AN INFORMATION AGE COMBAT MODEL

Jeffrey R. Cares
Alidade Incorporated

Produced for the Director, Net Assessment, Office of the Secretary of Defense
Under Contract TPD-01-C-0023
30 September 2004

ABSTRACT

This paper contains a formal description – a "model" – of the structure, dynamics and operational evolution of Information Age combat. It reviews the assumptions underlying extant (Industrial Age) combat models and discusses their potential applicability in the Information Age. Recent developments in combat modeling are reviewed. An Information Age Combat Model derived from the first principles and scientific fundamentals of distributed, networked systems is introduced and the mathematics of its structure, dynamics and operational evolution are presented. Implications of the model for policy assessment, concept development and systems engineering are discussed and suggestions for further research are explored. A technical appendix is included.

1 INTRODUCTION

Humans create a variety of collective schemes to achieve commercial, social or political tasks. With the development of modern information technology, these schemes and their patterns of human interaction began changing in transformational ways. Whether the change is manifested by a business professional conducting real-time collaboration with partners across the globe, youngsters pairing off against each other in virtual video games or an underdog candidate reinvigorating the electoral process with online, grass-roots campaigning, no aspect of society seems immune from the revolutionary impact of IT-enabled networks. The military is no different. Commanders who once relied on physical proximity or rigid hierarchy to pierce the fog of war can now use robust communications networks to disperse their forces and coordinate their behavior in real time, generating massed affects.[1] These two factors – distributed forces and networked control – hold the promise to revolutionize all aspects of warfare. The military profession, however, still lacks a suitable analytical model for describing distributed, networked combat.[2]

Despite the absence of a coherent Information Age theory of combat, significant recent research devoted to understanding distributed, networked systems in other domains can provide a starting point for a formal discussion of IT-enabled military networks. This research is providing new insight into the structure, dynamics and evolution of such systems as protein interactions,[3] the internet,[4] the worldwide web,[5] scientific collaborations,[6] ecological food webs,[7] open source software[8] and patterns in motion picture actor employment.[9] This work has identified new classes of network structures. A catalog of statistics has been developed to describe the most important characteristics of these new classes.[10] While ongoing research has focused on the many variants of distributed, networked systems in non-military contexts, this paper is the first effort to apply these new developments in network mathematics to distributed, networked military systems.

The paper is organized as follows. Section 2 starts with a review of contemporary combat models and describes their structure and potential for use in the Information Age. Section 3 defines the fundamental structure of networked combat, concluding that this structure constitutes the rudiments of an Information Age Combat Model. Section 4 shows how the elements in the fundamental structure conspire to create dynamic, networked effects. Section 5 explains how the structure and dynamics of a combat network can evolve as networked elements competitively interact in complex environments. Following a discussion in Section 6 of the implications and potential applications of the

Information Age Combat Model, Section 7 concludes by summarizing the main points of the paper and recommending topics for future research. Since the fundamental mathematics of the Information Age Combat Model is not well-known to the military community, a technical tutorial on recent advances in network theory is included as an appendix.

2 COMBAT MODELING

A common mistake in many defense decision-making contexts is that "modeling" is conflated with "simulation." While an increasing number of operational and executive decisions depend on the results of a growing list of large, complex computerized renditions of combat, only a small fraction of analysts who use these "simulations" fully understand the mathematical relations, or "models," that drive them. This can impart a false sense of formality and validity to the decisions the models support. Analysts often endorse analytical results as having come "from the simulation," as if that fact alone constitutes analytical validity. The match between the mathematical guts of a simulation and structure of the problem being simulated is often ignored. Despite widespread agreement in the importance of verification, validation and accreditation (VV&A) of simulations, VV&A is inconsistently applied in practice – particularly with regard to the suitability of mathematical models to represent real-world processes.[11] A new challenge has also arisen: mathematical models for new types of distributed, networked processes are not yet well developed. Analysts can only approximate new behaviors with old simulations, exacerbating the modeling-simulation conflation.

This section reviews mathematical models that are commonly used in warfare analyses and explores whether they have the potential to describe Information Age combat processes. The section will begin with a discussion of the assumptions underlying existing warfare models and continue with an assessment of the analysis community's ability to describe Information Age warfare. As part of the assessment, this section will define the characteristics of a model that sufficiently describes and supports understanding of Information Age combat processes.

2.1 Types of Combat Models

Although there is great variety in the specific application of combat models, the fundamental structure of most combat models is one of two basic types: deterministic (closed-form) or stochastic (probability-based) combat models.

