

**13th International Command & Control Research and Technology Symposium
C2 for Complex Endeavors**

Evaluation of Organizational Designs with Network-Centric Philosophy

Celestine A. Ntuen, Kim Gwang-Myung and Eui H. Park
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: 336-334-7780; Fax: 336-334-7729
Email: Ntuen@ncat.edu

Topical Areas: (3) Modeling and Simulation; (5) Organizational Issues; (6) C2 Assessment Tools and Metrics

Abstract: The concept of network-centric warfare (NCW) is an evolving construct that has altered the military organizational landscapes. In the asymmetric information domains, there are few studies that actually relate the daily agitations of each of the command centers to the vulnerability of the entire C2 structure. In addition, there are no existing studies that use daily events and incidents to understand the vulnerabilities of each organizational structure. This paper reports on the use of network and organizational theories to derive vulnerabilities of organizational structures based on probabilistic events on each C2 center. Vulnerability is calculated as a function of information surprisal. The results of an empirical study comparing organizational structure designs in terms of vulnerabilities are presented.

INTRODUCTION

An organization is a group of people intentionally brought together to accomplish an overall, common goal or a set of goals. Organizations can range in size from two to tens of thousands. One of the common ways to look at organizations is social systems (McNamara, 2005). Self-organizing networks show signs of high efficiency, but more thorough experimentation in larger numbers is needed to valid the results (ELICIT, 2006).

Command and Control in the 21st century is characterized by a design transformation from a hierarchical industrial age C2 to networked information age C2 concepts. While a requisite information infrastructure is widely recognized as enabler of networked C2, the use of information on events that perturb the overall system performance has been understudied¹. The authors argue that knowledge of how and to what degree daily events in Iraq and Afghanistan contribute to C2 network vulnerability is indispensable information for designing future C2 networks. Here is a simple rationale to this observation: A typical battlefield system is populated by at least two command and control (C2) centers. Each center is responsible for conducting the affairs of the designated area of interest. For the C2 centers to interoperate, information exchange is

¹ Carley, K.M & Lin, Z. (1997) A theoretical study of organizational performance under information distortion. *Management Science*, 43(7), 976-997.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JUN 2008		2. REPORT TYPE		3. DATES COVERED 00-00-2008 to 00-00-2008	
4. TITLE AND SUBTITLE Evaluation of Organizational Designs with Network-Centric Philosophy				5a. CONTRACT NUMBER	
				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, The Institute for Human-Machine Studies, 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 13th International Command and Control Research and Technology Symposia (ICCRTS 2008), 17-19 Jun 2008, Seattle, WA					
14. ABSTRACT The concept of network-centric warfare (NCW) is an evolving construct that has altered the military organizational landscapes. In the asymmetric information domains, there are few studies that actually relate the daily agitations of each of the command centers to the vulnerability of the entire C2 structure. In addition, there are no existing studies that use daily events and incidents to understand the vulnerabilities of each organizational structure. This paper reports on the use of network and organizational theories to derive vulnerabilities of organizational structures based on probabilistic events on each C2 center. Vulnerability is calculated as a function of information surprisal. The results of an empirical study comparing organizational structure designs in terms of vulnerabilities are presented.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 37	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

necessary. Interoperability implies the existence of diverse systems. Each C2 center is vulnerable to enemy attack in various dimensions. For this reason, there are many possibilities of information and communication loss. This is often measured in terms of entropy.² Another measure related to entropy is self information which has the content of information associated with one or many interacting system units. The amount of self-information contained in a probabilistic event depends only on the probability of that event. In the current conflict in Iraq, Bagdad command, e.g., is experiencing myriads of attacks on daily basis—kidnapping, suicide bombing, IED attacks, etc. These attacks are responsible for the agitation of the C2 centers—generating elements of nervousness, increase or decrease in communication activities with other C2 centers in the Iraq sectors of war, and so on. These events occur probabilistically. Threat mitigation is then the sole responsible of C2 centers.

It is the objective of the USA military to make network-centric C2 resilient and agile. But to accomplish this, many engineering metrics of performance must be implanted into the system during design and operation phases. Among such metrics are reliability, dependability, and vulnerability. The latest is the main concern of this paper

C2 NETWORK VULNERABILITY

Vulnerability analysis of military command and control (C2) systems is an increasingly important field of study as awareness grows of the leverage that information operations can provide in adversarial conflicts. However, there are many kinds of vulnerability analyses and which one is appropriate for a given C2 situation is not always obvious. Here, a metric for C2 network system vulnerability is developed based on elemental adversary events that agitate individual C2 nodes thereby causing the entire C2 network to increase in its vulnerability, leading to possible failure. Figure 1 illustrates the aspects of agitation in three different C2 centers in Iraq.

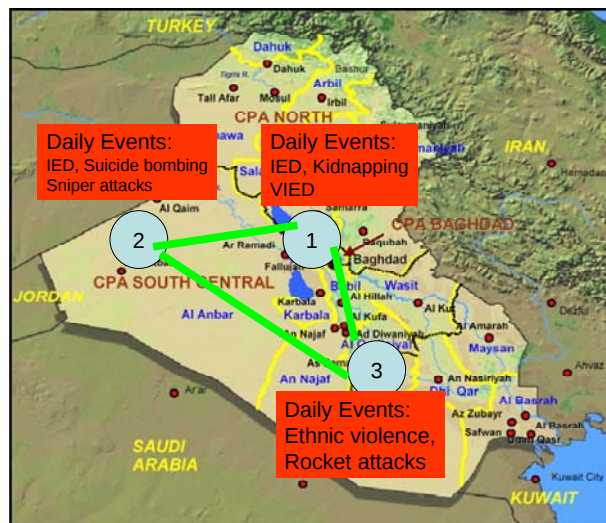


Figure 1. An illustration of a three node C2 network in Iraq

² Shannon, C.E & Weaver, W. (1969). The mathematical theory of communication. Urban, Illinois: The University of Illinois Press.

Vulnerability analysis of complex military systems with human elements has several levels: (a) Determination of critical nodes, subsystems, components, and links; (b) Evaluation of subsystem or component dysfunction modes; and (c) Evaluation of C2 support network reliability and dependability. In the physical (hardware) communication network, critical nodes are assessed by evaluating the reliability of the components, which by itself is a function of failure (due to design faults or adversary incursions)—this is relevant to levels (a) & (b) above. In evaluating reliability and dependability, network analysts are often concerned with determining the “optimum” conditions of the physical components that will yield the intended reliability or dependability factor—including intangibles like support systems such as spare parts and maintainability. When the human is considered a significant part of the network, the critical factors are the critical events in the battlefield that cause the human elements to be equally vulnerable—inducing stress, fatigue, and perhaps a failure to deploy the necessary communication and information infrastructures. We need a new definition and metric of vulnerability to account for these critical events in C2 operations. First, the level of agitation of a C2 node in the battle system must be understood. Second, a method to aggregate the individual information of each node agitation must be derived. Currently, there is no model that addresses this problem. The reason is simply, most analysis is focused on telecommunication network infrastructures³. In telecommunication network, functionality measures are based on considering a number of issues such as the number of alternate paths, path lengths, path type, and number of routers. From the organization design perspective, information loss due to attack on a system is a major indicator of vulnerability.

ORGANIZATIONAL DESIGNS

To illustrate our concepts of surprisal as a measure of vulnerability, several basic structural configurations are identified: one boss, dual authority, simple hierarchy, circle, and all-channel network (Bolman & Deal, 2003). In the one boss design (Figure 2); one person has authority over others; leading to bureaucracy and often delayed information flows between and across members in the organization.

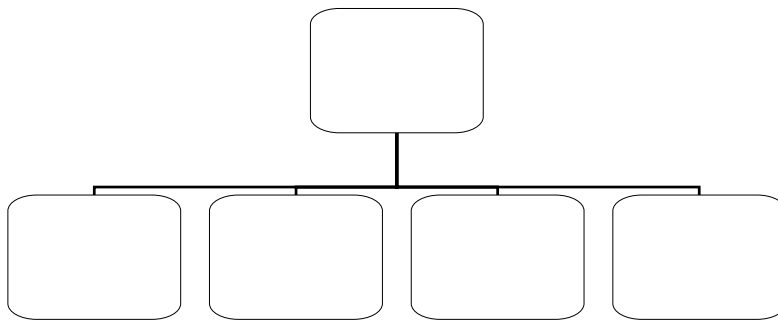


Figure 2. One Boss Design (Adapted from Bolman & Deal, 2003)

³ Gateau, J.B, et al. (2006). Hypothesis testing of edge organizations: Modeling the C2 organization design space. 12th ICCRTS, Newport, RI.

