AN INFORMATION AGE COMBAT MODEL

Jeffrey R. Cares
Alidade Incorporated

ABSTRACT

This paper reviews the assumptions underlying extant Industrial Age combat models and discusses limits to their use in the Information Age. Recent attempts at modern combat models are reviewed. An Information Age Combat Model is introduced and the mathematics of its structure, dynamics and operational evolution are presented. Policy, doctrine and acquisition implications are explored and tutorial of relevant mathematics is appended

1 INTRODUCTION

Significant recent research has focused on the structure of distributed networked systems. This research is providing new insight into the structure, dynamics and evolution of such systems as X, X, X and X. Through this work, new classes of network structure have been identified and new catalog of statistics and metrics describing their most important characteristics has been developed.

This research pertains exclusively to distributed networked systems in non-military contexts. This paper, however,

2 COMBAT MODELING

The basis of most combat modeling techniques used today comes from descriptions of the physical world that are over 100 years old. Not only is there evidence that these techniques never adequately explained data from actual combat at any time in the modern era,[1] they do not describe command and control (C^2) processes that exist today nor will they adequately describe the projected future C^2 processes in Information Age warfare.

This section will focus on the assumptions and underlying philosophy of existing combat models. Not only will the assumptions and philosophy of contemporary combat modeling be explored, but the discussion will also demonstrate the unsuitability of existing techniques to describe Information Age warfare and suggest the characteristics that will be required of models that better describe and support Information Age combat processes.

2.1 Traditional Attrition-Based Combat Models

There are two basic types of combat model in use today, deterministic (closed-form equations) and stochastic (probability-based) combat models.

Deterministic Models. The most famous example of a deterministic model are the eponymous Lanchester Equations, first published by a Victorian-era engineer who developed a mathematical force-on-force theory of combat in 1914.[2] This model is the basis for most of the current attrition-based combat models in use today. In brief, Lanchester's theory was that each side in a combat duel degrades the other side at some rate proportional to its own remaining size multiplied by the firing rate of an average shooter. Using differential equations, Lanchester could theoretically predict such results as the ultimate winner of a contest between combatants, the time required for the duel to conclude or the size of each force remaining (or destroyed) at the duel's conclusion.

Stochastic Models. In another common class of attrition-based model are stochastic models. These models typically represent combat as a chain of events, each with their own probability of occurrence or as sets of basic interaction equations with random variables representing operational processes. These models must be run a "statistically significant" number of times so that random behaviors will collectively converge on some stable, aggregate mathematical values.

Assumptions in Traditional Models. There are some very important underlying assumptions that impact the form and application of traditional deterministic and stochastic attrition-based models. The most important of these are:

- Command and control assumptions: C2 is rarely represented explicitly but rather implied by such devices as the relationships between variables or the sequence by which random variables are drawn.

- Regulation of random events: When random variables are used in traditional models it is assumed that the distribution of outcomes for a variable is not so skewed that a relatively small number of model runs will mitigate variation in the random variables.

- Monotonicity: This assumption requires that grossly non-linear outcomes should not be triggered by small changes in any input variable. For example, doubling a rate of fire or doubling the size of a force should roughly double the damage done to an adversary, not, say, triple the losses to one's own force.

- Independence: This assumption requires that complex chains of causality in the operational processes being modeled are inconsequential and that most processes can be modeled as either independent events or as chains of simple causality.

2.2 Recent Attrition Models

Traditional attrition models describe continuous fire combat, where one side erodes the combat power of another at some fixed rate over time. In the late 1980's Hughes developed an attrition model that described both the exchange of striking power during the Battle of Midway and the character of combat power exchanges in the "Missile Age". His salvo exchange model described combat as a "pulse" of offensive combat power designed to instantaneously penetrate an adversary's active defenses and to cause damage to the adversary's platforms[3]. Although this model has important descriptive power its two major drawbacks are that it only holds for homogeneous forces and it is strictly deterministic. These shortfalls were later addressed by introducing a version for heterogeneous forces and a stochastic variant[4]. Although these two variants were never combined into a stochastic, heterogeneous salvo model, such an exercise would be largely academic and not of practical use. The reason is that although the stochastic version allowed exploration of a more dynamic range of inputs, the heterogeneous variant required a high-dimensional "matching matrix" to define the interactions between elements of offensive combat power, defensive combat power, and staying power. In short, a full description of the matching matrix would be tantamount to an *a priori* description of the all the combat behaviors and supercede the need for the model to begin with.

One powerful feature of the salvo model is explicit calculation of "combat entropy" as a very normal condition of warfare. Combat entropy is one aspect of the uncertainty or "fog of war" that holds, in part, that there will often, if not always, be a sub-optimum assignment of combat power to targets. Later work explained the extent to which combat entropy and the sub-optimal assignment of combat power affects combat outcomes[5].

2.3 Command and Control (C^2) and Combat Modeling

Most Department of Defense (DoD) combat models are some variant of traditional models with additional C^2 parameters (in the case of deterministic models) or the addition of C^2 statistical terms (in the case of stochastic chains). Newer efforts (The Joint Warfare System (JWARS), for example) have attempted to more explicitly capture the most important command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR) operations. However, the underlying philosophy has not departed from embellishing traditional attrition models with C^4ISR parameters or processes.

2.4 Network Centric Warfare Modeling

The concept of Network-Centric Warfare (NCW) was pubicly introduced by Vice Admiral Cebrwoski and Mr. John Garstka in 1998.[6] Cebrowski and Garstka describe how the military must shift from platform-centric to network-centric warfare, drawing a parallel in warfare to the use of information technology in the business sector, a process of shifting from platform-centric computing to network-centric computing. They describe the power of network-centric warfare as being governed by Metcalfe's Law, such that the "power" of a network is related to the number of connected nodes in a network (specifically to the square of the number of nodes in a network). The power comes from the

"information-intensive interactions" between the nodes. Cebrowski and Gartska describe how NCW results in an increase in speed of command, self-synchronization of forces, and higher situational awareness.

Each of the services and the Joint Staff have their own operational vision relative to NCW: Ship-To-Objective Maneuver (STOM – Marines), Future Combat System (FCS – Army), FORCEnet (Navy), Effects Based Operations (EBO – Air Force), and the Joint Vision document series (Joint Vision 2010, Joint Vision 2020 – Joint Staff). Early attempts to model NCW used metaphors and thumb rules taken from the information technology (IT) industry or attempted to re-cast traditional models as NCW models.[7] In general, the NCW literature has never graduated beyond metaphor or the type of "glittering generalities" that motivated Chase to develop his attrition-based models.[8] In no case are the mechanisms for advantage of NCW or Information Age warfare articulated with enough specificity to produce meaningful research, scientifically valid experimentation or rigorous concept development.

Some NCW modeling efforts to date include the following:

- Use of IT industry models. The most prevalent of these is on page 250-256 of the basic NCW text, which suggests that warfare will be conducted according to "Metcalf's Law".[9] Recent research into network theory show that this is a naïve assumption – networked behavior is far more complex then a simple count of potential connections.

- Textual Descriptions: In another example from the same book, an attempt is made to describe self-synchronization in detail. The text asserts that a rule set and shared awareness produces self-synchronization. Counter to this assertion, however, is research that mathematically describes self-synchronization occurring without a common ruleset and without shared awareness. Like for to many similar examples, the textual model of desired behavior does not hold up against more formal mathematic treatment.

- Booz-Allen & Hamiltom Entropy Based Warfare Model™. At its core this model consists of Lanchester's attrition-based equations with additional tuning parameters. This model provides a poor representation of combat entropy and is, in essence, still a traditional attrition-based model with Industrial Age assumptions. Ironically, if one knew the value of the tuning parameters there would be little need for the combat model.

- RAND studies on NCW measures of effectiveness (MOEs) for the Army and Navy suffer from the same deficiency as Effects Based Warfare (EBW) work: they attach Information Age tuning parameters to what is essentially an Industrial Age model.[10]

- Description of Netwar by Arquilla and Ronfeldt.[11] Although this work is valuable in its description of networks as metaphors, we will see later how this approach inadequately describes the dynamic behavior of warfare networks.

2.5 Transformation and Modeling Philosophy

All of the models described in the previous sections are inadequate in describing Information Age warfare, because they all have the same underlying philosophy: they rely on mathematics that represent combat activities as independent processes and identically distributed variables, that the world is reducible, that variables of combat can be isolated for sensitivity analysis and that the performance of individual entities is well aggregated by average global behavior. Substantial evidence to the contrary, however, shows that combat processes are not independent. Many concepts for Information Age warfare show physical objects in "grids" where their relative positions to other objects are trivialized. Moreover, it has been long known that combat performance is better represented by skewed, rather than regular, distributions.[12] Ironically, EBO and NCW operations are said to capitalize on that fact.

Requirements for an effective Information Age combat model must include the following:

- Capture attrition

- Capture the search and detection process

- Explain how arrangements of entities contribute to combat outcomes

- Explicitly represent interdependencies

- Capture skewed behavior of human performance

In summary, such a model would be a transformation in combat modeling philosophy, and would represent a true Information Age combat model.

3 Structure of the Information Age Combat Model

3.1 Mathematical Structure of Complex Networks

As discussed in Section 2, combat models currently used in the DoD are insufficient models of network processes. In addition to the reasons previously given, they fail to contain the mathematics of network operations.[13]

One starting point for this discussion is the size of combat networks. Traditional network research and understanding is based on networks with relatively few nodes; today, however, networks easily consist of thousand or even millions of nodes.* In such a network it is not relevant to discuss the effect on removal of a single node, but rather to discuss the removal of a percentage of the nodes. In addition, with networks this large it is not possible to physically represent them, as in a diagram; instead, methods of statistical analysis are being developed to represent the structure and interactions of the network.[14]

A discussion of the general properties of networks and a determination of the type of properties an Information Age combat model would have is included in an appendix to this paper.

3.2 Basic Model Structure

An Information Age Combat Model should have a structure similar to the mathematical structure of complex networks. These basic networked structures consist of nodes connected by arcs.

3.2.1 Nodes

Nodes consist of sensors, decision points, influencers, and targets. Sensors receive phenomena from the environment. A decision point receives information from sensors and makes decisions about the present and future arrangement of other nodes. Influencers interact with other nodes in an attempt to affect the state of those nodes. A target is a node that has value (sensors and decision points can appear as targets because they have inherent value, but their primary function and attributes determine their classification as sensors and decision points). In addition, all nodes have a characteristic called "side" (i.e., blue, red, orange; friend, foe, neutral; etc.).