Deterministic Models. A deterministic model is one that fully describes all states in a given system with a set of closed-form equations. For example, Newton's Second Law, *f=ma,* which defines force, *f*, as the product of mass, *m*, and acceleration, *a*, does not admit for randomness or uncertainty in the mathematical representation of force. Because it completely "determines" theoretical relationships in a closed-form representation, the Second Law equation is a deterministic model. Deterministic models were particularly useful before digital computers made automated calculations more routine for the analysis of large, intricate systems.

Stochastic Models. Starting in the 1970s, the widespread use of digital simulation facilitated the inclusion of randomness and uncertainty in analytical models. A model that explicitly includes randomness and uncertainty is called a stochastic model; stochastic models are usually created by modifying one or more of the terms in a deterministic equation with random draws from some probability distribution. These models are run a certain number of times so that some of the effects of randomness or uncertainty cancel out and model results converge to stable, aggregate statistical values.

2.2 Assumptions in Deterministic and Stochastic Models

It has been said that all models are wrong, but some models are useful.[12] All models must be wrong because they cannot represent the infinite detail of the real world. Modelers must therefore decide which details to include in a representation and which details to exclude. Details that are included are said to be *explicitly* represented and the excluded detail is *implicitly* represented. After decisions about representation detail are implemented, a model is *useful* if it captures the essence of real world processes sufficiently so that one understands the real world better after the model was constructed than before.[13] If the real world changes significantly, the model can be rendered useless. Of course, the underlying assumptions of deterministic and stochastic models can also impact their usefulness.

Assumptions in Deterministic Models. Deterministic models are complete, closed form specifications of a system. Obviously, one cannot practically write an equation for every possible state or interaction that is observable in the process being modeled, so implicit representations necessarily abound. One of the most prevalent implicit representations in deterministic models is aggregation and dis-aggregation: modelers assume complex interactions at fine scales can be well represented at coarser scales by homogenizing behaviors and aggregating their effects. Aggregation relegates the differences in local behaviors throughout a system to a type of noise that can be represented by a parameter without loss of usefulness. Dis-aggregation is more challenging: it assumes coarser scale parameters can be reduced to pockets of differentiated local behavior. Aggregation and dis-aggregation assumptions apply to more than performance parameters: they assume that environmental conditions and localized tactics can be likewise aggregated and dis-aggregated.[14]

Another assumption prevalent in deterministic models is regularity. This assumption requires that grossly non-linear outcomes should not be triggered by small changes in input values. For example, doubling the value of an input should roughly equate to a doubling of its effect in the model and not, say, decreasing its effect by a factor of ten.

Finally, command, control or competitive processes are rarely explicitly represented in deterministic models. These effects are usually implied by such devices as the mathematical relationships between terms or the relative sequence in which processes are represented.[15]

Assumptions in Stochastic Models. Stochastic models also contain aggregation and regularity assumptions analogous to those found in deterministic models. Stochastic models have three additional significant assumptions. The first assumption stems from a basic problem in modeling uncertainty: since uncertainty implies incomplete knowledge of the input data required for a model, then some input parameters must be random variables. The second assumption flows from the first: since the data itself is to some extent uncertain, so are the interactions between inputs: the parameters must therefore be treated as independent random variables. In other words, complex chains of causality in the operational processes being modeled are considered inconsequential. It is assumed that most processes can be modeled as either independent events or as chains of simple causality.[16] Third, modelers frequently assume that the distribution of outcomes for these independent random variables is not so skewed that a relatively small number of model runs will mitigate variation in the random variables and produce statistical convergence.[17]

Command and control is more explicitly represented in stochastic models than in deterministic models. Stochastic models typically represent C2 processes in the same way other processes like attrition are represented, with draws from a probability distribution. A classis example of stochastic C2 modeling can be found in Anti-submarine Warfare (ASW) simulations. Initial detection of, say, a submarine by a surface ship sonar is drawn from a probability distribution, as is the probability that the submarine transitions from detection to tracking. As the simulation proceeds, a random draw is taken at specified time steps to determine if the ship continues tracking the target or, alternatively, if the submarine becomes undetected, whereupon the initial detection probability distribution is again invoked. Other types of C2 processes, such as communication, radar detection, etc., are treated in a similar manner.