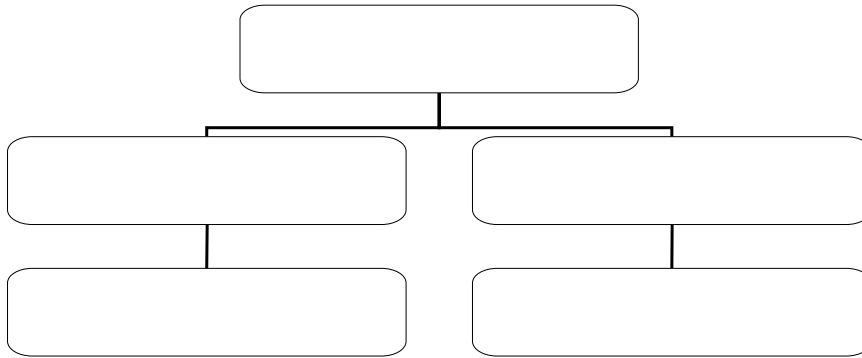


Figure 3. Dual Authority Design (Adapted from Bolman & Deal, 2003)

The dual authority design (Figure 3) creates a management level below the leader and two individuals are given authority over a specified area of the team's work. Information and decisions flow through them. Usually this arrangement is feasible when a task is divisible. This arrangement allows for the person in charge to focus more effort on strategy or relationships with higher authority. With the addition of a new layer of management, limitations occur with accessibility to communicate between lower levels to the boss and may eventually lower morale and performance. The additional layers also make communication slower.

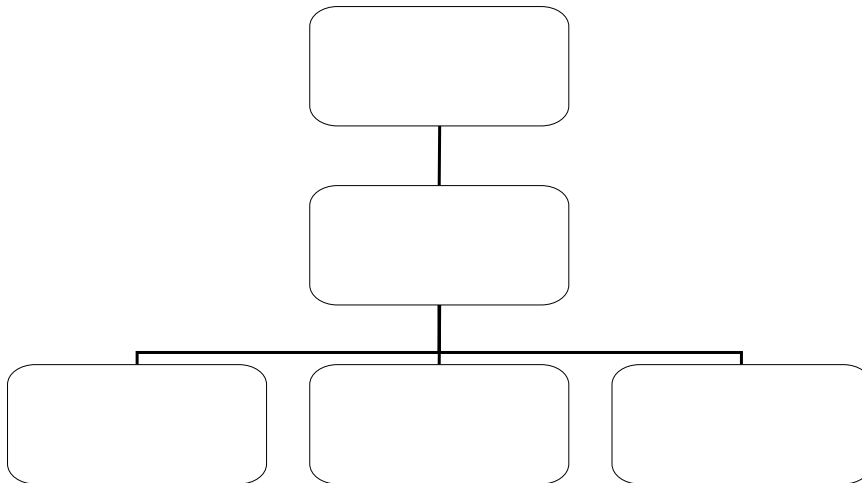


Figure 4. Simple Hierarchy (Adapted from Bolman & Deal, 2003)

The simple hierarchy has a middle manager who reports to the leader and supervised and communicates with others (Figure 4). This type of structure is used by the government (e.g. The White House). It tends to free the leader to focus on mission and external relations and leaves operational details to the manager. This structure like the dual authority design limits access to the top, but can be more efficient. This can cause conflict between the manager and the person in charge because the manager may want to take the leader's position.

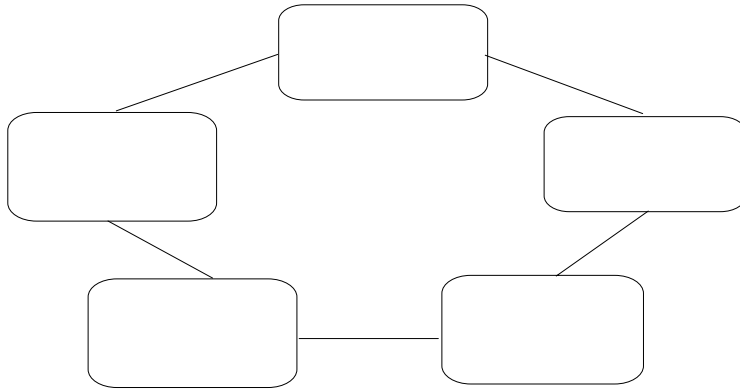


Figure 5. Circle Network Design (Adapted from Bolman & Deal, 2003)

Another option is a circle network, where information and decisions flow sequentially from one group member to another (Figure 6). In this structure each member can modify what comes to them. Communication is simplified and each member only has to deal with two others which make transactions either to manage. In this structure a weak link can undermine the entire team and complex tasks that require more reciprocity can hinder team performance. Within this design managers can come and go without seriously disrupting the team's ability to function and members of the team can be transferred from one team to another with relative ease. A new member can carry out responsibilities without significant adjustment.

The all channel or star network (Figure 6) creates multiple connections so that each person can talk to anyone else. There is free flow of information and decisions require interacting with multiple agents within the network. The arrangement usually works well if a task is unstructured or complicated, but it is slow and inefficient for a simpler task. The structure also works best when team members are willing to participate, embrace diversity, manage conflict, have well developed communication skills, and can tolerate ambiguity.

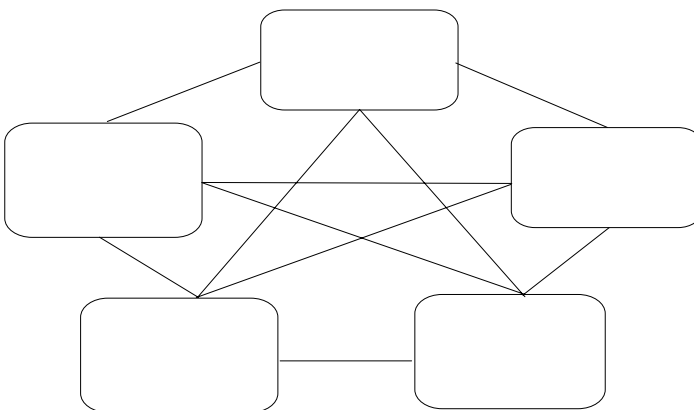


Figure 6. All Channel (Star) Network (Adapted from Bolman & Deal, 2003)
their work, subordinates usually become frustrated.

METRICS FOR EVALUATING ORGANIZATIONAL STRUCTURE VULNERABILITY

The main hypothesis is that given a set of nodal events that agitate a system, the overall vulnerabilities of each of the organizational designs are different. Information surprisal is used to assess the vulnerability of an organizational design as a function of information loss in the organizational system. The reasoning is as follows: For each design topology, an expert probability estimate that assesses the likelihood of command agitation is given by p_i , where i is an index for design type ($i=1, 2, \dots$). Each C2 center (a node in the command network) is subject to attack, denoted by number of events (NE), e.g., rocket attack, IED attack, kidnapping, sniper attack, suicide bombers, militia attacks, etc.; each attack has some level of risk and a weighting function that determine the cost of risk. In addition, each node, based on expert estimates, carries estimated initial probability of attack (p). Given this information, we can determine the level of node agitation defined by the intensity vector q_i defined in equation (1).

$$q_i = \left\{ \frac{\sum_{j=1}^{NE(i)} W_{ij} R_{ij}}{\sum_{j=1}^{NE(i)} W_{ij}} \right\} \quad (1)$$

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).

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

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. It was not until 1961 that 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. Tribus observed that the surprisal quantity allows us to measure how surprised you are for a given instant of an event. Given a specific event occurrence, if all messages are certain, i.e., P is certain ($P=1$) for all events, then $U=0$; a condition that is rare in systems that produce and process information. Other terms have been used, for example, relative or mutual entropy, or mutual information (Reza, 1991).

The extension of surprisal models to organizational information management is rare. However, the use of entropy, the average surprisal as defined by Shannon () are ubiquitous. We are interested in surprisal because of the context of information analyses that we encounter. 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.

c). Given 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 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.

