, 10% of node 2 control of node 5 is maintained by the main boss at node 1. the influence of node 1 to 2 becomes by
- $b_{12} = (1+ (1-b_{25}))*b_{12} = (1+ (1-0.9))*0.5 = 0.55$
- Apply same logic as one boss case to calculate the path weight



This procedure is repeated for all the edges to obtain the middle authority weight vector **m** = (b_{12}, b_{13}, b_{14}) = (0.55, 1.04, 0.8). **m*** = (0.23, 0.44, 0.33: scaled to 1.

Extended path weight, and the average network weight and surprisal using equations 3-5. For example $e_{125} = a_{1*}m^*_{12}*a_2*b_{25}*a_5$ =(0.638*0.23*0.612*0.9*0.8) = 0.0647; W = 0.076; h_2 = 3.718.

The Center for Human-Machine Studies

Evaluation Metric for Organization Design Comparison

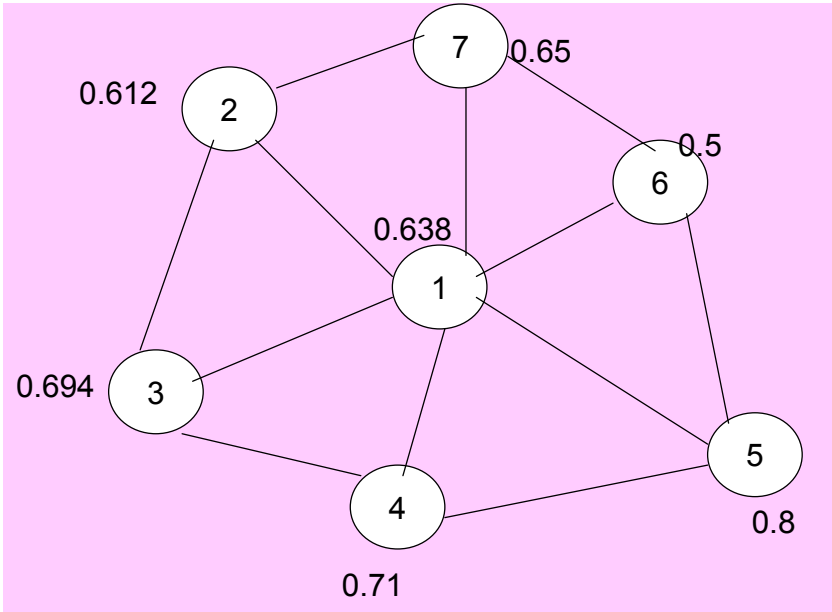
Circle Network

•Calculate the edge relationship: $e_{ij} = a_i * a_j$

Calculate the surprisal of the entire network due to interactions between nodes, h_e

•Calculate the surprisal of the network due to node authority, h_n

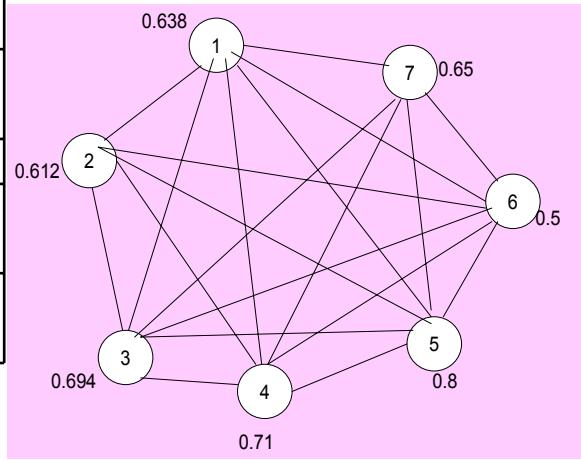
The design surprisal score is $h = h_e - h_n$



The Center for Human-Machine Studies

Evaluation Metric for Organization Design Comparison

	1	2	3	4	5	6	7	Row average
1	0	0.0.389	0.443	0.453	0.51	0.319	0.415	0.4215
2	0.389	0	0.425	0.435	0.4896	0.306	0.3978	0.407
3	0.443	0.425	0	0.493	0.555	0.347	0.451	0.4525
4	0.453	0.435	0.493	0	0.568	0.355	0.4615	0.4609
5	0.51	0.4896	0.555	0.568	0	0.4	0.52	0.5071
6	0.319	0.306	0347	0.355	0.4	0	0.325	0.342
7	0.415	0.3978	0.451	0.4615	0.52	0.325	0	0.4284
Average								0.4313



Channel star network

•Same method as circle Network design, except in eij, i ≠ j; in which case, we set the value to 0 in the matrix).