2.3 Common Combat Models

Some of the earliest deterministic attrition models described continuous fire combat, where one side erodes the combat power of another at some fixed rate over time. The most prevalent example of a deterministic combat 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.[18] In brief, Lanchester theorized 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 its shooters. Using differential equations, Lanchester Equations prescribe such results as the ultimate winner of a contest between combatants, the time required for a duel to conclude or the size of each force remaining at a duel's conclusion. This model is the basis for most of the current attrition-based combat simulations in use today. Indeed, there are dozens of variants of Lanchester's model representing ground or air combat processes in use today.[19] TACWAR is a prominent deterministic ground and air combat simulation that employs Lanchester equations as its underlying attrition model.[20]

Traditional stochastic combat models represent combat as a chain of independent events (each with their own probability of occurrence) or as sets of basic interaction equations (with random variables representing operational processes). Two popular uses of stochastic models are for representing undersea warfare (such as described in the previous section) and air defense. The Naval Simulation System (NSS),[21] the Extended Air Defense

Simulation (EADSIM)[22] and Joint Warfare System (JWARS)[23] are three prominent stochastic combat simulations that use stochastic modeling techniques.

2.4 Salvo Models

In the late 1980's Hughes brought combat modeling into the Missile Age by developing an attrition model inspired by the exchange of striking power during the World War II Battle of Midway. His Salvo Exchange model described combat as a pulse of offensive combat power designed to instantaneously penetrate an adversary's active defenses and cause damage to an adversary's platforms.[24] Although this model has important descriptive power, two major drawbacks to its predictive power are that it only holds for identical, homogeneous forces for all sides and it is strictly deterministic. Of course, homogenous force-on-force scenarios would be rare, and deterministic, instantaneous attrition obscures the importance of sensing or the sequencing of attacks.

These shortfalls were later addressed by introducing a version for heterogeneous forces as well as a stochastic variant.[25] The heterogeneous variant required a high-dimensional "matching matrix" to define every interaction between elements of offensive combat power, defensive combat power, and staying power, but the problem of deterministic, instantaneous attrition remained. The stochastic version only worked for homogenous forces. Although these two variants were never combined into a stochastic, heterogeneous salvo model, such an exercise would be largely academic and impractical. In short, a full description of the matching matrix would be tantamount to an *a priori* description of all salvo exchanges and would obviate the need for the model to begin with.

One powerful feature of the salvo model is its use for explicit calculations of "combat entropy," a very normal condition of warfare. Combat entropy stems from the uncertainties of combat and results in sub-optimal 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.[26]

2.5 Suitability of Common Combat Models to Describe Information Age Combat

Industrial Age combat was characterized by limited communications, massed forces, and centralized command, control and decision making. Since information was difficult to obtain and hard to share, commanders relied more on force than on a deep insight into tactical intricacies. Although important exceptions existed such as Fleet Anti-air Warfare, which pioneered rudimentary digital networks more than three decades ago, a more prevalent sentiment was exemplified by the Soviet Red Army, who insisted on a 3:1 force advantage before ever going on the offensive.[27]

Information technology and computer networks have been introduced into military processes to improve on this brute force approach by exchanging information for physical force where appropriate. As a result of these efforts, military systems are increasingly characterized by dispersal of physical assets, information distribution and decentralized cognition. A new value system is emerging where arrangement of distributed, networked assets is more important than mere massing of force.

Since they have no better tools, defense analysts continue to use traditional models to simulate new, Information Age operational concepts. Sometimes these models are embellished with additional C2 parameters (in the case of deterministic models) or the addition of C2 statistical terms (in the case of stochastic models). Newer efforts such as JWARS have attempted to more explicitly capture the most important command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) operations. However, the underlying philosophy of models like JWARS has not departed from merely modifying traditional attrition models with C2 parameters or processes. Existing models have failed to represent the impact of new forms of command and control on combat outcomes because they are all based on physical models of attrition. In these physical models of attrition, advantage accrued by arrangement of assets is devalued in favor advantage accrued by greater numbers of assets. For this reason, none of the common models discussed here are suitable candidates for an Information Age combat model.