Nodes can be contracted into a single node. For example, a single node can contain the attributes of a sensor, influencer, a decision point and a target as well. In fact, contracting sensors, decision points, influencers, and targets into a single nodes leads to the interesting result that network mathematics and interactions replicate Lanchester's equations. The technique of contraction, however, removes the networked character of the model. For this reason, traditional models cannot be used to represent networked combat.

3.2.2 Arcs

Nodes are linked to each other by directional connections known as arcs. Arcs are directional since information flows in one direction at a time. For example, targets give off phenomenology that travels to and is detected by a sensor. Examples include radio frequency (RF) energy, infrared signals, reflected light, communications, and acoustic energy, to name a few. Sensors give off phenomenology, which is why they can also be thought of as targets. Active sensors (radars, active sonars, etc.) give off energy, and passive sensors give off visual cues, magnetic signatures, etc. Decision points give off phenomenology, such as RF energy, communications traffic, visual cues, acoustic energy, etc. (a key assumption here is that a decision node must physically exist). Finally, influencers give off phenomenology and interact with other nodes, typically in an effort to destroy or render useless those nodes. Examples include weapons, jammers, and decoys.

There are multiple types of arcs, or links, in a network. Targets generate phenomena into the environment that is received by sensors. Sensors relay information to a decision point. Decision points give positioning orders to sensors, targets, and influencers, and engagement orders to influencers. Finally, influencers interact directly with targets. Figure 1 presents the graphical representation of the most basic combat network, while Figure 2 represents what a two-sided system might look.

* JEFF: Do you want to present an example of this? A combat aircraft or a networked infantryman, for example? People might not see the largeness of the number intuitively., especially if they are still thinking about platforms…

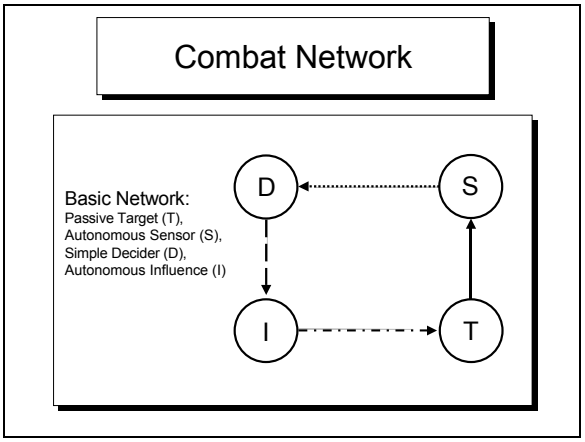

Figure 1 - Simplest Possible Combat Network

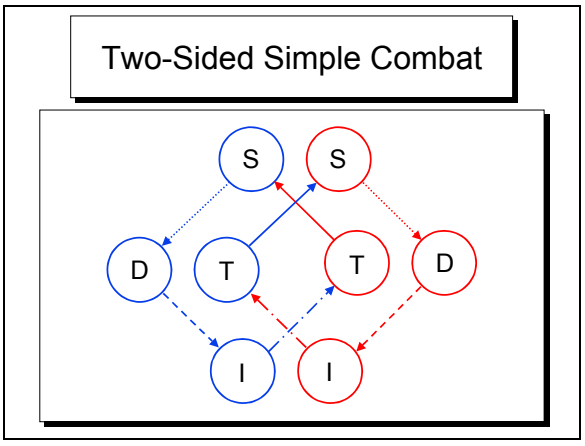

Figure 2 - Simplest Possible Two-Sided Combat Network

To clarify the relationships in Figure 1 and Figure 2, assume Combat Models have the following characteristics:

- Sensor logic does not equate to decision-making capability. That is, any logic within the sensor that governs sensor operations does not mean that it has the de facto capability of a decision node.

- All sensor information that passes to an influencer does so through a decision point; "sensor to shooter" is allowed, "sensor to bullet" is not. Take, for example, the case of an acoustic homing torpedo that has an active or passive sensor onboard that provides positional information on the target. The targeting logic within the weapon is considered the decision point (enabled, by the way, by another decision point, the platform that launched the weapon). This is, of course, an example of a contracted node, where both the decision point and the influencer have been collapsed into a single node.

- Targets could be vehicle platforms, without sensing, influencing or decision making capability, and therefore have "maneuver logic."

- Targets provide information (locator data, for example) through sensors; there is no direct path from targets to their side's decision points.

- S_x, D_x and I_x all have independence, locomotion and communications capability, but can forfeit independence and locomotion under contraction. For example, a single platform that contains all three removes the independence of each and accounts for their locomotion, but communication must remain between the three or they become targets.

- I_Y can influence S_x independent of T_x. An example of this is a jammer or an anti-radiation missile that renders the sensor impotent without otherwise destroying the target.

3.2.3 Simplest Complete Information Age Combat Model

Figure 3 represents the simplest complete Combat Model.

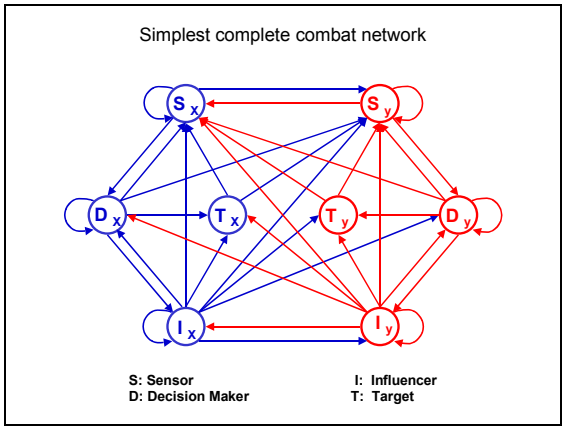

Figure 3 - Simplest Complete Combat Network

This model represents all the ways that sensors, decision nodes, influence mechanisms, and targets

meaningfully interact with each other. The two dimensions of the surface of this paper obscure the inherent complexity of even this simple model: there are 36 different dimensions in which this model operates.

In the adjacency matrix, a 1 indicates that there is a connection between the nodes in that row and column, and a 0 indicates that there is no direct connection between those nodes. Note that the connections are also directional in nature, and that the column headers represent reception of information. For example, Ix can receive information from its own side decision node (D_x), itself, and the enemy influencer (I_y), but not from its own side sensor (S_x) or target (T_x) or from the enemy sensor (S_y), decision node (D_y), or target (T_y).

Recall that this is the simplest complete model. One could, for example, include many more targets, sensors, decision nodes, and influencers. In general, the number of different subnetworks possible that can be created from an N x N matrix is $2^{(N^2)}$. This number gets very large for even small values of N. Figure 4 is a plot of $2^{(N^2)}$.

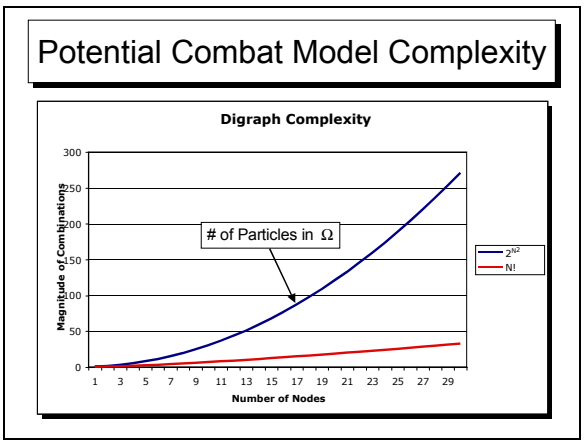

Figure 4 - Plot of $2^{(N^2)}$

For purpose of illustration, values of N larger than 20 can create more possible subnetworks then there are particles of matter in the known universe. There is some relief, however, in that the adjacency matrices created by the combat networks that have been researched to date are in a class called "sparse matrices." This means that for the simplest complete combat network only a small fraction of the 1,844,670,000,000,000,000,000,000 subnetworks that are possible are actually formed. These subnetworks are in 4 general types. The first type is a control cycles that represents direct control of one side's assets. Figure 5 displays three of the eight possible control cycle types.

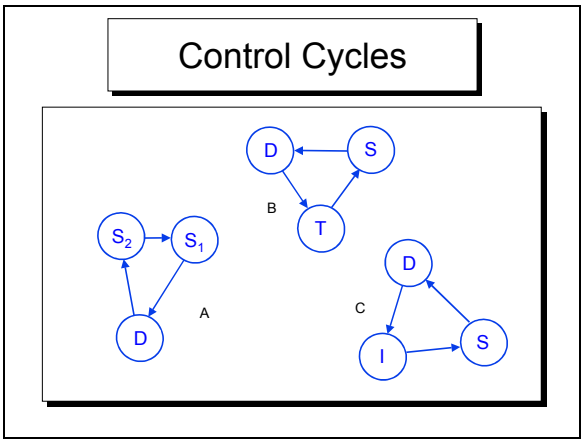

Figure 5 – Control Cycles

A is an example of the first type of control cycle, where the decision node, D, implements direct control of sensor S_2, and S_1 receives information from S_2 and reports it to D. B is a representation of a control cycle where a sensor S receives information from a target T and passes that information to a decision node D, which initiates contact with T. In the third example, D initiates an influencer I which receives information from a sensor S, which communicates back to D.

The second type of subnetwork consists of catalytic control cycles that represent control of one side's assets based on information about the state of other of the side's own assets. Figure 6 shows three of the 50 possible catalytic control cycles.

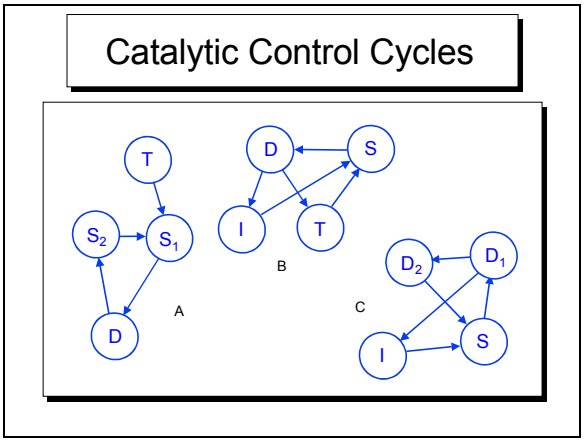

Figure 6 – Catalytic Control Cycles

In catalytic control cycle A, D controls sensor S_2, while S_1 receives information from both S_2 and target T and reports it to D. In B, decision node D controls influencer I. Sensor S receives information from both I and target T, and relays this information to D, which communicates with T. In the final example, decision node D_1 communicates with D_2 and controls influencer I. Sensor S receives information from both D_2 and I and relays information to D_1.

The third type are catalytic competition cycles that represent control of one side's assets based on information about one's own assets and the other side's assets. Figure 7 shows <TBD> of the 4,950 possible catalytic competition cycles.