It is surmised that the use of surprisal as a metric to study organizational design might help to convey local based quantitative information on how interactions are perceived by the organizational entities. For example, one may desire to reduce the surprisal of information loss between at least two entities which may be caused by many factors, such as equivocation, information ambiguity, or modality of information conveyance.

Network Vulnerability Score

Algorithms based on information surprisal and event probabilities are derived for each design topology. For each topology, a relationship table that contains information on the strength of authority or command directives is defined by b_{ij} (where j reports to i). For example in the one boss structure in the figure below, Table 1 is used.

In the figure to the right, we assume the values of a_i ($i=1,..4$). Node a_1 is the parent node, and nodes 2,3,4 receive directives from node a_1 . Here, node 2 receives directives from a_1 , 50% of the time, a_2 , 80%, and a_4 , 80%.

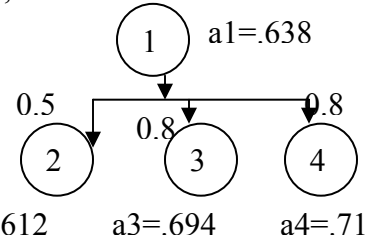


Table 1. Sample command relationship strengths

	1	2	3	4
1		0.5	0.8	0.8
2				
3				
4				

For the one boss design, assume b_{ij} ($i \neq j$), we scale all the influence or authority scores such that their sum is 1 (in probability sense). Then, we calculate the edge weights in the network by

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

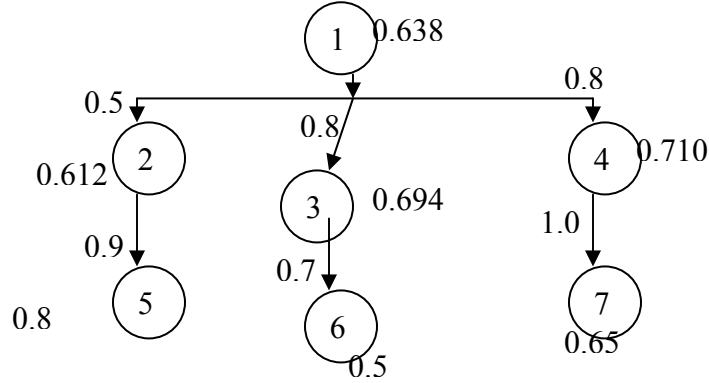
where e_{ij} is the edge weight between parent i and child j ; b^*_{ij} is scaled probabilistic influence. We then calculate the average network weight, W by

$$W = (1/N) \sum_{i=1}^N \sum_{j=2}^{n(i)} e_{ij} \text{-----} (4)$$

N = number of nodes in the network, $n(i)$ is the number of children of node i , the information surprisal score, h for design type k is defined by

$$h_k = \log_2 \left(\frac{1}{W} \right) \quad (5)$$

In the dual authority design, we have to account for the percentage of authority retained by the boss. We shall use the figure below to illustrate this.



Consider the influence $b_{25} = 0.9$; the extra 10% authority is the influence of command of node 1 on node 5. Thus, the we need to scale the effective influence of node 1 on node 2 by taking into consideration the 10% of influence of node 1 on node 5. This is calculated by $b_{12} = (1 + (1 - b_{25})) * b_{12} = (1 + (1 - 0.9)) * 0.5 = 0.55$. This procedure is repeated for all the edges to obtain the middle authority weight vector $\mathbf{m} = (b_{12}, b_{13}, b_{14}) = (0.55, 1.04, 0.8)$. The next step is to scale $\mathbf{m}$ vector to sum to 1 in probability sense. This gives $\mathbf{m}^* = (0.23, 0.44, 0.33)$. We apply the same logic as in the one boss design to calculate the extended path weight, and the average network weight and its surprisal using equations 3-5. For example $e_{125} = a_1 * m^*_{12} * a_2 * b_{25} * a_5 = (0.638 * 0.23 * 0.612 * 0.9 * 0.8) = 0.0647$; $W = 0.076$; $h_2 = 3.718$. We apply the same logic in design 2 above to a simple hierarchy design in Figure 4. The algorithm for circle network design (Figure 5) and all channel star design (Figure 6) are similar and use a different logic. Exhibits 1 and 2 below are used to illustrate the calculations. In the circle network, each edge score is calculated by equation 6.

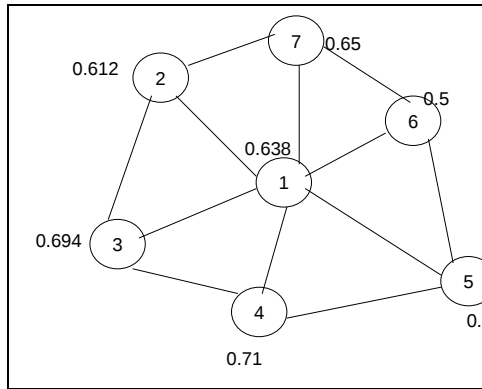


Exhibit 2 Circle network

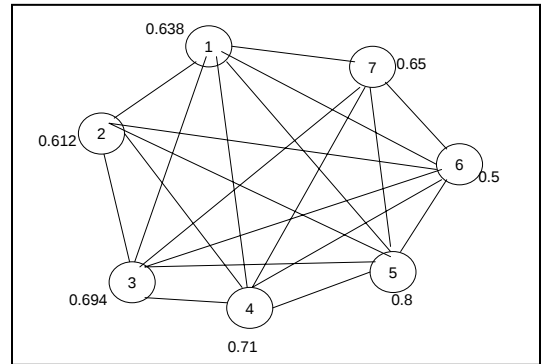


Exhibit 3. Channel star

$$e_{ij} = a_i * a_j \quad (6)$$

Equations 4 and 5 are applied to calculate the surprisal of the network; the surprisal is determined by the different between the surprisal from interaction and the surprisal from node agitations; i.e.,

$$h = h_e - h_n \quad (7)$$

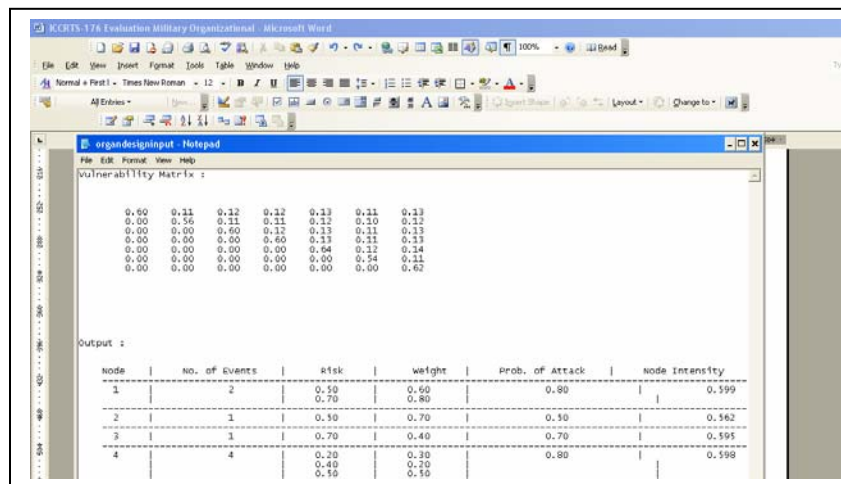
where h_e is the surprisal due to interaction effect and h_n is the surprisal due to node agitations. In Exhibit 3, the channel star design has no central command. Here we create a symmetric confusion (a sort of energy dissipation) matrix and calculate the average weighted event probability whose value is use to calculate h_e . The elements of the matrix is calculated from equation 6 above (except $i \neq j$; in which case, we set the value to 0 in the matrix). Table 2 show sample matrix values and the average row values.

Table 2. Sample interaction matrix for channel star design.

	1	2	3	4	5	6	7	Row average
1	0	0.0389	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	0.347	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

SAMPLE SIMULATION RESULTS

We have implemented the computation as an interactive program, allowing the user to choose the number of nodes in the network and the type of organizational structure desired. Exhibit 4- shows sample input date for a network with 7 nodes, including the relevant information on the node.



The screenshot shows a software window titled "organizationalinput Notepad" with a menu bar (File, Edit, Format, View, Help). The main area displays a "Vulnerability Matrix" and an "Output" table.