2.6 Network Centric Warfare Modeling

A newer set of models has been described by researchers attempting to add more specificity to the concept of Network Centric Warfare, the predominant theory of warfare in the Information Age. Cebrwoski and Garstka introduced the Network Centric Warfare (NCW) concept in 1998. They describe how the military must shift from platform-centric to network-centric combat, 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 square of the number of nodes in a network. This power comes from "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.[28] 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.[29] In general, the NCW literature has never graduated beyond weak metaphor or the type of "glittering generalities" that motivated frustrated Victorians to finally develop traditional attrition-based models.[30] In no case are the mechanisms of advantage for NCW defined with enough specificity to produce meaningful research, scientifically valid experimentation or rigorous concept development. Some NCW modeling efforts to date include:

- Use of IT industry models. The most prevalent of these is in the basic NCW text, which suggests that warfare will be conducted according to "Metcalf's Law."[31] Recent research into network theory shows that this is a naïve assumption – networked behavior is far more complex then a simple count of potential connections.
- Textual Descriptions. Attempts to describe self-synchronization in detail assert that rule sets and shared awareness produce self-synchronization. Counter to this assertion, however, is research that mathematically proves self-synchronization can occur without a common rule set or without shared awareness.[32] There are many more examples in the NCW literature of imprecise textual models that do not hold up against more formal mathematic treatment.
- Booz-Allen & Hamilton's Entropy Based Warfare Model.™ At its core this simulation consists of Lanchester's attrition-based equations with additional tuning parameters. Ironically, if one knew the value of the tuning parameters there would be no need for the combat model. This model is poor representation of combat entropy[33] and is a traditional attrition-based model with Industrial Age assumptions.[34]
- RAND studies on NCW measures of effectiveness (MOEs) for the Army and Navy suffer from the same deficiency as Entropy Based Warfare (EBW) work – they attach Information Age tuning parameters to what is essentially an Industrial Age model.[35]
- Description of "Netwar" by Arquilla and Ronfeldt.[36] Although this work is valuable for its use of networks as metaphors, their descriptions of the dynamic behavior of networks does not correspond with the technical literature.
- Research on Complexity Theory and Network Centric Warfare by Moffat.[37] This work disregards whole thematic topics in complex systems research and focuses too narrowly on agent-based modeling and the RAND NCW research mentioned above.

As these examples show, the NCW modeling efforts to date are also unsuitable candidates for an Information Age combat model.

2.7 Transformation in Modeling Philosophy

The basic structure of contemporary combat models is over 100 years old and a direct product of Victorian Era science, technology and philosophy. It is clear that these models, described in the previous sections, are inadequate for representing Information Age warfare. To summarize, they are inadequate for three main reasons:

- A process that can aggregate and dis-aggregate fine-scaled behaviors by definition must treat these local behaviors as noise at the aggregate level. Such a process cannot adequately represent local arrangement of elements, clever use of information or massed effects from distributed forces. These, of course, are all important Information Age Warfare precepts.
- The models rely on mathematics that represent combat activities as independent processes. Networked processes are by definition inter-dependent.
- The distribution of networked performance is highly skewed as feedback loops create "tipping point" behaviors.[38] Although NCW concepts are said to capitalize on this fact, contemporary models actually enforce regularity and depend on

less-skewed performance distributions. As mentioned above, standard stochastic modeling techniques depend upon statistical convergence in a moderate number of runs. Simulations that contain models with skewed distributions require an exhaustively large number of runs for statistical representation.

An Information Age combat model will require a transformation in military modeling philosophy and must therefore address these challenges by properly representing complex local behaviors, explicitly representing interdependencies and capturing the skewed distribution of networked performance. In addition, an Information Age combat model must capture both the attrition processes and the search and detection processes important to distributed, networked warfare. Such a model would be a bona fide transformation in combat modeling philosophy and constitute a true Information Age Combat Model.

3 STRUCTURE OF THE INFORMATION AGE COMBAT MODEL

The objective of this paper is to propose an Information Age Combat Model that satisfies the requirements of this transformation in combat modeling. Since the model must explicitly address networks, the section will briefly introduce the topic of networks and then describe and develop the basic structure of the proposed model.[39]

3.1 Mathematical Structure of Networks

The term "network" has become a ubiquitous synonym for any connected system; other synonyms like "grid," "chain" or "mesh" are likewise creeping into operational language. Very few who use these words exhibit understanding that the terms have very specific technical definitions. Although a detailed review of the mathematics of networks is included as an appendix, it is worth discussing an example here. A "grid," for example, is technically a "lattice of degree four," which means there are exactly four links connected to each node. This means there are no shortcuts in a grid and it has a very rigid structure, properties, among others, that make it a poor candidate for a real operational network. The popularity of this term as a descriptor for operational military networks suggests that it is used metaphorically rather than technically, but the fact that it is not even a good metaphor seems to be missed altogether. This is not an arcane distinction – one should care about the specific mathematical properties of a network for two very practical reasons. The first reason is that different networks have dramatically different properties, and blindly choosing a network type simply because it is popular is the worst kind of engineering, resulting in systems with the wrong properties for the tasks they are required to perform. Second, many of the characteristics which concept developers ascribe to new operational concepts, such as "adaptation," "self-synchronization," "networked effects" or "robustness," have specific mathematical definitions that can be derived from the science of networks. Any model of distributed, networked combat that ignores the mathematics of networks would therefore inappropriately represent combat in the Information Age.