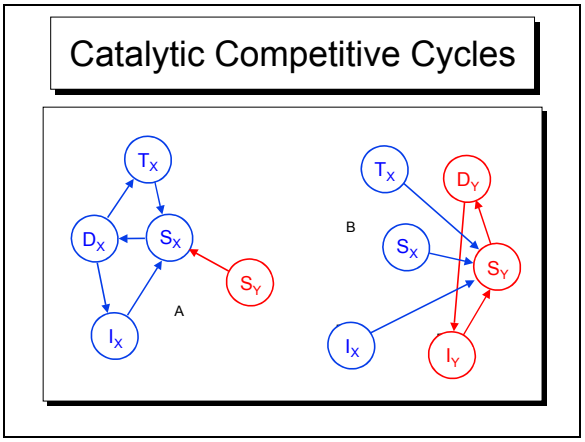

Figure 7 – Catalytic Competitive Cycles

In catalytic competitive cycle A, D_x communicates with T_x and I_x, and S_x receives information from S_y and relays it to D_x. In example B, S_y receives information from T_x, S_x, I_x, and own-side influencer I_y, and communicates with D_y, which controls I_y.

The fourth type are combat cycles that represent application of combat power from one side to the other. Figure 8 represents two of the 14 possible combat cycles.

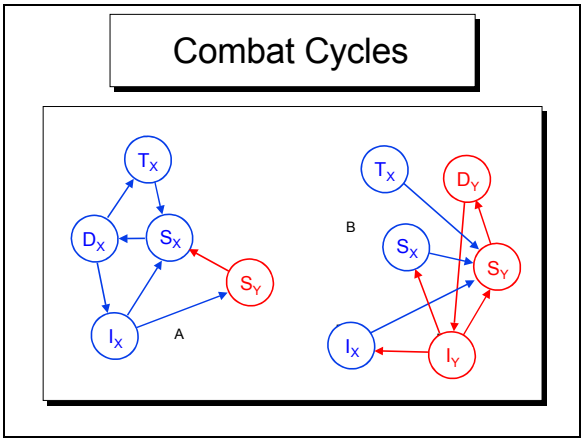

Figure 8 – Combat Cycles

In combat cycle A, sensor S_y generates information that is received by S_x. S_x relays information to D_x, which communicates with target T_x and initiates influencer Ix. S_x receives information from T_x and I_x, as I_x interacts with S_y. In example B, sensor S_y receives information from T_x, S_x, and Ix, and relays this information to decision node D_y. D_y controls I_y which then interacts with I_x and generates information that is received by S_x.

Calculating the relative frequency for each of the four types of subnetworks suggests that Information Age combat is focused much more on creating competitive arrangements of the elements of combat power to engagement than the actual application of that combat power. In the case of the simplest complete combat model, combat represents less than 0.28% of the allowable subnetworks.

Another important point one can immediately conclude is that network models previously proposed that have maximally connected networks overstate the required connectivity by many orders of magnitude. In the case of the simplest complete combat model, there are approximately 10^{24} more subnetworks connected in the 2^{64} maximally connected subnetworks than the ????? sparsely connected network.

The "snapshot" subnetwork structure of this model does not fully describe the potential for network effects in the IACM. The next section will define and describe the dynamics of the IACM.

4 DYNAMICS

The essence of networked behavior comes from the fact that dynamic behaviors are not contained in the static structural property, but are contained in dynamic interactions of arcs and nodes. If there is to be advantage in using networked forces it must arise from these dynamic network effects. Current NCW literature and contemporary combat models do not describe these effects.

4.1 Matrix Representations of Networks

Networks with directional flows can be represented as a matrix of 1's and 0's (an "adjacency matrix") for mathematical manipulation. Figure 9 is a matrix that describes the simplest complete combat network.

Adjacency Matrix for Simplest, Complete Combat Network

	S_x	D_x	I_x	T_x	S_y	D_y	I_y	T_y
S_x	1	1	0	0	1	0	0	0
D_x	1	1	1	1	1	0	0	0
I_x	1	1	1	1	1	1	1	1
T_x	1	0	0	0	1	0	0	0
S_y	1	0	0	0	1	1	0	0
D_y	1	0	0	0	1	1	1	1
I_y	1	1	1	1	1	1	1	1
T_y	1	0	0	0	1	0	0	0

row maps directionally to column = 1, 0 otherwise

Figure 9 - Simplest Combat Network Adjacency Matrix

4.2 Mathematical Manipulation of Matrices

Once a network has been converted to a matrix representation, various mathematical operations can be performed. A very rich and formal field of mathematics exists to perform these operations. [15] One of the most useful operations is the calculation of eigenvalues.[16] An eigenvalue, usually denoted by the Greek symbol λ, is a measure of the value of the networked system described by the adjacency matrix.

4.3 Measuring Networked Effects

The adjacency matrices that describe the IACM are of a particular type, "sparse non-negative matrices", that have an important property that allows for measurement of networked effects. The Perron-Frebonius theorem states that for matrices with this property, there exists at least one real non-negative eigenvalue larger than all others.* In addition, since the entries in an adjacency matrix are 1's and 0's, the Perron-Frebonius eigenvalue (PFE) will have three distinct ranges of values which correspond to three distinct values of networked effects: the absence of a cycle, the presence of a simple cycle, and the magnitude of networked effects.

The left side of Figure 10 shows a network without a cycle, indicated by the absence of a path from any node that returns to that node. The right side of the figure is the adjacency matrix that describes that non-cyclical network. The PFE for the adjacency matrix is 0. By definition, an adjacency matrix with a PFE of 0 represents a network with no cycles.

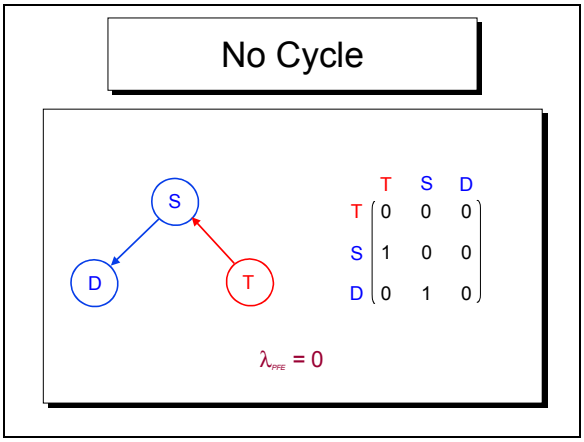

Figure 10 - Network with No Cycles

Figure 11, by contrast, contains a simple cycle. The PFE of its adjacency matrix equals exactly 1. By definition, an adjacency matrix with a PFE of 1 represents a network with a simple cycle. A network with a simple cycle has no networked effects.

Figure 12 shows additional network structures, over and above the simple cycle in Figure 11. Such additional arcs and nodes add value to a network and are the mechanism by which networked effects accrue. The PFE of the matrix representing such an adjacency matrix measures the magnitude of

* As with any multi-variant mathematical problem, there can be more than one eigenvalue that represents the value of a matrix.

networked effects and can be used to compare the topologies of various networks with respect to their potential for dynamic networked effects. These networks are called autocatalytic sets (ACS) because the additional structure creates feed-forward and feedback linkages that create networked effects.

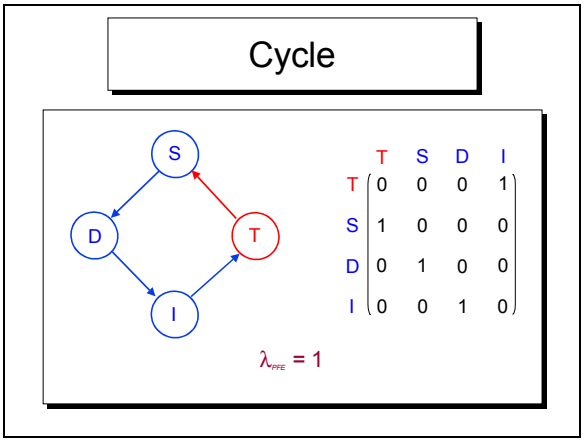

Figure 11 - Network with a Single Simple Cycle

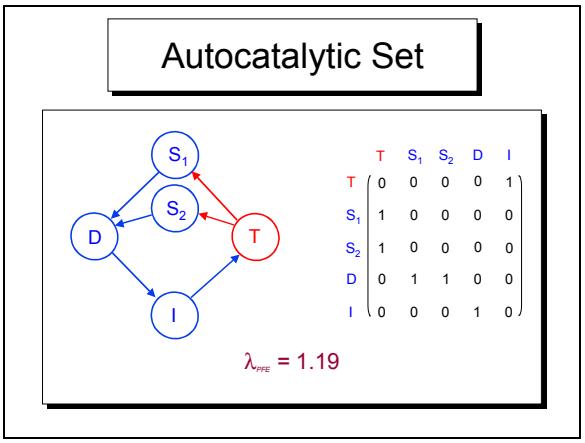

Figure 12 - Network with an Autocatalytic Set (ACS)

Figure 13 shows how the PFE increases with additional linkage. Not all additional linkages, however, contribute to networked effects. Figure 14, for example, shows how the addition of an arc and a node to the basic structure in Figure 12 does not change the value of the PFE. Figure 12 is the "core" process of the network in Figure 14. A core process is the set of arcs and nodes that contains all the mechanisms for networked effects in a network. Additional arcs and nodes that do not contribute to an increased PFE are called "peripheral" arcs and nodes. In larger networks, however, it is possible to have more than one core.

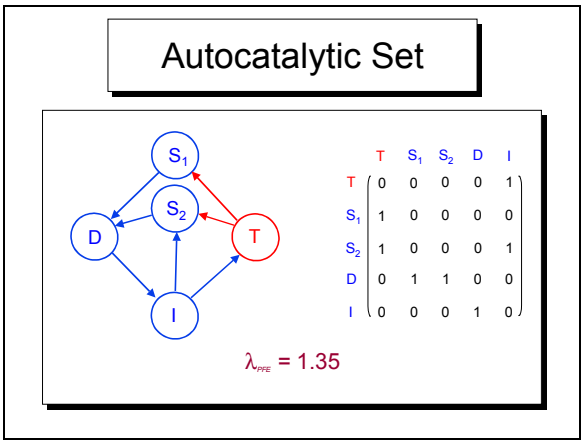

Figure 13 – ACS with Additional Linkages

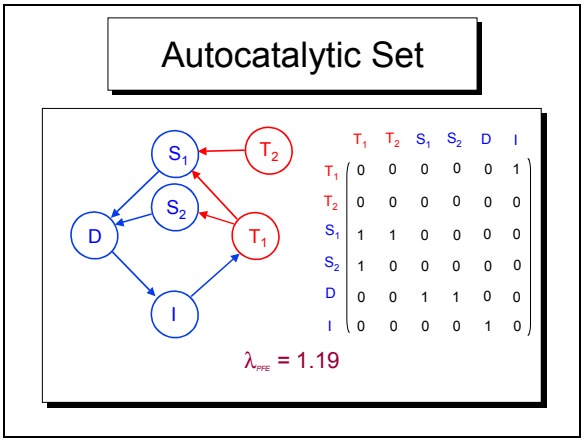

Figure 14 – Network with Peripheral Arc and Node

Figure 15 shows the different ways that networked effects can accrue. (Jeff: Not sure why Fig 15 doesn't show up on my PC).