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	0.50	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	0.14	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	0.80	0.80	0.599
2	1	0.10	0.70	0.10	0.162
3	3	0.70	0.40	0.70	0.595
4	4	0.20	0.30	0.80	0.598
		0.40	0.10		
		0.10	0.10		

Exhibit 4. Sample input screen

Sample simulation results for each design topology are shown in Exhibits 5-8 below.

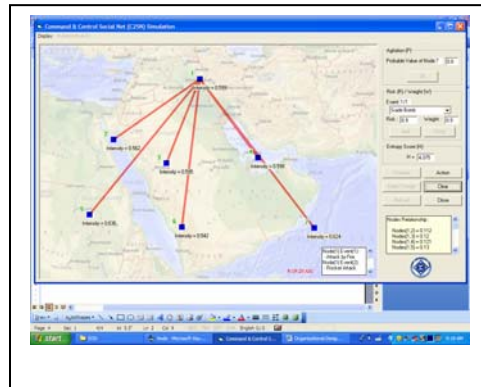
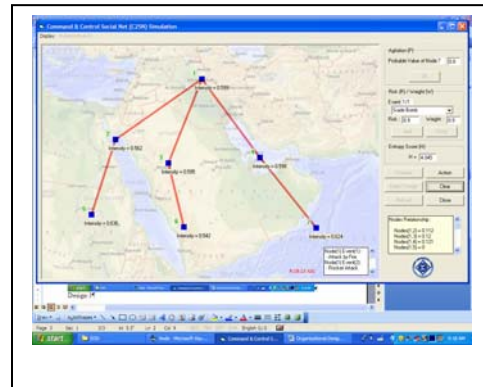


Exhibit 5. One boss design ($h=2.857$)



Dual authority design ($h=1.94$)

Based primarily on the input used for this validation analysis, the one boss design tends to have higher information surprisal (a value of 2.86). This may be attributed to the rigid authority concentrated on one command node. Both the dual authority and simple hierarchy design did not show any significant difference (with values of 1.94 and 1.91, respectively). All channel design showed a marginal gain above circle network design.

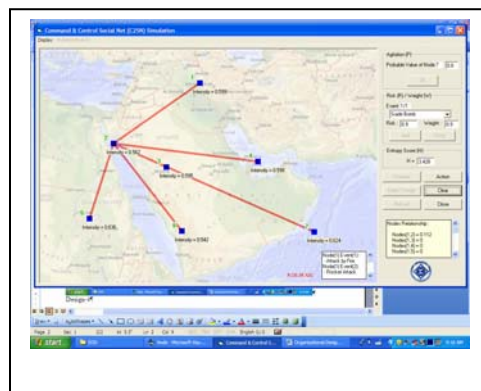


Exhibit 6. Simple hierarchy ($h=1.91$)

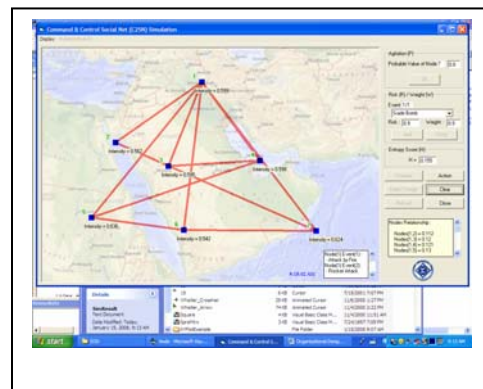


Exhibit 7. Circle network ($h=0.6418$)

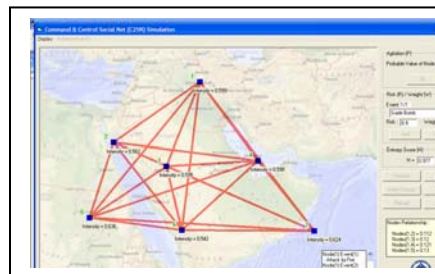


Exhibit 8. All channel design ($h=0.609$)

However, in all cases, both circle network and all channel designs outperform the classical hierarchical design. This result confirms the premise of network-centric gains in information distribution advocated by Alberts, Garska and Stein (1999).

CONCLUSION

It is believed here that tactical events in the battlefield network moderate the behaviors of the network in time and space. It is thus important to understand the level of agitation and vulnerability caused by such events. 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. This nascent model has some short comings that need further research. These are: (1) We need to improve on the user interface; (2) We need to add dynamic database 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 behavior of the network and its node dynamics. The generality of our modeling effort is illustrated with multi-node information communication network in Exhibit 9.

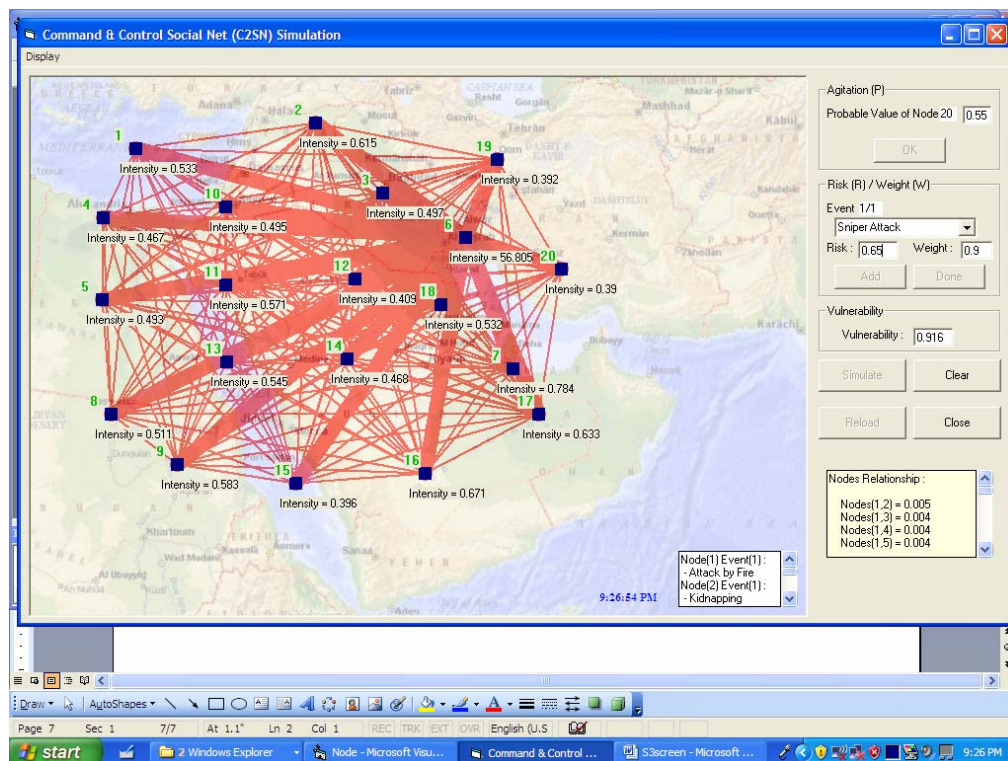


Exhibit 9. Sample result from multi-node network vulnerability

ACKNOWLEDGMENT:

This project is supported by 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

- Alberts, D., Garstka, J. and Stein, F. (1999) Network Centric Warfare: developing and leveraging information superiority, 2nd Edition, CCRP Publications, Washington DC.
- Alberts, D. and Hayes, R. (2006) Understanding Command and Control, CCRP Publications, CCRP, Washington DC
- Bolman, L.G., & Deal, T.E. (2003). *Reframing Organizations: Artistry, Choice, and Leadership*. 3rd Edition. San Francisco, CA: Jossey-Bass.
- Hamilton, John A., Jr., Simulation to Support Security Issues Related to System interoperability, Summer Computer Simulation Conference, July 14- 18, 2002 San Diego, California, USA
- Leblebici, H. and Salancik, G. R. (1981). Effects of environmental uncertainty on information and decision processes in banks. *Administrative Science Quarterly*, 26, 578-596.
- Lospinoso, J. (2006). The ELICIT experiment: Eliciting organizational effectiveness and efficiency under shared belief. ELICIT Report, Experiments in Command and Control within Edge Organization, Command and Control Research Program, U.S. Department of defense, EBR, June.
- Lyle, D., Chan, Y. and Head, E. (1999) Improving information-network performance: reliability versus invulnerability, *IIE Transactions*, 31, pp. 909-919.
- O'Neill, P. (1999) Assessing Network Vulnerabilities, Proc.TTCP Symposium on C2RT, Rhode Island, 1999.
- Reza, F. (1994). Introduction to Information Theory, Dover Press.
- Shannon, C.E. (1948). A mathematical theory of communication. The Bell System Technical Journal, vol. 27, pp. 379-423, 623-656.
- Tribus, M. (1961). Thermostatistics and Thermodynamics. Princeton, NJ: D. van Nostrand Company, Inc.