3.2 Basic Combat Network Structure

Distributed, networked warfare should be represented as a "combat network." The resulting Information Age Combat Model should have the mathematical structure of a network, which at its most basic level is represented by *nodes* connected with *links*.

For the purpose of an Information Age Combat Model, *nodes* are defined as elements in a process that are *sensors*, *deciders*, *influencers*, or *targets*. By definition, sensors receive observable phenomena from other nodes and send them to deciders. Deciders receive information from sensors and make decisions about the present and future arrangement of other nodes. Influencers receive direction from deciders and interact with other nodes to affect the state of those nodes. A target is a node that has some military value but is not a sensor, decider or influencer. In addition, all nodes have a characteristic called "side" (e.g., blue, red; friend, foe, neutral; etc.).

Nodes can be "contracted" so that the functions or values of more than one node can be contained in a smaller number of nodes. For example, a single node can contain the attributes of a sensor, influencer, decider or a target. This allows for representation of a decider and sensor on the same platform.

Contracting a group of sensors, deciders, influencers, and targets into a group of nodes (with one sensor, decider, influencer and target each) leads to an interesting result that approximates Lanchester equations. This shows the potential for a very helpful result of the network model approach: if traditional models can be represented using this framework, then traditional warfare and distributed, networked warfare can be compared using the same model. This comparison is currently impossible with existing models.

Nodes are linked to each other by directional connections called "links." An example of a link is an observable phenomenon that emanates from a node and is detected by a sensor is a link. In this case, links might be radio frequency (RF) energy, infrared signals, reflected light, communications or acoustic energy. Phenomena detected by sensors are communicated to deciders, constituting another kind of link. Deciders issue orders to nodes and influencers interact with other nodes, typically in an effort to destroy or render useless those nodes. These are further examples of links. Note that links are not necessarily IT connections between nodes, but represent something more functional – the operative interactions between nodes.

3.3 Combat Networks

The links and nodes as defined above constitute a combat network. Figure 1 graphically represents the most basic combat network, while Figure 2 represents a two-sided system. The use of different line styles in these figures underscores that the links are not homogenous. For clarity, these styles will be omitted in later figures. In addition, the nodes on each side are represented by different colors.

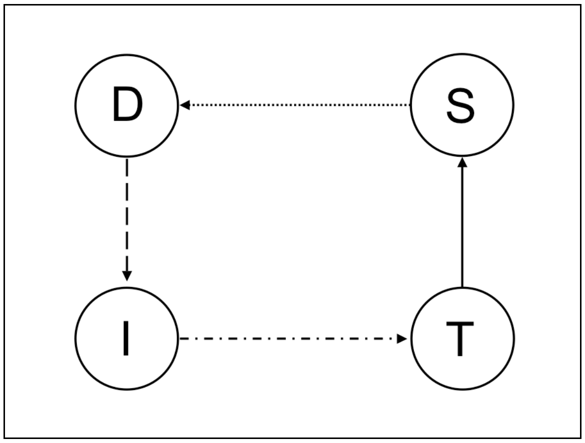


Figure 1 - Simplest Combat Network

The relationships in the networks in Figure 1 and 2 have the following characteristics:

- Sensor logic does not equate to decision-making capability
- All sensor information that passes to an influencer must do so through a decider; "sensor-to-shooter" is allowed, "sensor-to-bullet" is not
- Targets can be vehicle platforms without sensing, influencing or decision making capability
- Targets, influencers and sensors are located by sensors; there is no direct path from targets, influencers or disconnected sensors directly to deciders