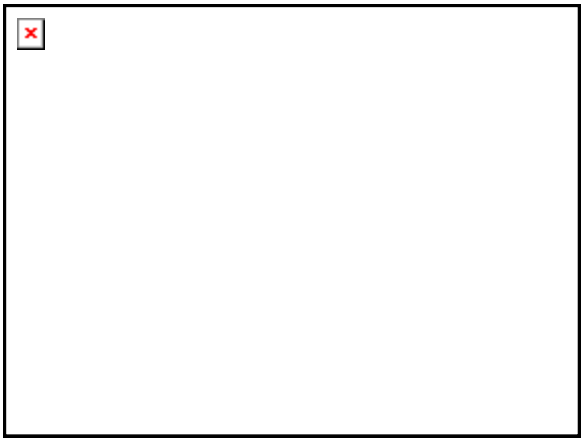

Figure 15 - TBD

This section has described the mechanisms by which networked effects accrue. What is more important for competition between networks, such as is represented by the IACM, is long timescale dynamics, or "network evolution", discussed in the next section.

5 EVOLUTION

USS Shallow Water, a littoral combat ship (LCS), equipped with an anti-air warfare combat systems package, is operating in a hostile littoral environment providing anti-air support to a mine countermeasures vessel. Shallow Water is operating a phased array air and surface search radar, a surface navigation radar, maintains a visual lookout via a mast-mounted video camera, and communicates tactical data to the mine countermeasures vessel via Link 16. Suddenly the video camera operator spots three small combat raider rubber craft (CRRC) approaching at high speed, and reports their bearing to the Tactical Action Officer (TAO). At the same time the Weapons Coordinator reports that the phased array radar has established a fire control track on the approaching craft and has locked onto them. The TAO orders the CRRCs engaged with the Shallow Water's close-in gun system (CIG), which receives tracking data from the phased array radar and quickly blows the approaching craft out of the water. The entire engagement is automatically reported to the mine countermeasure ship via Link 16.

This section describes the growth and evolution of complex networks, the exploitable properties that arise from these processes, growth and evolution, and the long-term statistics that arise in evolved complex networks.

5.1 Punctuated Growth in Complex Networks

As complex networks are formed for purpose (Jeff: FORCEnet Engagement Packs!), ACS's create a punctuated growth in networked connectivity (or for networks such as the IACM in which work is done between arcs and nodes, a punctuated increase in networked effects.

A simple thought experiment demonstrates that even a random arrangement of arcs and nodes can result in good connectivity. Imagine that there are 400 buttons and many pieces of string on a table. A button a piece of string are selected randomly from the table, picked up, tied together a piece of string and placed back on the table. This process is repeated indefinitely.

Figure 16 is a plot of the number of buttons connected to other buttons and the ratio of strings to buttons.

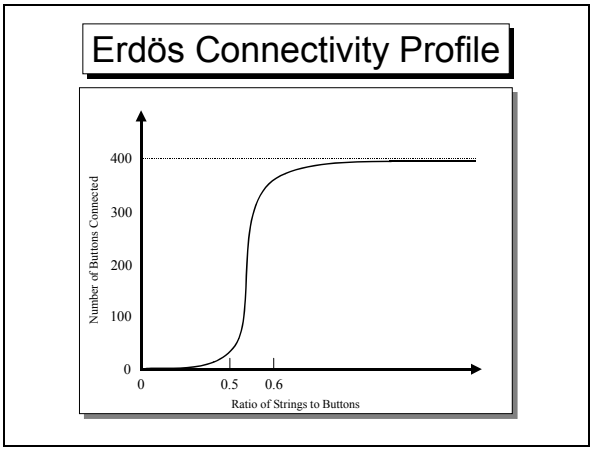

Figure 16 - Buttons and Strings

The resulting curve shows that as the ratio of strings to buttons approaches 0.5, the connectivity of the buttons dramatically increases. The curve flattens quickly, however, and each additional string adds only marginally fewer buttons to the network. Obviously, a connected network is not guaranteed by this method (the curve is asymptotic to the maximum number of buttons) but the method clearly displays the nature of the transition from an unconnected group of nodes to a highly connected network.[17]

Although the buttons and strings is a purely random process, other complex networks experience the same type of punctuated growth.

5.2 Learning and Adaptation in Complex Networks

The part of the connectivity curve in Figure 16 to the left of the tipping point at 0.5 is more important than the tipping point itself. This is because it represents latent connections that must be present for the tipping point to occur. In complex networks that are formed for purpose, particularly an IACM with sensors, this point of the curve represents two distinct behaviors. The first behavior is a kind of learning, in the sense that arcs and nodes that are initially placed inform the placement and connection of subsequent arcs and nodes. As additional arcs and nodes are added, the network evolves from one with no cycles to one with multiple simple cycles, and finally to one with ACS's and networked effects. [18] These mature networks can then be used for intended purposes if networked effects can be exploited. If the environment or

competition changes substantially, it is possible that the arrangement of arcs and nodes and, therefore, the networked effects become irrelevant to the competition or environment until such time as feedback or feed-forward results in reconfiguration of the network for its new relevant purpose.

The second behavior is adaptation. While subtlety distinct from the first behavior, reactive learning, adaptivity exploits the presence of additional latent arcs and nodes to help the network morph smoothly to respond to environmental or competition changes. A simple chain of arcs and nodes can not be a complex network; a complex network, however, can invoke simple chains within it. Complex networks can adapt by chaining portions of simple chains by drawing out of latent structure. Indeed, one measure of adaptivity is the amount of latent structure (an additional use of the PFE).

5.3 Core Shifts in Complex Networks

Section 4.3 talked about the presence of cores in complex networks. As competition unfolds or the environment changes, learning or adaptation can profoundly affect the evolution of complex networks. One of the most profound types of change is the "core shift". In a core shift the central mechanisms of networked effects can move from one subset of arcs and nodes to another. We should expect to see core shifts in the normal course of military operations in the IACM as a combat network moves from sensing a group of targets to attacking those targets. Figure 17 through Figure 20 mathematically describe just such a core shift. In Figure 17 the core portion of the adjacency matrix is outlined by a box. The portion of the adjacency matrix outside of the box represents the presence of the two peripheral nodes (I_1 and I_2), as well as a target node (T).

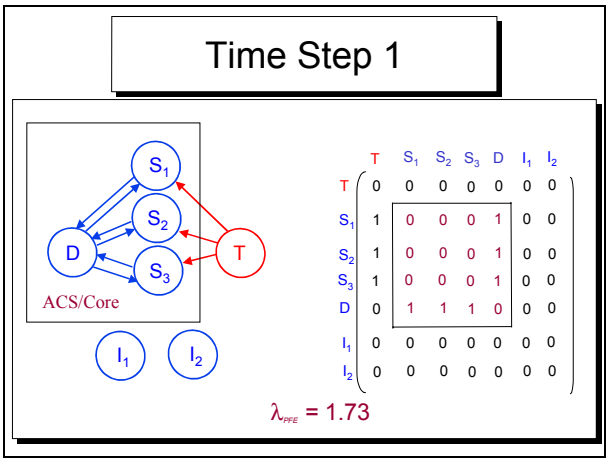

Figure 17 - TBD

Figure 18 shows the sensor S_1 reacting to T (i.e., reporting positional information to the decision node, D), and the decision node passing targeting information to two influencers (i.e., weapons), I_1 and I_2. In addition, I_1 and I_2 have identified themselves to the sensors for tracking during the coming attack. Note that the core (outlined by the box in the adjacency matrix portion of Figure 18) has expanded to include the influencers, and the PFE has changed as a result.

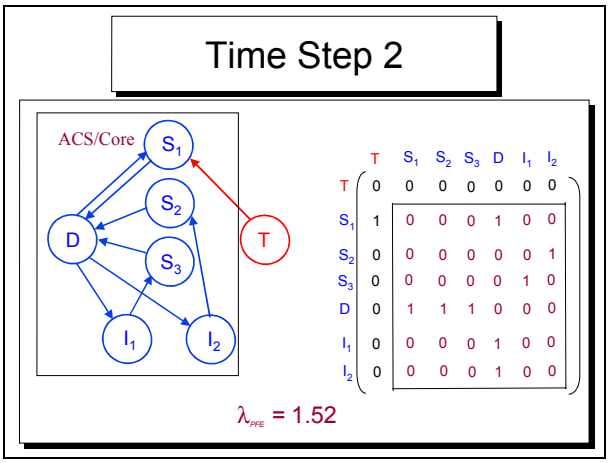

Figure 18 - TBD

In Figure 19 the network has initiated an attack on T. In addition, sensors S_1 and S_2 have been re-allocated away from the immediate problem, as they no longer serve any direct role in the attack. As a result the core has shifted and is now represented by the portions of the adjacency matrix in the lower right corner and along the left side and top. The portion of the adjacency matrix in the center represents the fact that S_1 and S_2 are now peripheral to the network. Again, the PFE has changed with this shift in the core.

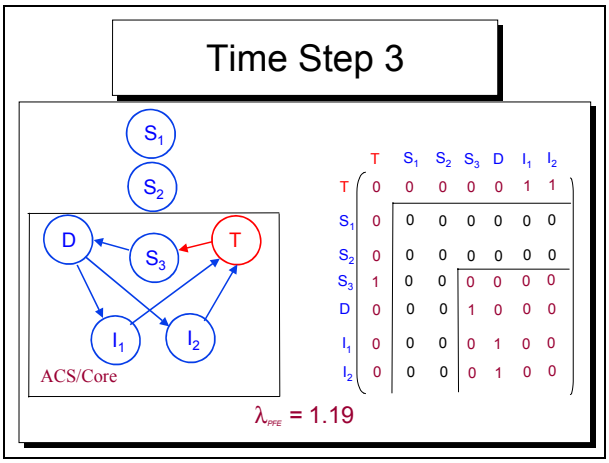

Figure 19 - TBD

In Figure 20 the attack is underway: the influencers are approaching T, and their progress is monitored by sensor S_3 which communicates data to the decision node D, which in turn sends additional guidance data to I_1 and I_2. Note that while the underlying structure of the adjacency matrix has not changed (i.e., there has been no further core shift), the additional network interactions have resulted in a new PFE.