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.

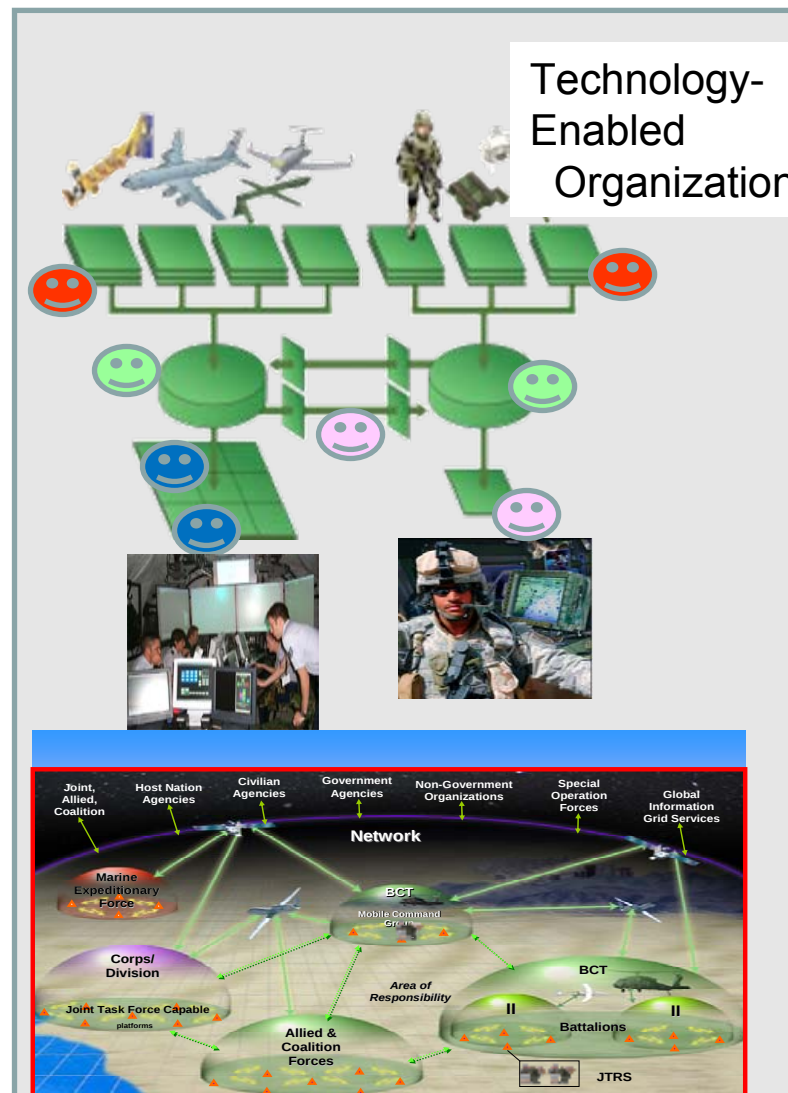
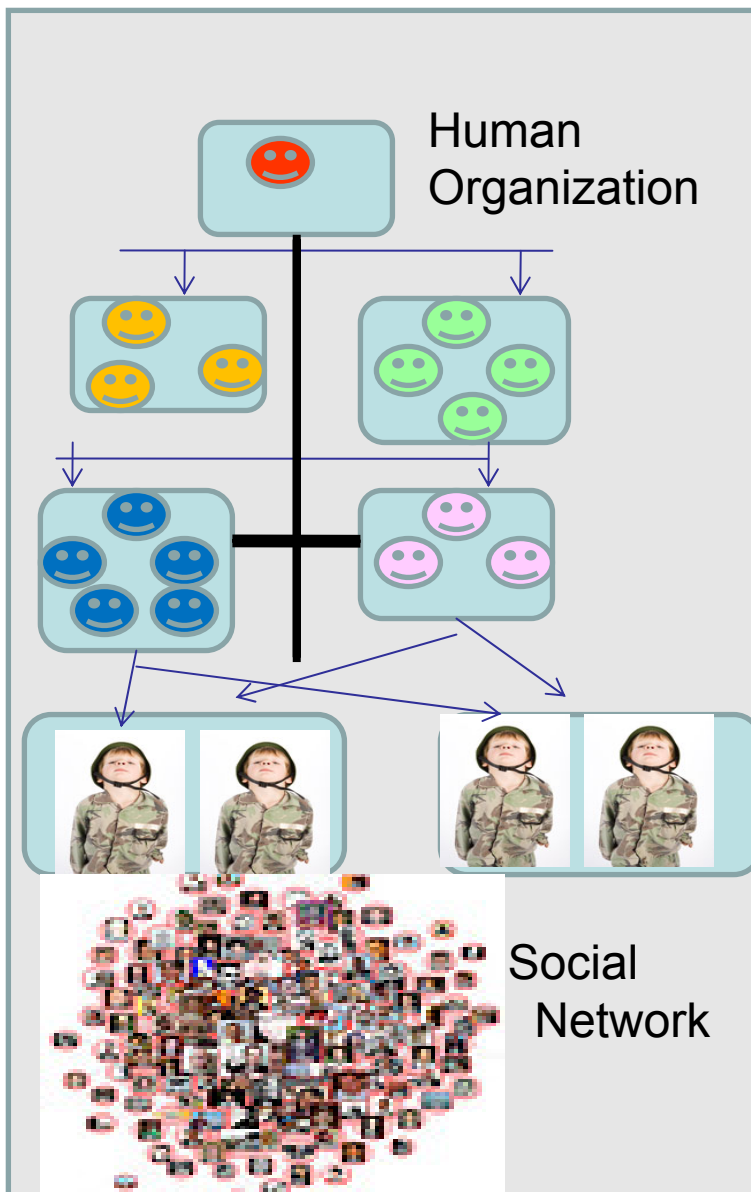


Presentation Outline

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



A Network View of Organizations





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.

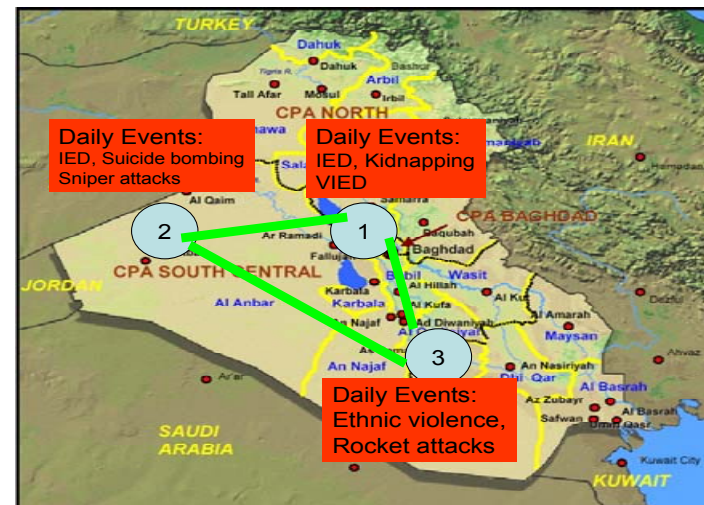
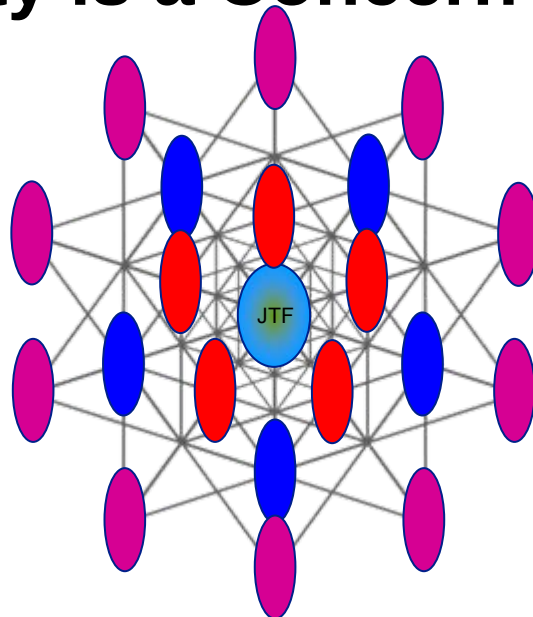


A Brief on Network-Centric Organizations

- 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.