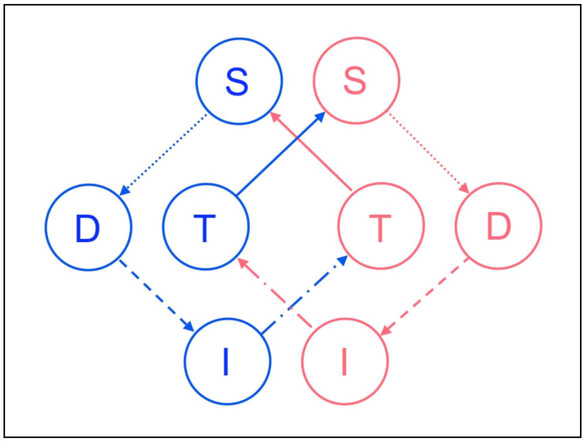


Figure 2 - Simplest Two-Sided Combat Network

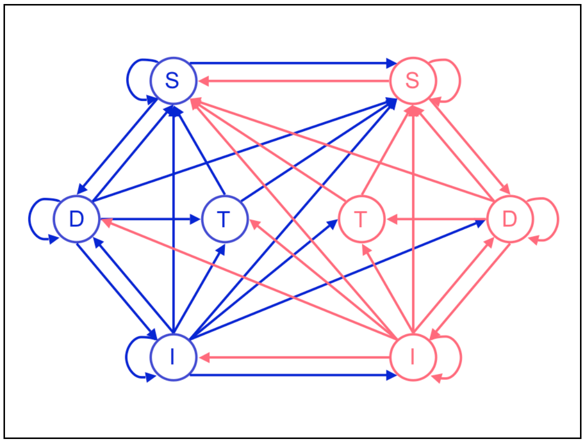
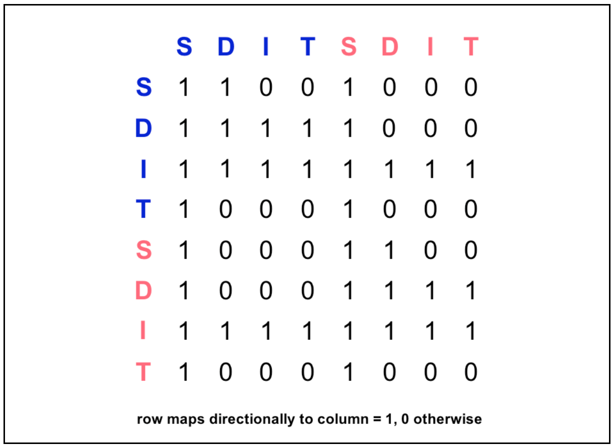


Figure 3 - Simplest Complete Combat Network

Figure 3 represents the simplest complete combat network that is created from these assumptions. This diagram represents all the ways that sensors, deciders, influencers and targets interact meaningfully with each other.

3.4 Dimensions and Complexity

The two dimensional surface of this paper obscures the inherent complexity of this "simple" network: there are at least 36 different dimensions in which this network operates. This dimensionality is more evident in a different type of network representation, the *adjacency matrix.* The adjacency matrix in Figure 4 is an equivalent representation of the network in Figure 3. A "1" in the matrix indicates that there is a link from node listed at the head of the row to the node listed at the head of the column. A "0" indicates that there is no link between those nodes. Note that the connections are directional from rows to columns. For example, the blue side "I" has a link from its own side's decider, D, and the red side influencer, I, but not from its own side's sensor, S, or target, T, or from the red sensor, S, decision node, D, or target, T. Counting up all the matrix entries filled with a "1" provides the dimensionality of the simplest, complete combat network, 36. Recall that this is the simplest complete model; one could include many more targets, sensors, decision nodes, and influencers.



	S	D	I	T	S	D	I	T
S	1	1	0	0	1	0	0	0
D	1	1	1	1	1	0	0	0
I	1	1	1	1	1	1	1	1
T	1	0	0	0	1	0	0	0
S	1	0	0	0	1	1	0	0
D	1	0	0	0	1	1	1	1
I	1	1	1	1	1	1	1	1
T	1	0	0	0	1	0	0	0

row maps directionally to column = 1, 0 otherwise

Figure 4 - Adjacency Matrix

Not only is this structure high dimensional, but it is also complex, in the sense that there is an extraordinary large number of different sub-networks that can be created from this combat network. In general, the number of different sub-networks that can be created from an N x N matrix is $2^{(N^2)}$. This number gets very large even for small values of N. Figure 5 is a plot of $2^{(N^2)}$.

Values of N larger than 17 can create more possible sub-networks then there are particles of matter in the known universe (Ω, in Figure 5). Trying to find the best arrangements of nodes and links in this huge space of possibilities can be quite exhaustive. There is some relief, however, in that the adjacency matrices created by combat networks are in a class called "sparse matrices." This means that for the simplest complete combat network only a fraction of the 1,844,670 billion billion possible sub-networks are actually formed.