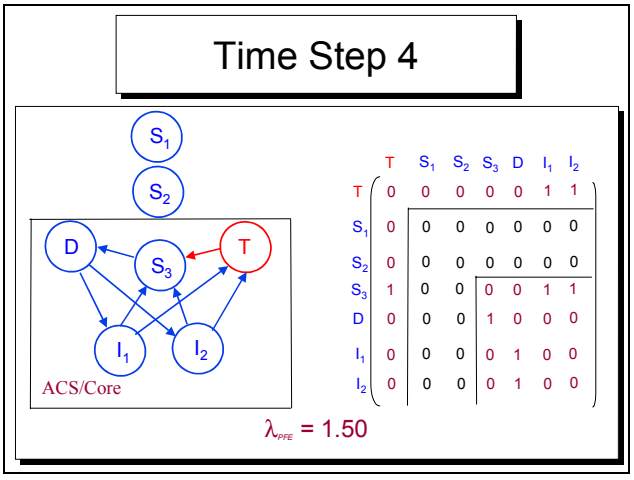

Figure 20 - TBD

5.4 Long Term Structure of Complex Military Networks

As complex networks grow and evolve their long term statistics converge on a growing number of important characteristic statistics. These statistics have been the subject of intense study over the last five years. This research suggests ththe long term statistics should pertain to complex military networks. At a minimum, the following properties and their proposed ranges of values should be used as thumb rules for information age analysis and experimentation.

Number of nodes, n. Although some future concepts contain, for example, references to "network-centric warships", networked effects depend greatly on the presence of a large number of nodes. In general, significant networked effects are unlikely to be realized in a network of fewer than 50 nodes. The steepness of the generic connectivity profile in Figure 16, for example, is precisely a function of the number of buttons: the more buttons, the steeper the curve. One of the claims of some network-centric military concepts is that the numbers count. There is ample evidence in the science of complex networks to support this claim.

Number of links, I. Just as important as the number of nodes is the number of links. Early NCW presentations and some of the existing literature suggested that all nodes should be directly linked to al other nodes, claiming that the power of the networkis equal to the square of the number of nodes (Metcalf's Law). [19] As Figure 16 shows, very good connectivity can be achieved with many fewer links than this.* Networks in which every node is directly connected to every other node have the same complexity portrayed in Figure 4. Such networks, then, needlessly incur extraordinarily excessive overhead. As a general rule, the ratio of links to nodes in complex networks should be about, on average, two.

Degree distribution. The average number of links to nodes, however, observes what is essentially an adaptive property of complex networks, their degree distribution. A node's degree is a measure of the number of links connected to it. In complex networks, there is a skew distribution of degree. + A skew distribution means that there are a very small number of highly connected nodes, a moderate number of moderately connected nodes, and a very large number of minimally connected nodes. It is this property that creates flexibility, adaptability, and modularity.

* In addition, refer to Sections 8.1.1 and 8.1.2

+ In many networks this is represented by a power law distribution; see Section TBD for additional information.

Properties of the largest hub. In most complex networks the skewed degree distribution creates a very small number of very well connected nodes. The largest hub, typically containing fewer than 100 links, has a remarkable property: it appears, recedes, and then re-appears in a different part of the network with the receiving of only about 5 to 10% of the links in the network.

Characteristic path length. Although there are a very large number of minimally connected nodes and only about two links per node, the median of the mean of the lengths of all shortest paths from each node to every other node is nonetheless relatively short. This value, the characteristic path length, grows only by the order of the number of nodes in the network. In other words, a network of 10^4 nodes has a characteristic path length of 4 links.

Clustering. Just as important to network topology and behavior as degree distribution is the distribution of the measure of local node cohesion, the clustering coefficient. The clustering coefficient measures the number of a node's direct neighbors that are also direct neighbors of each other. In complex networks this distribution is also skewed. This means that not all nodes in a cluster of mutually supporting nodes interact directly with nodes outside the cluster. The distribution of the clustering coefficient is a formal definition of the adaptive organization of the structure of hierarchy in a complex network.

Between-ness. Between-ness is a measure of a node's importance to dynamic behaviors in a complex network. Between-ness measures the number of shortest paths that pass through a node. A node need not be the most well connected node (the largest hub) in order to have the highest between-ness value. Between-ness can be used to identify the highest value nodes in a network, to control cascades of pathological behaviors in a network, or to identify potential bottlenecks.

Path horizon. Path horizon is a measure of how many nodes, on average, that a node must interact with for self-synchronization to occur. Only in very simple environments can each node successfully interact with all other nodes. Clearly interacting with no other nodes can prevent self-synchronization. [*] As a general rule, good self-synchronizing behavior occurs when the path horizon is approximately the order of the number of nodes in the network. For example, a network with 10^2 nodes will work best with a path horizon of about 2.

Susceptibility. Susceptibility is a measure of the number of links or nodes that can be removed before networked effects begin to break down. This breakdown can be measured in the loss of all of the previously listed properties.

Neutrality. Neutrality is a measurement of the amount of additional, latent structure in a complex network. This additional latent structure, where properly configured with the properties above, is exactly the source of networked effects, adaptability, and modularity in complex networks.

Figure 21 summarizes these thumb rules for analysis and experimentation.

<Figure TBP>

Figure 21 - Thumb Rules for Analysis and Experimentation

Although we can describe statistically the long term behaviors of complex military networks, we fall short of being able to use our IACM to describe the evaluation of complex military networks. The best tool for further study of these networks is an agent-based model which can translate the model into a dynamic, evolving system that achieves the above statistics. Such an effort is already in progress by the author for the Office of the Secretary of Defense.

[*] This is a contra-positive.

6 IMPLICATION

7 CONCLUSION

8 APPENDIX - COMPLEX NETWORK PRIMER

The research supporting this paper included an extensive examination of Network Flows and Graphs (including very recent research into scale free networks, much of which is still developing), Diffusion Models, Social Network Analysis, Multi-scale Representations, Complex Control Theory and the Physics of Information.

8.1 Network Theory

What is commonly called a *network* is actually a *graph*. A graph is a simple collection of *arcs* and *nodes*. When values are assigned to the arcs and nodes, a system with its own logic is created and this system is properly called a *network.*[*] Networks are typically used to mathematically model flows, analyze network circulation or evaluate costs in a dynamic, distributed system. Properties that help characterize the performance of networks include:

- Robustness: The extent to which a network can avoid catastrophic failure as arcs are removed. The opposite of a "robust network" is a "brittle network."[20]
- Characteristic Path Length (CPL): The median (middle value of ranked values) of the average distance from each node to every other node in a network. A short CPL means that commodities proliferate without passing through too many nodes.[21] (I'm not sure I understand how path length is calculated: does the length of the arcs in a path make a difference, or is it just the number of nodes in a path? I believe it is the number of arcs it takes to get from one node to a given other node. Is that correct? And if so, how does arc length figure into CPL (L)?)
- Clustering: A measure of local cohesion in a network. The clustering coefficient, γ, is the ratio of the number of arcs between neighbors to the number of possible arcs between neighbors. Highly clustered networks tend to have pockets of connectivity, which can increase the connectivity and redundancy of the whole network.[22]
- Scale: A measure of the distribution of arcs among nodes in a network. If the distribution is uniformly or normally distributed, then the network is said to have a definite scale. If the distribution belongs to the family of skewed distributions similar to the distribution of wealth in some societies, then the network is said to be scale free. Formally, a scale free network has arcs distributed according to a Power Law, where the probability that a node has exactly k links is $P(k) \sim k^{-b}$, where b is called the degree exponent.[23]

8.1.1 Minimally Connected Networks

A *connected network* is one in which every node, n, is attached to the network by at least one arc. A *minimally connected network* is one in which the nodes are all connected with the minimum number of arcs possible, i.e., $n - 1$ arcs. Figure 22 shows a minimally connected network with 16 nodes and 15 arcs. In general, a minimally connected network contains

$$\sum_{i}^{n-1} i$$

different sub-networks. The number of subnets in Figure 22 is 120. Minimally connected networks have fewer arcs and fewer subnets than any other connected network and are therefore the cheapest and simplest connected networks, but they have less redundancy and commodities take much longer to proliferate among the nodes. Note, for example, the relatively high CPL, which is also dynamically represented by the table entries listing the average number of nodes reachable from each node in n steps. Even after 4 switches, each node on average can reach only 9 nodes (including itself). Also note the graph in the lower left, which portrays the number of arcs attached to a node (horizontal axis) and the number of nodes in each category (vertical axis). This graph defines the scale of the network, which in this case is very close to two, because the great majority of nodes are connected with only two arcs. Note also that the clustering coefficient is zero, which indicates that there is very little local network structure.

[*] For the purposes of this exposition the values can be removed, greatly simplifying the discussion without a loss of validity.

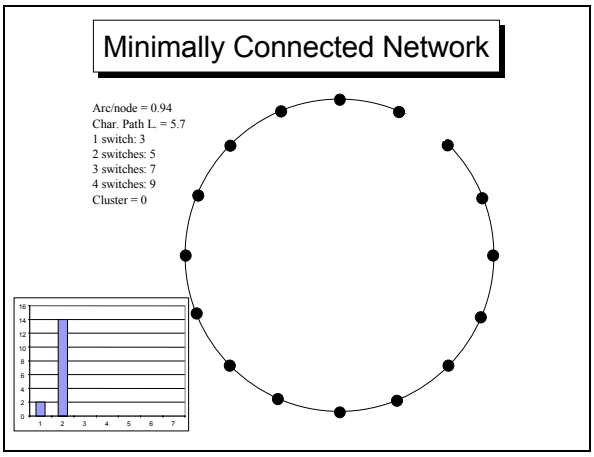

Figure 22 - Minimally Connected Network

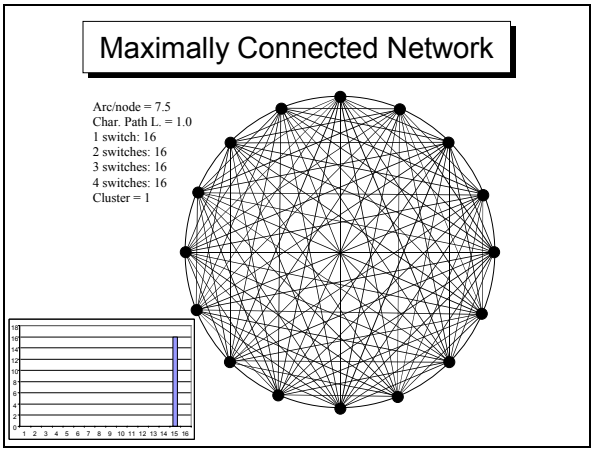

Figure 23 - Maximally Connected Network

8.1.2 Maximally Connected Networks

A *maximally connected network* is one in which every node is directly connected to every other node by one arc, i.e.,

$$\sum_{i}^{n-1} i$$

arcs. Figure 23 shows a maximally connected network with 16 nodes and 120 arcs. A maximally connected network contains $n!$ different sub-networks.* The number of subnets in Figure 23 is over 20 trillion. Maximally connected networks have more arcs and more subnets than any other type of connected network and are therefore the most expensive and complex connected networks. They have more redundancy and commodities are proliferated more quickly to the nodes (that is, they have the shortest possible characteristic path length). The fundamental drawback of maximally connected networks is that the number of subnets can easily overwhelm attempts to use them efficiently (that is, each flow calculation for the network in Figure 23 requires over 20 trillion calculations). The scale is fixed at 15, and the network is maximally clustered.