Computational Implementation

Visual Basic and Excel Spreadsheet

ICCRTS-176 Evaluation Military Organizational - Microsoft Word

organdesigninput - Notepad

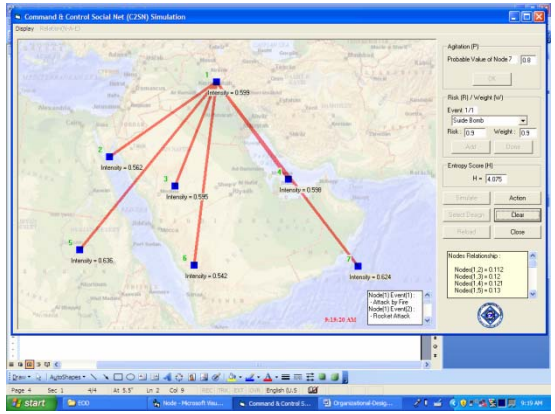
Vulnerability Matrix :

0.60	0.11	0.12	0.12	0.13	0.11	0.13
0.00	0.56	0.11	0.11	0.12	0.10	0.12
0.00	0.00	0.60	0.12	0.13	0.11	0.13
0.00	0.00	0.00	0.60	0.13	0.11	0.13
0.00	0.00	0.00	0.00	0.64	0.12	0.14
0.00	0.00	0.00	0.00	0.00	0.54	0.11
0.00	0.00	0.00	0.00	0.00	0.00	0.62

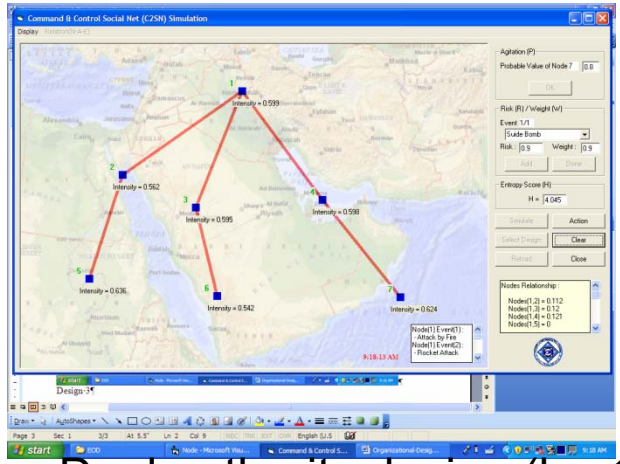
Output :

Node	No. of Events	Risk	Weight	Prob. of Attack	Node Intensity
1	2	0.50 0.70	0.60 0.80	0.80	0.599
2	1	0.50	0.70	0.50	0.562
3	1	0.70	0.40	0.70	0.595
4	4	0.20 0.40 0.50 0.80	0.30 0.20 0.50 0.70	0.80	0.598
5	1	0.90	0.90	0.90	0.636
6	2	0.30 0.70	0.60 0.70	0.30	0.542
7	1	0.90	0.90	0.80	0.624

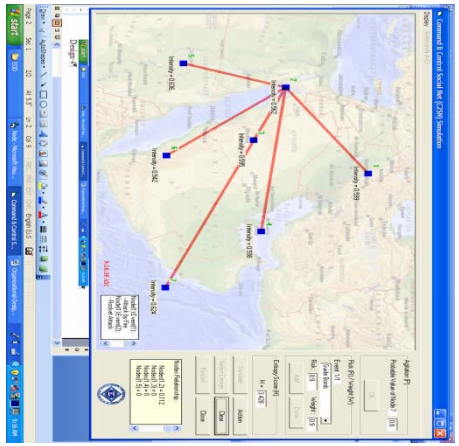
Computational Evaluation



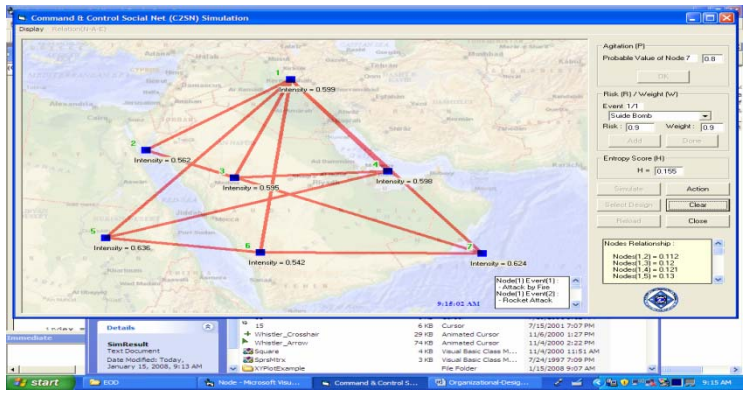
One boss design (h =2.857)