In the Military Domain, C2 Network Vulnerability is a Concern

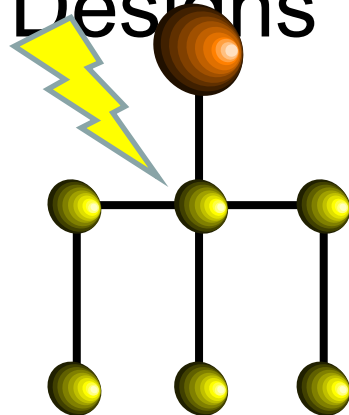
Current measures of network vulnerability consider:

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

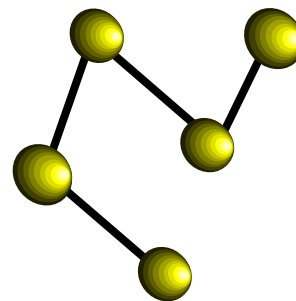
Must be considered:

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.

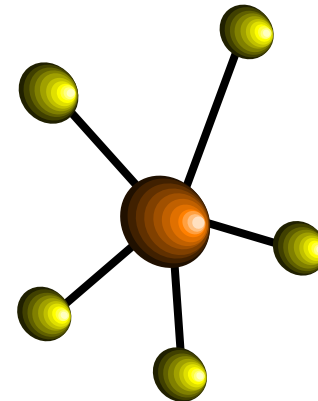
Selected Types of Organization Designs



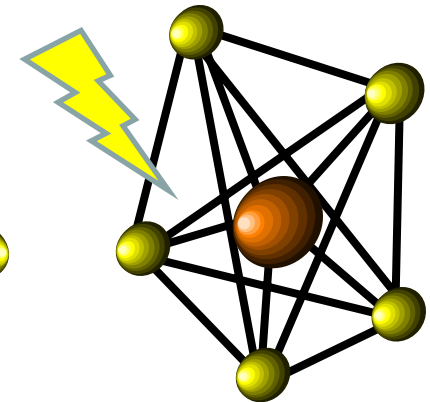
Standard Hierarchy
(one Boss)



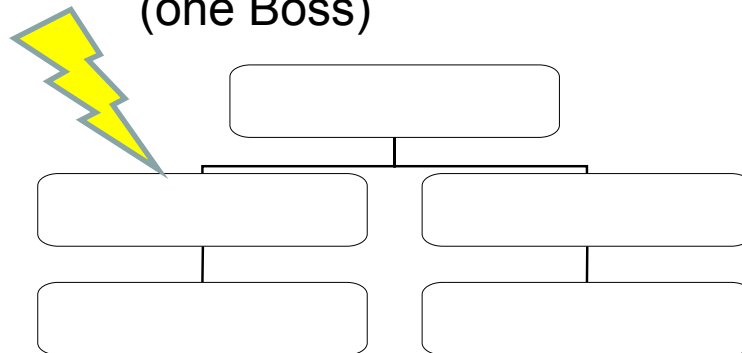
Chain Network



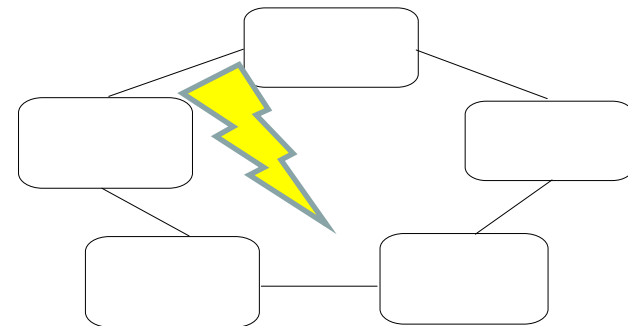
Hub & Spoke



All-Channel



Dual authority



Circle Network design

Considered for the study



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 likelihood 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).

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

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).