(I'm having difficulty understanding the difference between "scale" and "degree"; the terms seem to be used almost interchangeably. Also, in Figure 23 it is said that the "scale is fixed at 15", but that appears to be the "number of arcs attached to a node" (horizontal axis definition), not the "measure of the distribution of arcs among nodes in a network" (scale definition).)

8.1.3 Random Networks

Minimally connected and maximally connected networks represent the extremes of network connectivity. For most warfare network applications, neither of these two extremes are useful. Figure 24 shows such a randomly connected network.* The ratio arcs to nodes in this network is 2 (that is, there are 32 arcs, about twice as many as the minimally connected network in Figure 5 yet only about a quarter of the maximally connected network in Figure 6). The characteristic path length of this network is about halfway between the minimally connected network and the maximally connected network. The random network therefore, is more redundant and commodities are proliferated more quickly than the minimally connected network yet the number of arcs and subnets is dramatically lower than the maximally connected network. Two drawbacks arise from the random connection of arcs and nodes. The first is that the network is irregular in the sense that L has a large variation from node to node. The second is that the network is irregular in the sense that there is a large variation in the number of nodes that are immediate neighbors to each other. Irregularity in L and γ can cause great unpredictability in networks. Note that the scale of the network seems to spread out with a peak at about 3. If more nodes were added, a smoother bell-curve (Normal distribution) would emerge (although the peak would move more to the right). This portrays a

* $n! = n(n - 1)(n - 2)(n - 3) \ldots (1)$. $n!$ (spoken, "n factorial") is the highest level of "computational complexity" in network mathematics.

* To be technically accurate, this network is actually pseudo-random, since true random sequences cannot be guaranteed by computer algorithm (see note 20).

property of random networks: the arcs are distributed with a Normal distribution with the network scale defined by the peak of the resulting bell curve.[24]

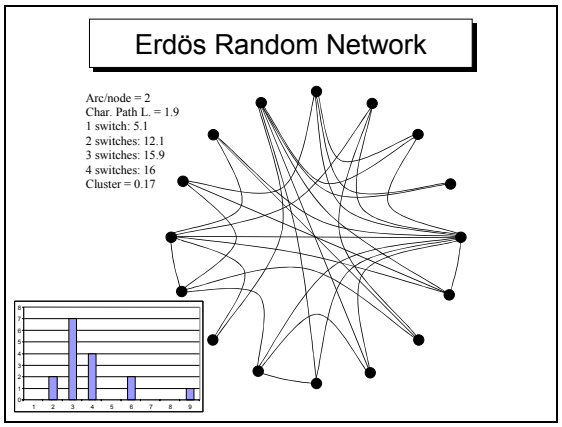

Figure 24 - Erdos Random Network

8.1.4 Regular Networks

Figure 25 shows a completely regular network (otherwise known as a "lattice") that has the same ratio of arcs to nodes as the irregular, random network. Although the clustering of this network is much more regular than the random network, the characteristic path length increases significantly (although *L* becomes more regular). The scale of this network is set at 4. Note that the maximally connected network is a special case of a regular, lattice network. Note also the dramatic difference in arc distribution between the regular and random networks, although the number of arcs and nodes is identical.

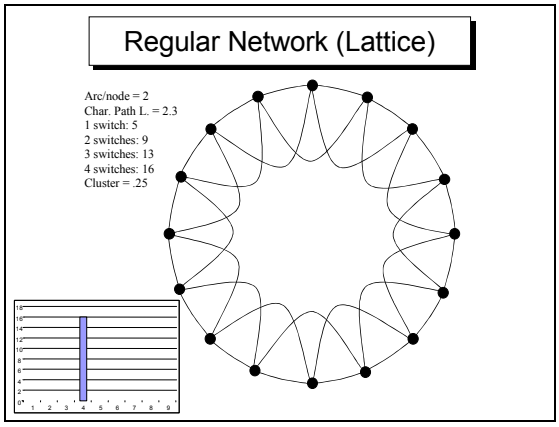

Figure 25 - Regular Network (Lattice)

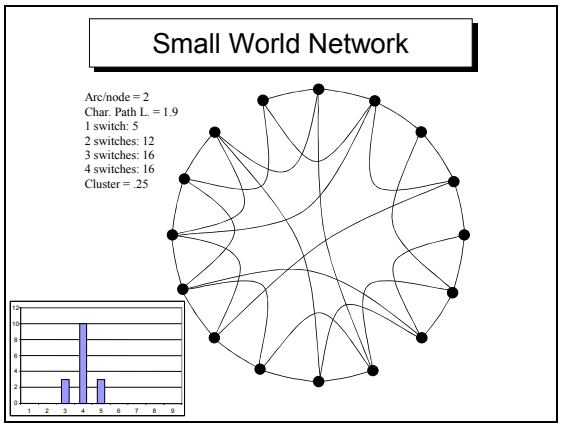

Figure 26 - Small World Network

8.1.5 Small World Networks

A minor "re-wiring" of the regular network can create a "Small World" network with a high degree of regularity, good clustering and a shorter characteristic path length. In a Small World network, remote clustered groups share members with other remote groups so that the average number of links connecting all members remains small (just like handshakes in its cultural counterpart). Figure 26 shows that a regular network (as in Figure 25) can be re-wired to create a Small World network.

8.1.6 Random Network with Growth

For many decades, Graph Theory research depended on two assumptions that were in fact obstacles to the development of the more advanced network structures needed to understand Information Age processes. These two assumptions were that, first, all the nodes in a theoretical network should be prescribed before analysis or theoretical investigation began and, second, that links were always added according to a fixed distribution. The network in Figure 27 shows what happens when analysis is not constrained by the first of these assumptions. This network experiences *growth*, in that new nodes are added to the network as the number of links grows. An obvious result of networks with growth (in this case, with random connections) is that the oldest nodes are most likely to have the highest degree because there are more opportunities for connection.[25] In other words, it is impossible to connect to nodes that don't yet exist, while the very first node in the network has *n* connection opportunities by the time the *nth* node is added.[*] Note that the network is about as clustered as the

[*] This might very well explain one source of "first mover advantage" in Information Age marketplaces.

random network, yet the scale has started to become less defined – one might just as well say that the scale of this network is 1 as they might say it is 2. Also note that with only half the links of the random, lattice and Small World networks, the network still has a fairly good clustering and the CPL grows by no more than about 50%.

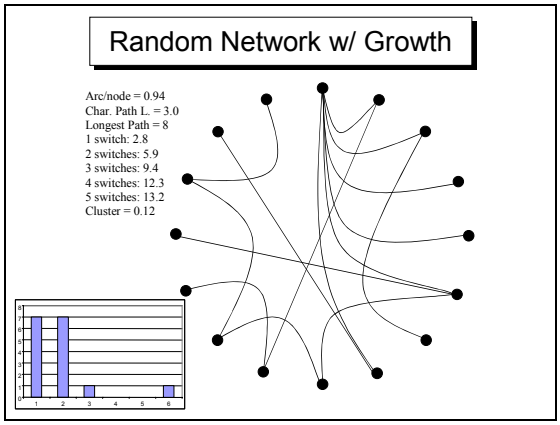

Figure 27 - Random Network with Growth

8.1.7 Scale Free Network with Preferential Attachment

If one removes the constraints of both assumptions, so that the connection of nodes is somehow unbiased and the network is grown, then a class of networks is created that quite well represents very many real world networked structures. The network in Figure 11 was grown by iteratively attaching each new node to a node in the network based on the number of links each node already possesses. Technically, this was achieved by weighting the probability that a node is selected by the degree of the node. This rich-get-richer scheme is mimicked in many Information Age processes that experience what economists call "network externalities," as well as the distribution of connections to routers in the internet, the distribution of links to web pages on the world wide web, and a host of other adaptive, dynamic network topologies.[26] The statistics of this network are a bit different than the previous examples (the network cannot be as well clustered as the others with so few links and the CPL is almost as long as the lattice) but it has one very nice property that marks it as a very adaptive network – it is a scale free network. Indeed, if this network were to be filled out with more arcs and nodes, the scale of the distribution would completely disappear and be best represented by a skewed curve (like the one approximated above the histogram in Figure 11). The generic form of the equation defined by these curves is the "Power Law." * A scale free distribution of arcs defined by a Power Law would have very many nodes with a very small degree, a moderate number with a moderate degree and a very few with a very high degree.

8.2 Analysis

8.2.1 Network Statistics

Table 1 is a summary of the statistics from the networks described in Section III. These statistics are the number of arcs, the number of nodes, the ratio of arcs to nodes, the characteristic path length *L,* the average number of nodes reached by traversing some number of arcs (or the number of "switches", listed for 1 to 4 arcs) and the clustering coefficient γ.

The minimally connected network has a low ratio of arcs to nodes, yet the characteristic path length is high. This is because the average number of additional nodes reached for each additional arc length traversed increases only by two for each additional arc. L = 1 in the maximally connected network, yet the overhead incurred is an order of magnitude more arcs and a factorial number of additional subnets. The minimally connected network has no clustering and the maximally connected network is maximally clustered.