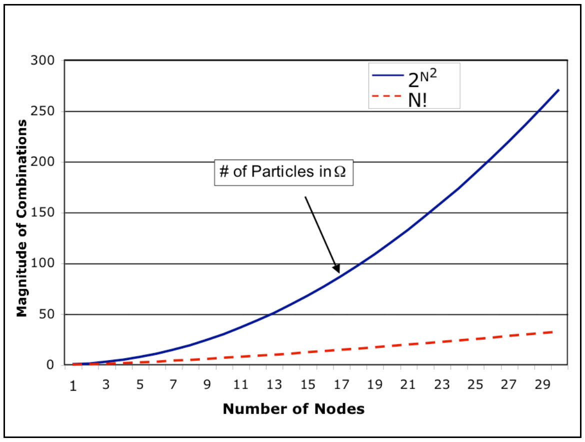


Figure 5 – Network Dimensionality

4 DYNAMICS

An understanding of networked behavior comes from recognizing that dynamic behaviors are not found in static structure but result from the interactions of nodes over links. Specific arrangements of links and nodes that create value are "cycles," sub-networks in which the functions of nodes flow into each other over a path that revisits at least one node once. If there are no cycles in a network, then no useful networked function is completed. If there is to be advantage in using networked forces it must arise from these dynamic, often *autocatalytic* networked effects. Current NCW literature and contemporary combat models do not adequately describe these effects.

Not all collections of links and nodes, however, create cycles. Sub-networks with one or two nodes are not very robust or survivable as networks and would be more rare than fuller cycles. For example, a single sensor disconnected from a combat network is a sub-network of the larger set, but is not interesting from a combat network perspective. The same is true of a simple target-sensor pairing. These are known as 1- and 2-cycles, respectively. 3- and higher-dimension cycles contribute more to networked effects. In the Information Age Combat Model, there are of four general types of cycles.

4.1 Types of Cycles

The first type is a *control cycle* that accomplishes direct control of a side's assets. Figure 6 displays three control cycles. Cycle A is a control cycle where the decision node, D, implements direct control of a first sensor S_1. A second sensor, S_2, receives phenomena from S_1 (perhaps locating data about S_1) and reports it to D. D can then change the position of S_1, which completes the cycle. Similarly, Cycle B is a representation of a control cycle where sensor S receives information from target T and passes that information to decider D, which can then send a control signal to T. In the third cycle, C, decider D sends an order to influencer I. Phenomena concerning I's state are detected by S, which communicates back to D, who now can continue the cycle by sending another control signal to I.

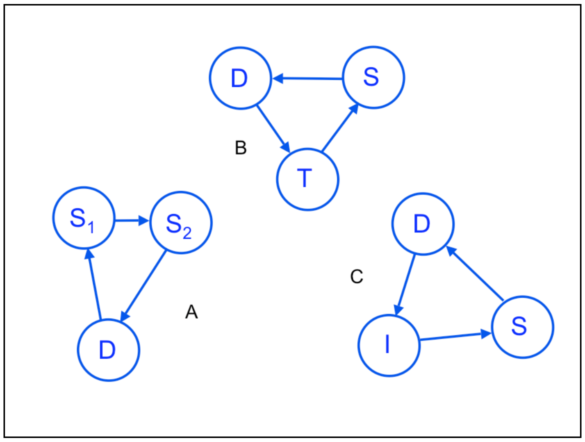


Figure 6 – Control Cycles

The second type of cycle is a *catalytic control cycle* in which one side's assets are controlled based on information about the states of other assets on that side. Figure 7 shows three catalytic control cycles. In catalytic control cycle A, D controls sensor S_2 while sensor S_1 receives information from both S_2 and target, T, and reports it to D. In this case, D may be seeking, say, to place S_2 farther away from itself than S_1, perhaps to better sense near T. D's decision about S_2 is directly influenced by S_2 but also indirectly influenced, or "catalyzed," by information about T. Similar catalytic control activity can be observed in Cycles B and C.

The third type of cycle is a *catalytic competitive cycle* that represents control of one side's assets based on information about one's own assets (side "x" in the diagrams) and a competing side's assets (side "y"). Figure 8 shows two catalytic competitive cycles.