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

Evaluation Metric for Organization Design Comparison

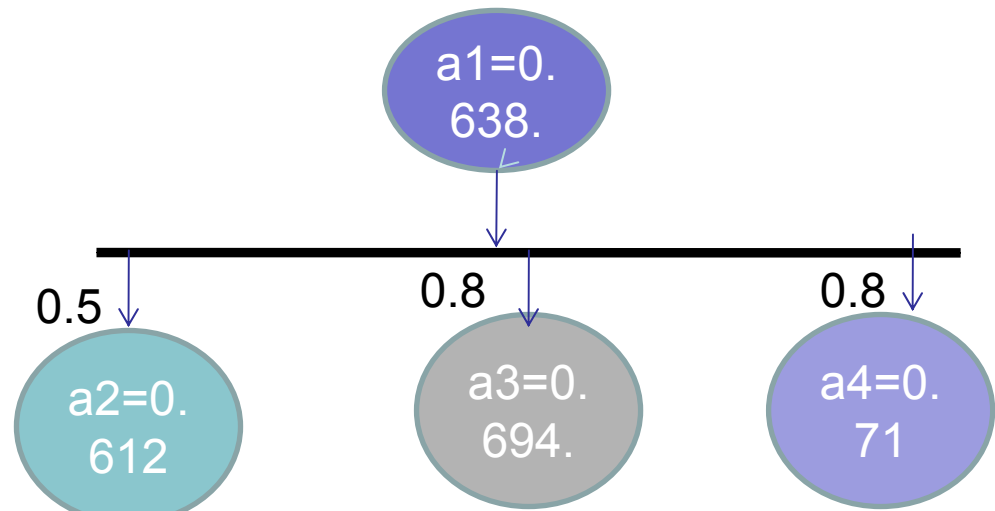
One Boss Analysis

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

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



	1	2	3	4
1		0.5	0.8	0.8
2				
3				
4				

Information surprisal score, $h_k = \log_2 \left(\frac{1}{W} \right)$



Evaluation Metric for Organization Design

Comparison

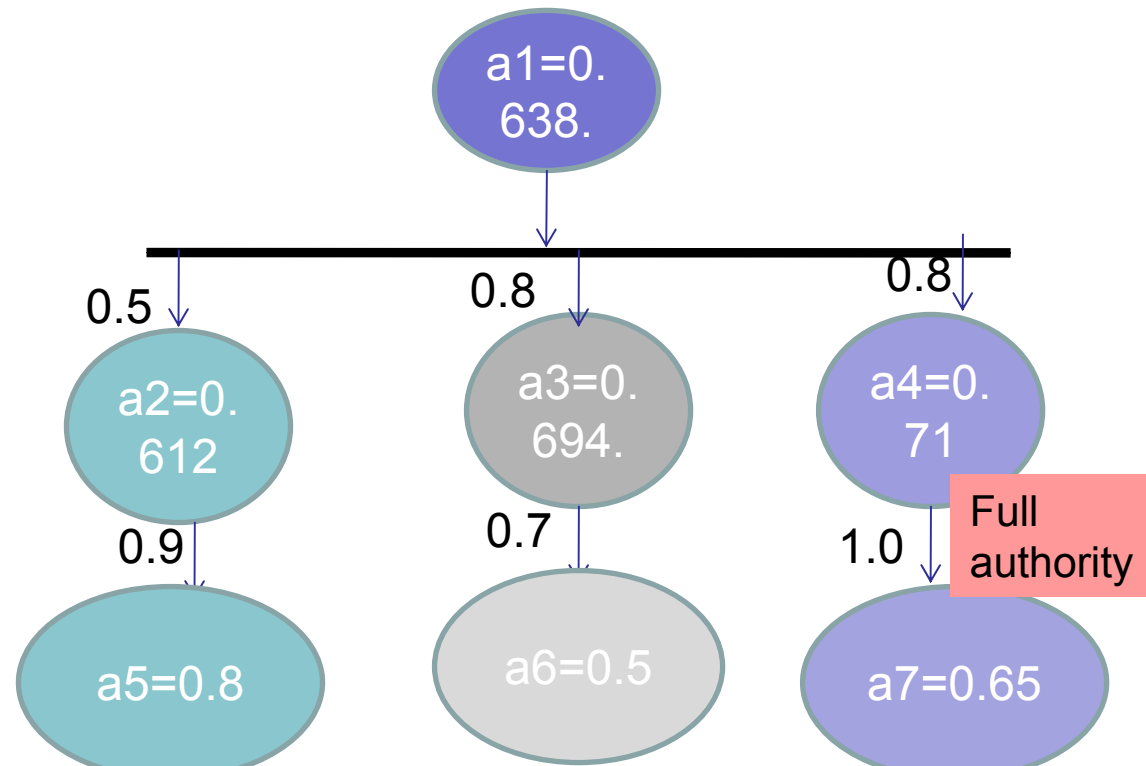
Dual Authority

- 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

$$\bullet b_{12} = (1 + (1 - b_{25})) * b_{12} = (1 + (1 - 0.9)) * 0.5 = 0.55$$

- 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 $\mathbf{m} = (b_{12}, b_{13}, b_{14}) = (0.55, 1.04, 0.8)$. $\mathbf{m}^* = (0.23, 0.44, 0.33)$: scaled to 1.



Extended path weight, and the average network weight and surprisal using equations 3-5. For example $e_{125} = a_1 * m_{12}^* * a_2 * b_{25} * a_5 = (0.638 * 0.23 * 0.612 * 0.9 * 0.8) = 0.0647$; $W = 0.076$; $h_2 = 3.718$.



Evaluation Metric for Organization Design Comparison

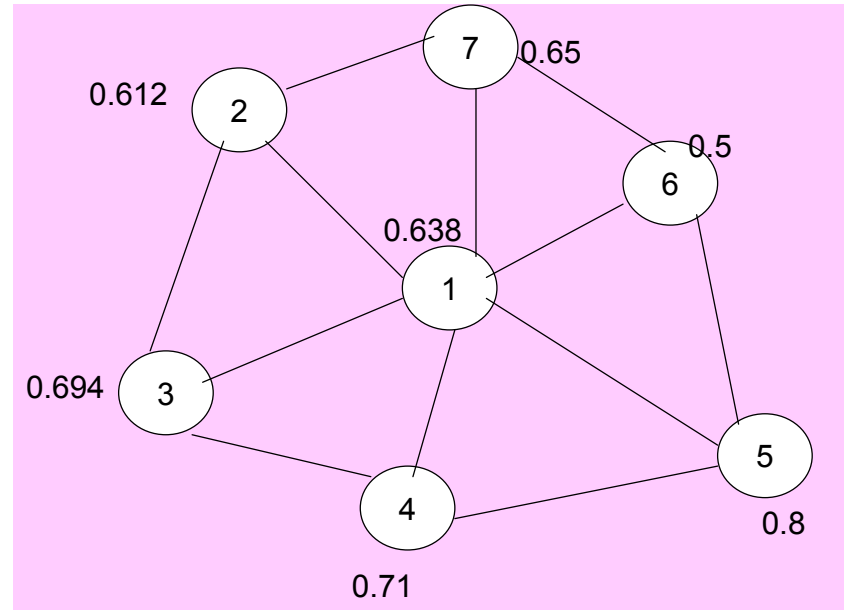
Circle Network

- 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 $h = h_e - h_n$

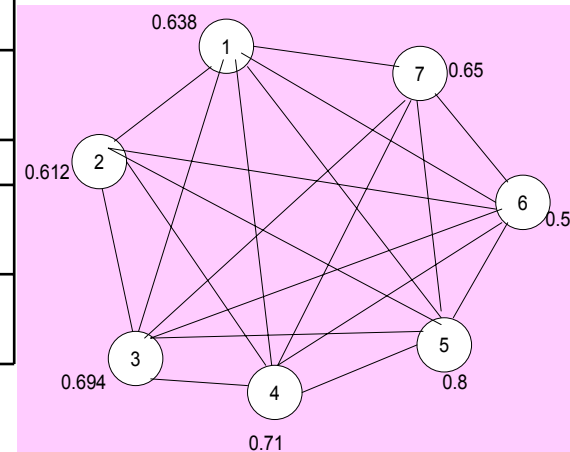


Evaluation Metric for Organization Design Comparison

	1	2	3	4	5	6	7	Row average
1	0	0.0389	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	0.347	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 e_{ij} , $i \neq j$; 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

orgadesigninput - 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

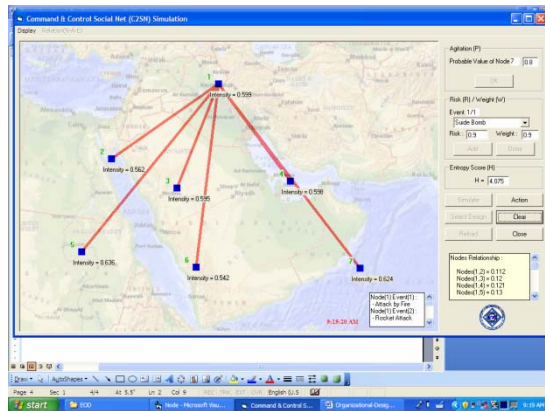
output :

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

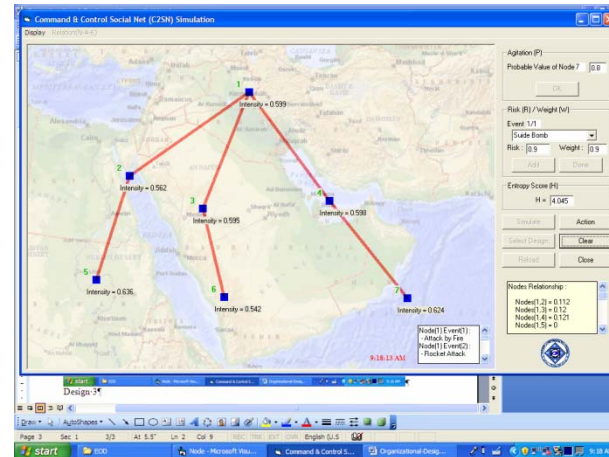
Page 7 Sec 1 7/8 At 278.2pt Ln 13 Col 1 REC TRK EXT OVR English (U.S)

Start 13CRRT Removable Disk (H:) ICCRTS-176 Evaluat... orgadesigninput ... 2:17 PM

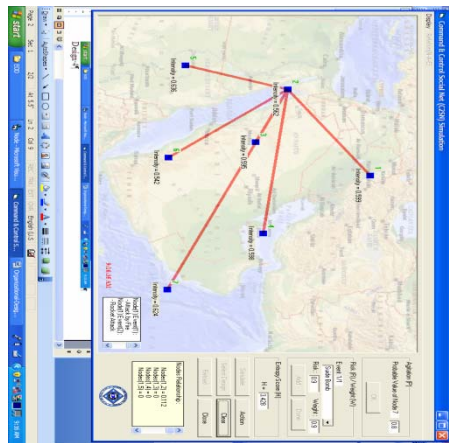
Computational Evaluation



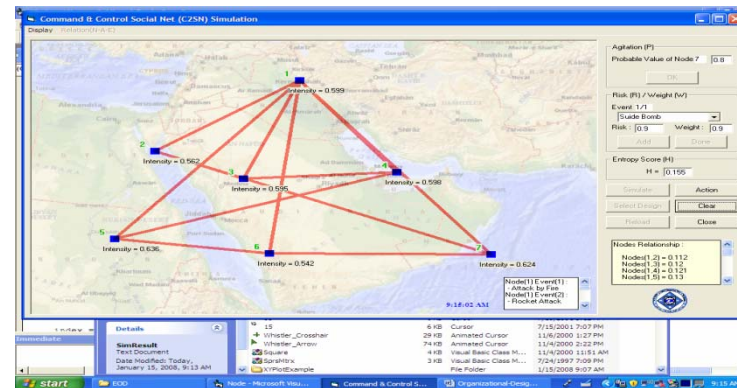
One boss design ($h = 2.857$)



Dual authority design ($h = 1.94$)