Dual authority design (h =1.94)

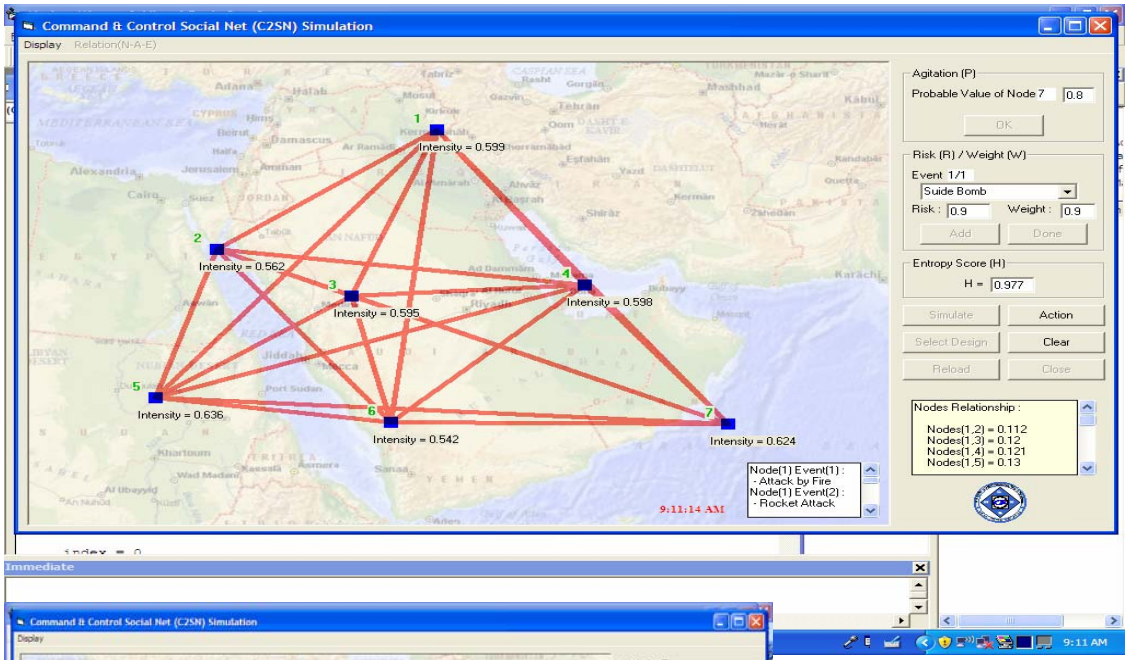


Simple hierarchy design (h =1.91)

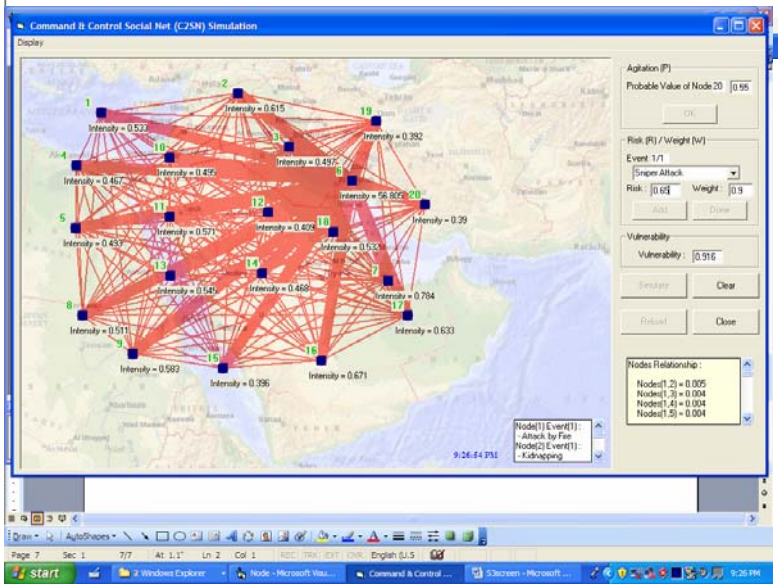


Circle Network design (h = 0.6418)

Computational Evaluation



All-channel design(h =0.609)