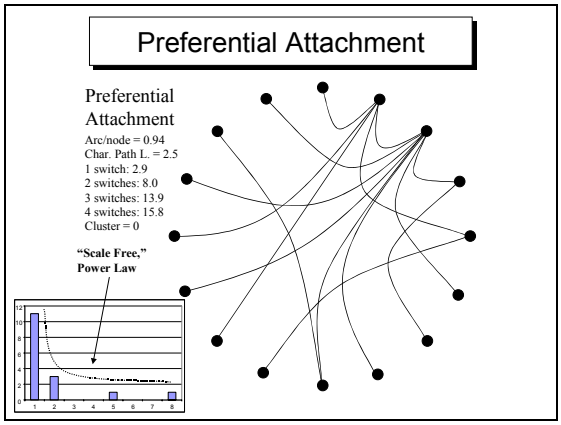

Figure 28 - Preferential Attachment

Random connection of arcs and nodes with an arc-node ratio of 2 can connect all nodes in only about 3 switches, L is low (1.9) and clustering is also better. Although the random network provides better

* A Power Law is an equation of the form $P[x = X] \sim x^{-a}$. To more fully appreciate the behavior of these functions, the reader is encouraged to experiment with the Power Law using easily available software like MicroSoft Excel™ and sample values of x and a.

performance than the minimally connected network and avoids the overhead of a maximally connected network, the network is irregular. One measure of regularity of a system is the standard deviation of the measurements within the system.[1] The standard deviation of γ listed in Table 1 for the random network means that some nodes may have values of γ similar to the minimally connected network. Arranging the same number of arcs and nodes in a more regular network, however, reduces the irregularity γ but L gets more irregular. The regular network also has a longer L (that is, commodities proliferate much more slowly in the network in Figure 22).

The Small World network uses the same ratio of arcs to nodes in a network that is fairly regular and clustered yet still proliferates commodities quickly. In other words, the Small World network uses as few nodes as possible to perform as well as the random network while retaining some regularity.

The preceding analysis demonstrates that the arrangement of arcs and nodes affects the behavior and performance of a network. Operational requirements determine this arrangement. Some theories of Information Age refer to "fully-netted" forces; Section III shows that confusing "fully-netted" with maximal connectivity will produce unnecessary cost and complexity. Minimal connectivity, however, will not produce satisfactory network performance and redundancy. Therefore, the connectivity of warfare networks must be at some "sufficient" level. Table 1 suggests that Small World networks are simpler, perform better and require lower overhead than other networks.

8.3 Conclusion

This paper has presented a variety of networks, network behaviors and network statistics. The networks listed here are mathematical abstractions of real-world phenomena. In real-world networks, the operational requirements for which a network is designed define how the network will be configured. Moreover, the rational behind the design is derived from organizational principles and organization theory. Therefore, the best configuration for a network should be an extension of the purposes and intent implied by the function, roles and behavior of the agents that operate the network, the nature of the tasks required of the networked group and the physical restrictions that may impact the logical connections.

- Minimally Connected Network
  - Too brittle, long CPL, poor clustering, simple pattern, simple control, scaled
- Maximally Connected Network
  - Robust, short CPL, too clustered, simple pattern, complex control, scaled
- Regular Network (Lattice)
  - Robust, long CPL, high cluster, simple pattern, simple control (<k> < 5), scaled
- Erdös Random Network
  - Brittle, short CPL, low cluster, random pattern, complex control, scaled
- Small World Network
  - Robust, short CPL, high cluster, complex pattern, complex control, less scaled
- Random Network with Growth
  - Less brittle, short CPL, low cluster, random pattern, complex control, less scaled
- Network with Preferential Attachment
  - Robust, short CPL, low cluster, complex pattern, complex control, scale free
- Networks do not connect randomly
  - But Random Assumption was still status quo in 1999
- "Scale Free" Networks
  - Hubs distributed by Power Law
  - Short path lengths
  - Good Connectivity
  - VERY robust
- Complex Networks (e.g., diffusion, scale free, etc.)
  - Steepness of profile, shape a function of structure
- Seed structure, critical mass, spreading rate, inflection points
  - Scale-Free Networks have some of the steepest curves
- Hubs can disappear/reappear with +/- very few arcs
- Patterns can disappear/reappear with +/- very few arcs

8.3.1 Desirable Network Properties

You use a number of terms in the "Desirable Network Properties" section that have not yet been defined: autocatalysis, neutrality, reconfiguration, tipping points, resiliency.

Most ongoing research focuses on the statistics of particular types of networks, such as the World Wide Web or the structure of a particular data set from sociology. One of the aims of this paper is to answer

the obverse question: if we could choose the type of Combat Network we should design, what properties should it possess?

8.3.1.1 Node and Link Types and Properties

The combat model will have many different types of nodes and links.

8.3.1.2 Flow

Combat Networks should expect to capitalize on the existence of cycles and the properties of autocatalysis and neutrality. The should therefore be directed networks.

8.3.1.3 Number of Nodes

Most of the more important and exploitable network effects do not occur unless a network contains at least about 100 nodes. Combat Networks that possess fewer than 50 nodes will not likely have robust behaviors such as rapid reconfiguration, tipping points and resiliency.

8.3.1.4 Number of Links

Although early Network Centric Warfare concepts suggested that each node should be directly linked to every other node for best performance (that is, about N^2 links for every N nodes), most adaptive, complex networks have only about 2N links per N nodes without suffering noticeable degradation in performance. Indeed, having fewer links provides a kind of economy that limits network overhead (including protection of links and nodes) without adversely affecting performance. Combat Networks should have about two links for every node.

8.3.1.5 Degree

8.3.1.5.1 Degree Distribution

The most adaptive, re-configurable and resilient of all networks known to date is the Scale Free Network. As stated earlier, these networks have very many nodes with have very few links, a moderate number of nodes with a moderate number of links, and very few nodes with very many links. These networks contain powerful hubs, which can be adaptively reconfigured. Combat Networks should be Scale Free Networks.

8.3.1.5.2 Mean Degree

Since Scale Free Networks do not have a meaningful "average" number (or "scale") of connections per node, mean degree is not a useful measure of Combat Networks. A better measure is the degree distribution.

8.3.1.5.3 Maximum Degree

In Scale Free Networks, the maximum degree is roughly proportional to $N^{0.5}$ for N nodes. The Figure 29 plots maximum degree against number of nodes.

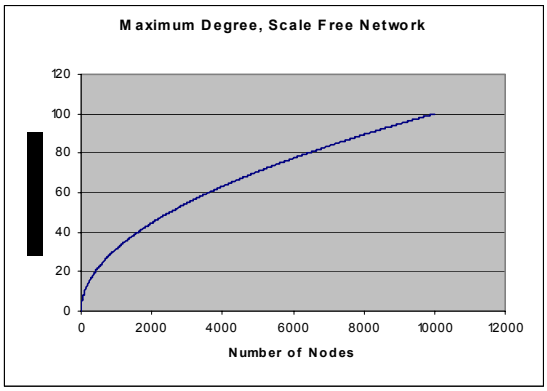

Figure 29 - Maximum Degree, Scale Free Network

8.3.1.5.4 Degree Correlation

It is not necessary that Scale Free Networks contain highly correlated high degree nodes. Recent research indicates scale free degree distributions can occur in networks that even have a negative correlation between high degree nodes. This is a desirable characteristic; since if an adversary can locate a hub, one would not want the existence of adjacent "hubs" that could be put at risk as well.

8.3.1.6 Geodesic

8.3.1.6.1 Mean Geodesic

As shown in **Figure 30**, the mean geodesic in chains grows on the order of n/4k, where n is the number of nodes and k is the mean degree. The mean geodesic in random graphs grows proportional to log n/log k and in Small World and Scale Free networks proportional to log k or slower. Combat Networks should therefore have mean geodesics on the order of log k or shorter. This means that for networks as large as 10,000 nodes, one would expect the average distance between nodes to be no more than about 4.

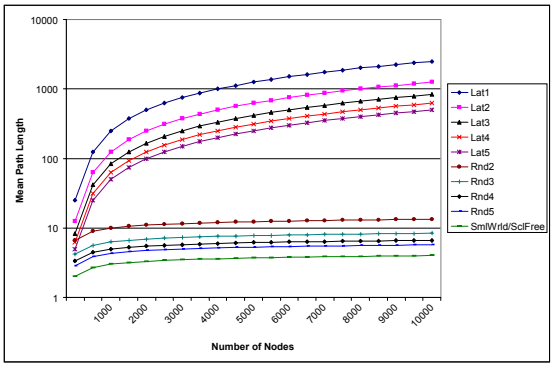

Figure 30 – Mean Geodesic Network Growth

8.3.1.6.2 Component Sizes

For sound military reasons, namely that no node should be isolated during military operations, the size of the giant component in Combat Networks should be about the size of the entire network. Smaller sub-components are advisable for certain tasks, such service specific operations in a joint environment or independent special operations. In addition, since Scale Free Networks have a great deal of neutrality, Combat Networks should have a great deal of neutrality as well. For example, typical Scale Free Networks can realign links to create high-degree nodes by rearranging only about 5 percent of the total number of links in the network.

8.3.1.7 Clustering Coefficient

Combat Networks, like other Scale Free Networks, will have low clustering coefficients. At face, this seems to violate military values such as coherence and mutual support. Clustering Coefficients, however, are measured globally over an entire network; Scale Free Networks can still have good clustering properties in the localities of the largest hubs. This local clustering provides the type of cohesion and mutual support that military operations will mandate for the most important nodes in a network.

8.3.1.8 Resilience

Figure 31, [Newman, 2003], plots the mean geodesic against the fraction of nodes removed in a Scale Free Network. Random removal provides almost a horizontal line (no growth, meaning good connection properties remain), whereas removal by degree rank (highest first) shows a rapid growth. This is intuitive because there are many more low rank nodes in a complex network than high-rank nodes and a random selection of nodes should favor low degree nodes over those with high degree. Combat Networks, since they should be Scale Free Networks, should therefore be extremely resilient to random attack. Figure 31, of course, also tells the opposite story, that Combat Networks can be very susceptible to attack. This is true so long as adversaries are allow to know the location of all links and nodes as well as the detailed structure of the network. Since Scale Free Networks have a great deal of neutrality, it is very possible – in fact it is a fundamental property of such networks – to obscure the detailed structure of a Combat Network until it is ready to be configured for use.