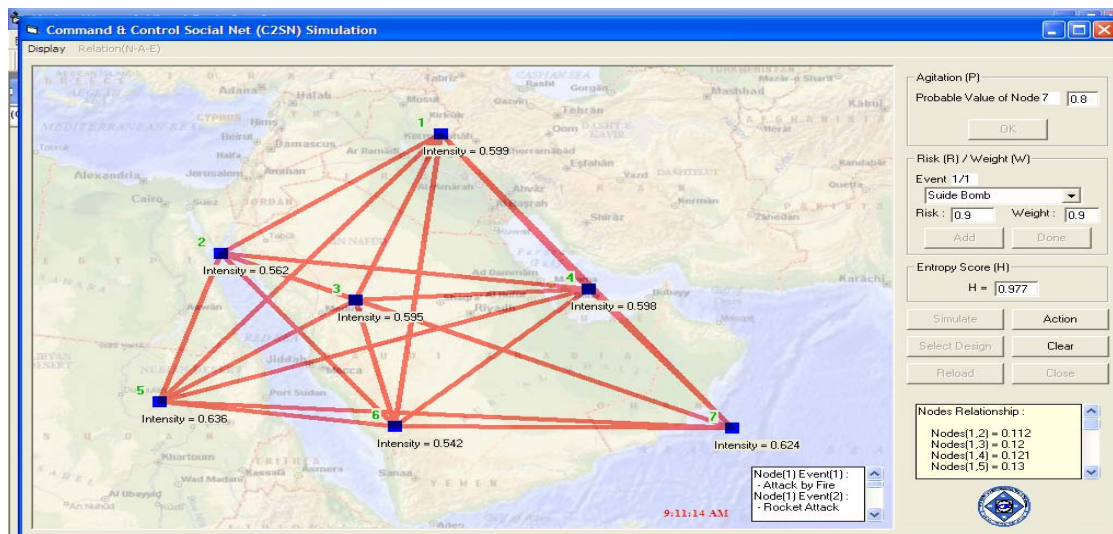


Simple hierarchy design
($h = 1.91$)

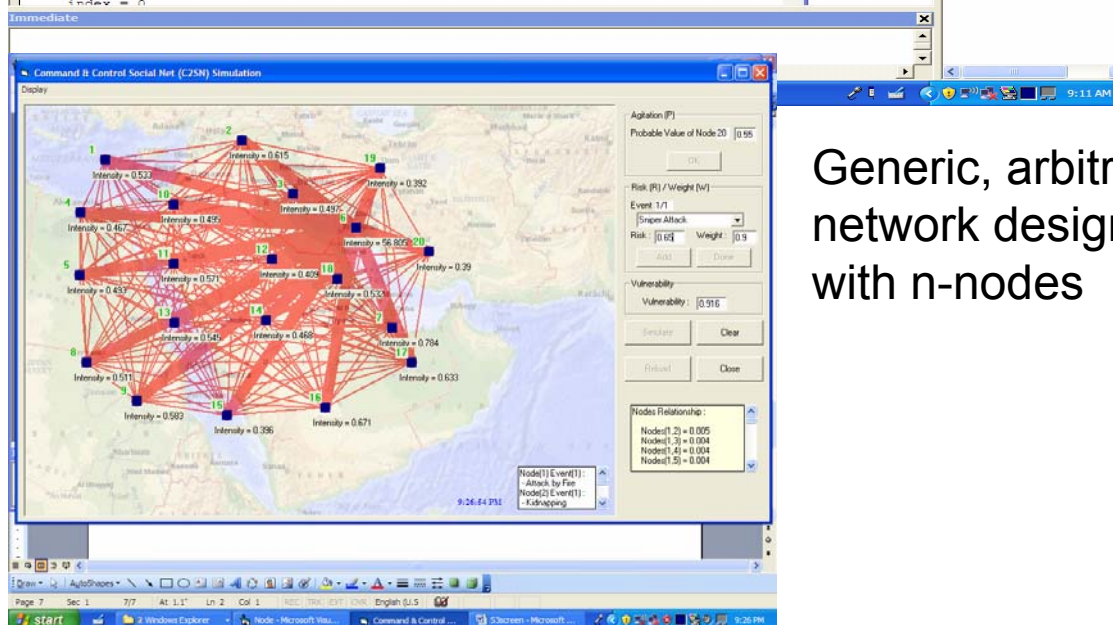


Circle Network design ($h = 0.6418$)

Computational Evaluation



All-channel
design($h = 0.609$)



Generic, arbitrary
network design
with n-nodes

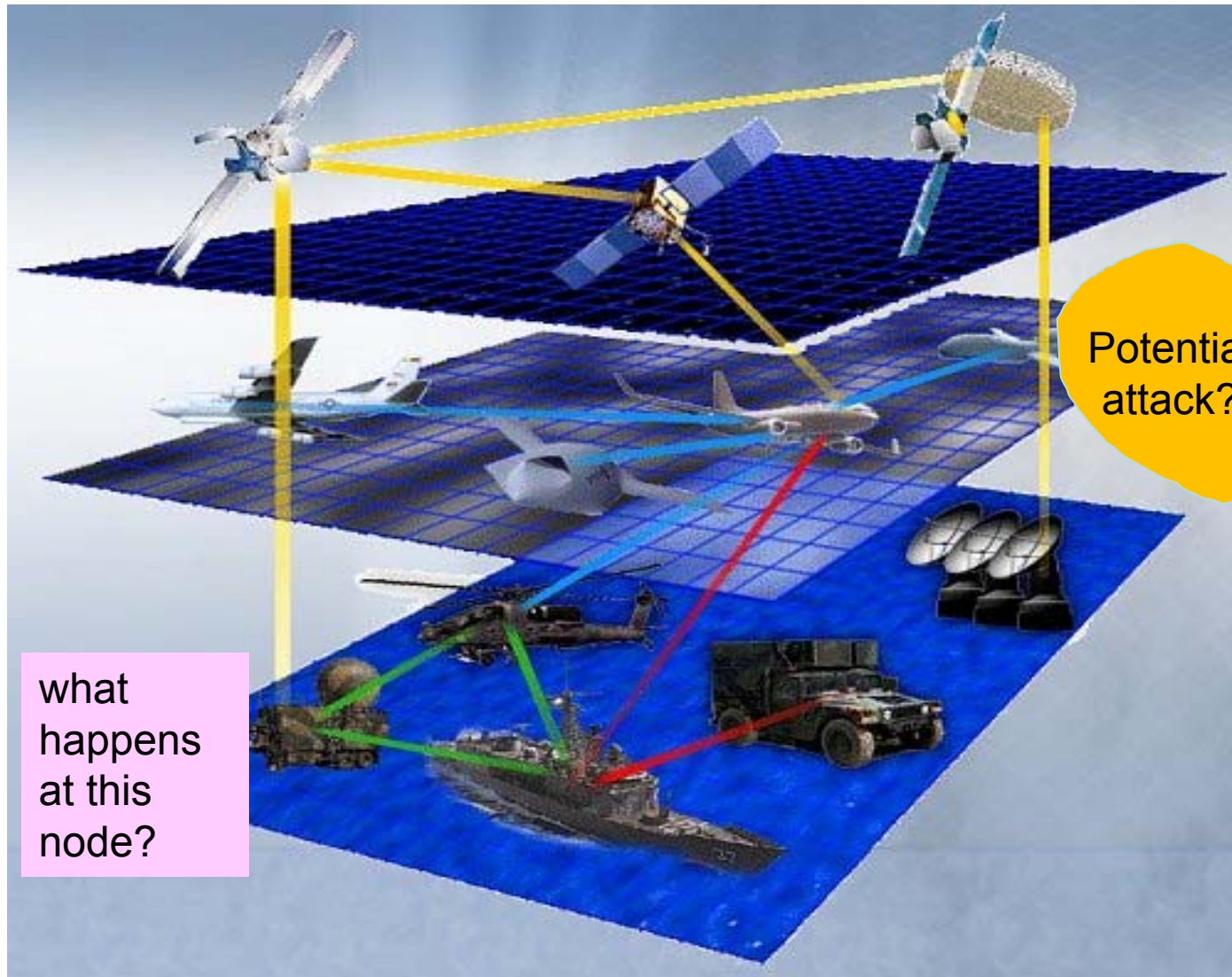


Summary and Results

- 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.