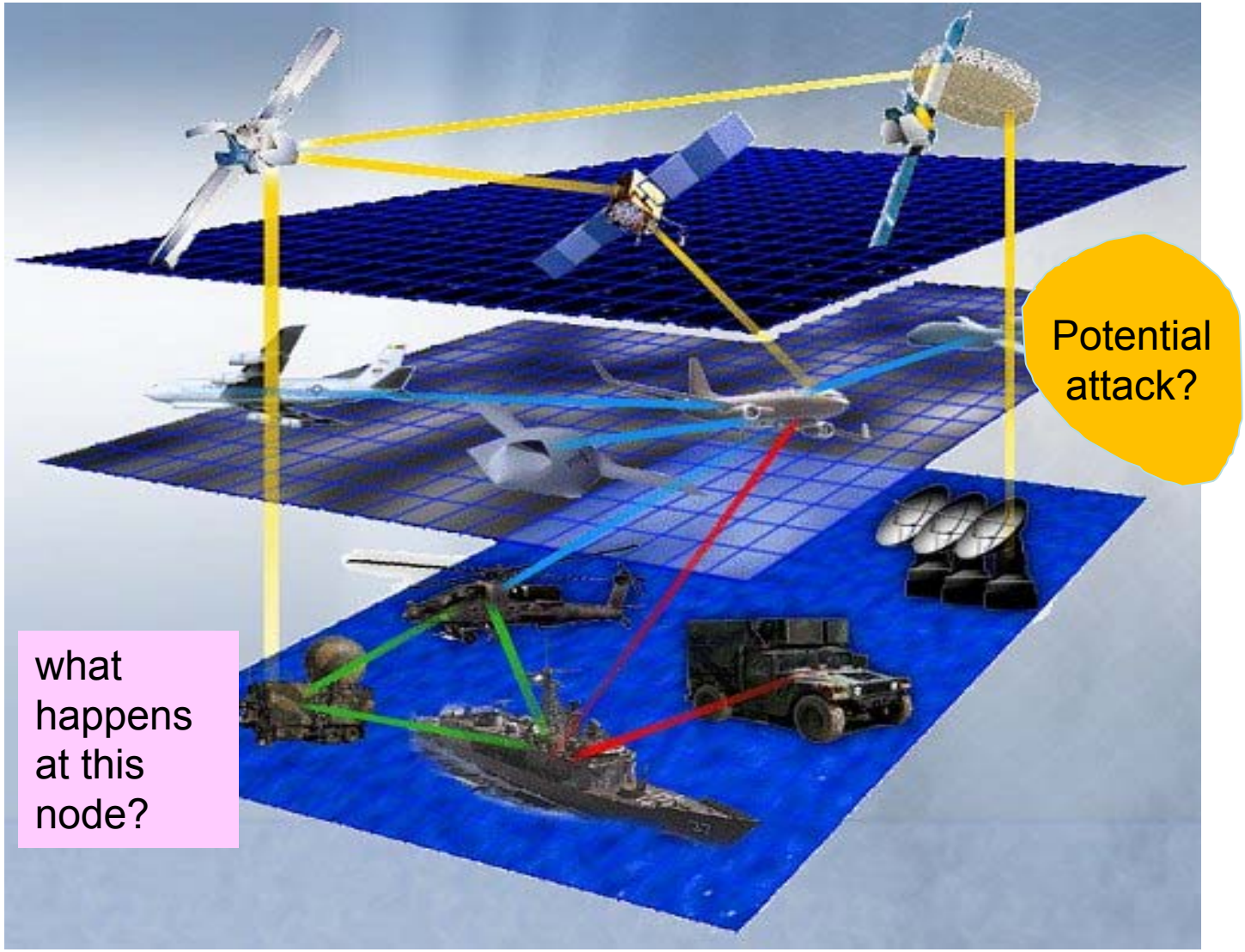


Generic, arbitrary network design with n-nodes

Summary and Results

- It is important to understand the level of agitation and vulnerability caused by probabilistic events in the network-centric organizations.
- Our results are promising; and can be extended to dynamic network risk assessment, latent semantic network evaluation, and reliability of network-centric C2 based on tactical events

Summary and Results



Summary and Results

Observations:

This nascent model has some short comings that need further research.

(1)We need to improve on the user interface;
(2) We need to add dynamic databases to capture time-based input events;
(3) We need to make the network simulation dynamic based on spatio-temporal events—that is learn its behaviors from dynamic input sourced from multiple databases; and
(4) Investigate the use of robust analytical models, such as chaos theory, complexity theory, information theory, or neural network model to control the adaptive behaviors of the network and its node dynamics.