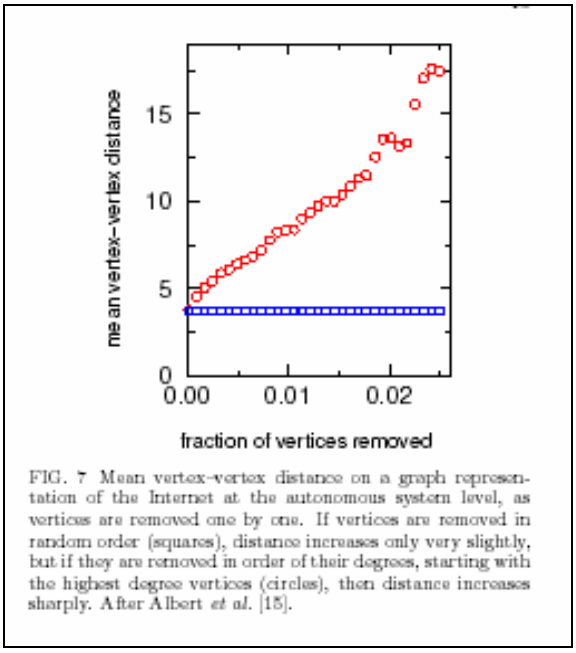

FIG. 7 Mean vertex–vertex distance on a graph representation of the Internet at the autonomous system level, as vertices are removed one by one. If vertices are removed in random order (squares), distance increases only very slightly, but if they are removed in order of their degrees, starting with the highest degree vertices (circles), then distance increases sharply. After Albert *et al.* [15].

Figure 31 - Measure of Resilience

8.3.1.9 Diffusion Rates

Figure 32 shows the type of diffusion patterns typical of complex networks, including Scale Free Networks. As discussed earlier autocatalysis and neutrality contribute to the "S" shape of these diffusion curves. These "tipping points" are useful in a military context because they can obscure the "hub" nodes to an adversary, and therefore the specific purpose for which the network is formed, until such time as friendly commanders desire to rapidly and adaptively align the network for purpose.

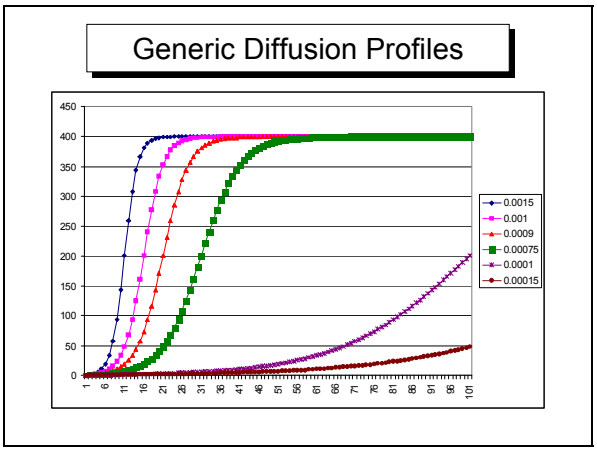

Figure 32 - Generic Diffusion Profiles: Complex Networks

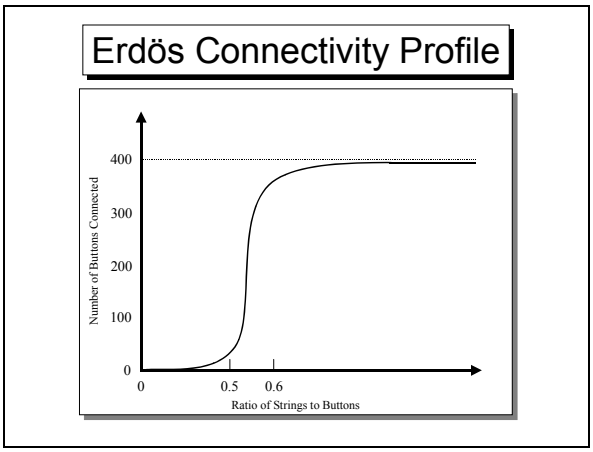

Figure 33 - Erdos Connectivity Profile

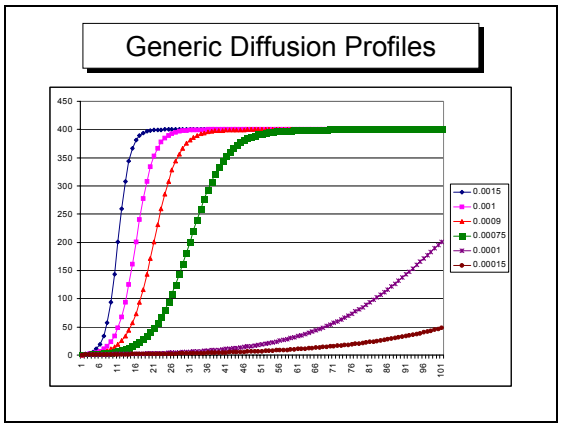

Figure 34 - Generic Diffusion Profiles: TBD

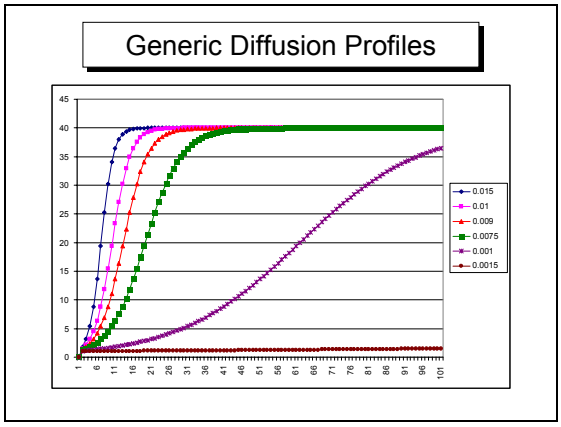

Figure 35 - Generic Diffusion Profiles: TBD

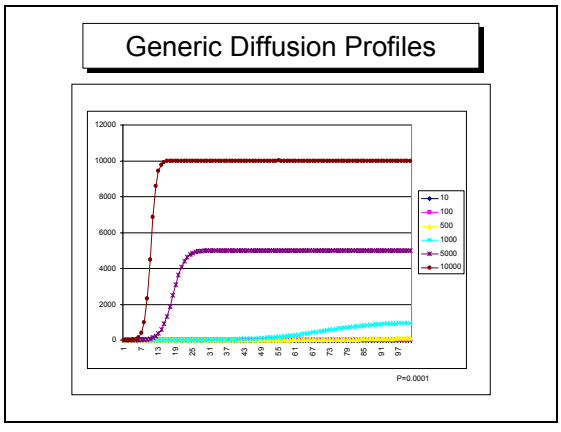

Figure 36 - Generic Diffusion Profiles: TBD

Network	# of Arcs	# of Nodes	Arcs / Nodes	*L*	1 Arc (Nodes)	2 Arcs (Nodes)	3 Arcs (Nodes)	4 Arcs (Nodes)	γ
Minimally Connected	**5**	**16**	**0.94**	**5.7**	**3**	**5**	**7**	**9**	**0**

Maximally Connected	**20**	**16**	**7.5**	**1.0**	**16**	**16**	**16**	**16**	**1**
Random	**2**	**16**	**2**	**1.9**	**5.1**	**12.1**	**15.9**	**16**	**0.17**
"Regular"	**32**	**16**	**2**	**2.3**	**5**	**9**	**13**	**16**	**0.25**
Small World	**32**	**16**	**2**	**1.9**	**5**	**12**	**16**	**16**	**0.25**
Random with Growth	**5**	**16**	**0.94**	**3.0**	**2.8**	**5.9**	**9.4**	**12.3**	**0.12**
Preferential Attachment	**5**	**16**	**0.94**	**2.5**	**2.9**	**8.0**	**13.9**	**15.8**	**0**

Table 1 - Network Properties

I don't understand the "1 Arc" through "4 Arc" columns in the network statistics table. If I traverse one arc (by definition the connection between two nodes), I will have only reached one node, won't I?

[1] Lanchester critique reference here.
[2] James G. Taylor, Lanchester-Type Models of Warfare, (Monterey, CA: U.S. Naval Postgraduate School, 1980).
[3] Wayne P. Hughes, "A Salvo Model of Warships in Missile Combat Used to Evaluate Their Staying Power," Warfare Modeling, (Danvers, MA: John Wiley & Sons, Inc., 1995), pp. 121-143.
[4] **TBD** Johns, **TBD**, (**TBD**: **TBD**, **TBD**), p. **TBD**.
[5] **TBD** Ho, **TBD**, **TBD**, (**TBD**: **TBD**, **TBD**), p. **TBD**.
[6] Arthur K. Cebrowski, and John J. Garstka,; "Network-centric warfare: it's origin and future", (U.S. Naval Institute Proceedings, January 1998).
[7] David S. Alberts, John J. Garstka, and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, (Washington, DC: National Defense University Press, 1999). See also 2d ed. Rev., 2001. Available online: <http://www.dodccrp.org/NCW/NCW_report/start.htm> ; and David S. Alberts, John J. Garstka, Richard E. Hayes, and David A. Signori, Understanding Information Age Warfare, (Washington, DC: CCRP Publication series, 2001), p. **TBD**. Available online: http://www.dodccrp.org/NCW/NCW_report/start.htm.
[8] Bradley A. Fiske, The Navy as a Fighting Machine (rev. ed.), (Annapolis: United States Naval Institute, 1988), pp. 375-376.
[9] Alberts, et al, pp. 250-256.
[10] Richard Darilek, Walter Perry, Jerome Bracken, John Gordon, and Brian Nichiporouk, Measures of Effectiveness for the Information-Age Army, (Santa Monica, CA: RAND, **TBD**), p. **TBD**.; and Walter Perry, Robert W. Button, Jerome Bracken, Thomas Sullivan, and Jonathan Mitchell, Measures of Effectiveness for the Information-Age Navy: The Effects of Network-Centric Operations on Combat Outcomes, (Santa Monica, CA: RAND, 2002), p. **TBD**.
[11] David Ronfeldt and John Arquilla (Ed's.), Networks and Netwars: The Future of Terror, Crime, and Militancy, (Santa Monica, CA: RAND, 2001).
[12] Bill Marchuck (sp?), TBD
[13] In this paper, the word "network" refers to graph theoretic (arcs and nodes) representation of systems, not necessarily to information technology (IT) network structures.
[14] Newman, M.E.J.; "The structure and function of complex networks", (**TBD**).
[15]

[16]

[17] Kauffman, *At Home in the Universe,* p. 54-7.

[18]

[19] Alberts, et al, p. 256.

[20] See http://www.santafe.edu/sfi/research/focus/robustness/index.html, accessed 11 Oct 2002, for a deeper technical treatment of robustness.

[21] Watts, *Small Worlds.*

[22] Ibid.

[23] Barabasi, *Linked: The New Science of Networks,* Chapter 6.

[24] Ibid, Chapter 11.

[25] Ibid, Chapter 6.

[26] See Oz Shy, *The Economics of Networked Industries,* (Cambridge University Press, New York, 2001), and Barabasi, Chapter 7.