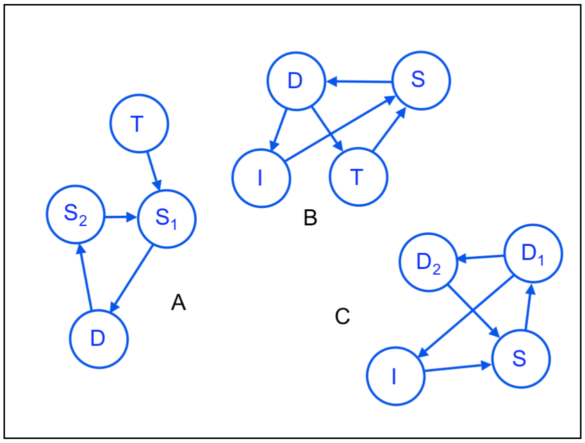


Figure 7 – Catalytic Control Cycles

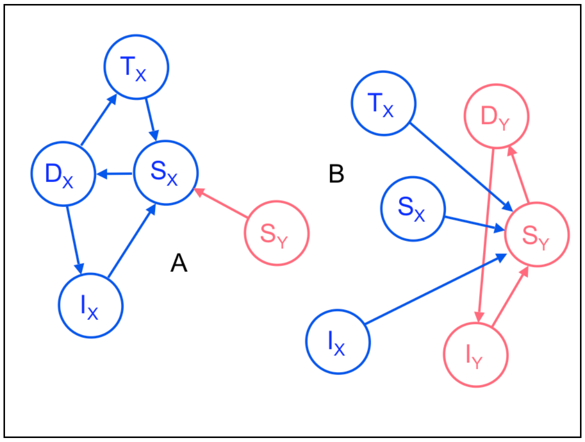


Figure 8 – Catalytic Competitive Cycles

In catalytic competitive cycle A, D_x controls T_x and I_x. S_x discerns the geolocation of S_y, T_x, and I_x, and relays it to D_x. D_x uses this information to relocate T_x and I_x. This movement is recognized by S_x and reported to D_x, completing the cycle. In example B, similar catalytic control occurs when D_y controls I_y based on a report by S_y of the activity of T_x, S_x, and I_x.

The fourth type is a *combat cycle* that represents application of combat power from one side to another (or accidental application from one side to itself). Figure 9 portrays two 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 I_x. 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 I_x, 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.

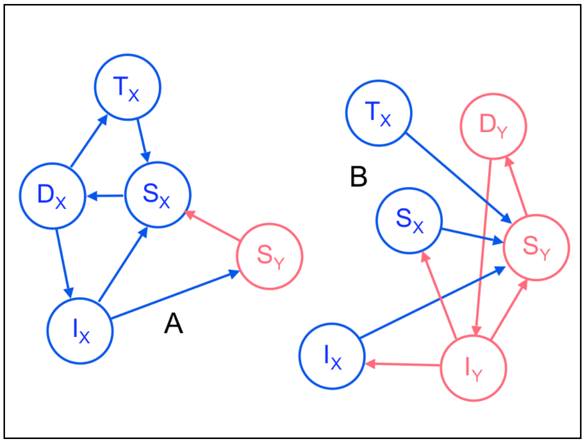
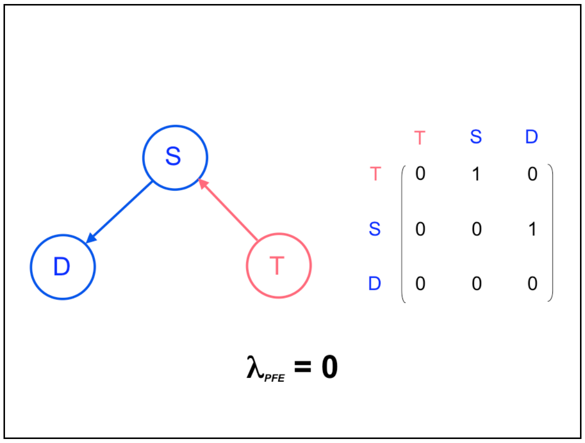


Figure 9 – Combat Cycles

4.2 Measuring Networked Effects

Various mathematical operations can be performed once a network has been converted to a matrix representation. A very rich and formal field of mathematics exists to perform these operations. One of the most useful operations is the calculation of eigenvalues. An eigenvalue, usually denoted by the Greek symbol λ, is a measure of the value of the network and is derived from the adjacency matrix.[40]



$$\begin{array}{c|ccc} & T & S & D \\ \hline T & 0 & 1 & 0 \\ S & 0 & 0 & 1 \\ D & 0 & 0 & 0 \end{array}$$

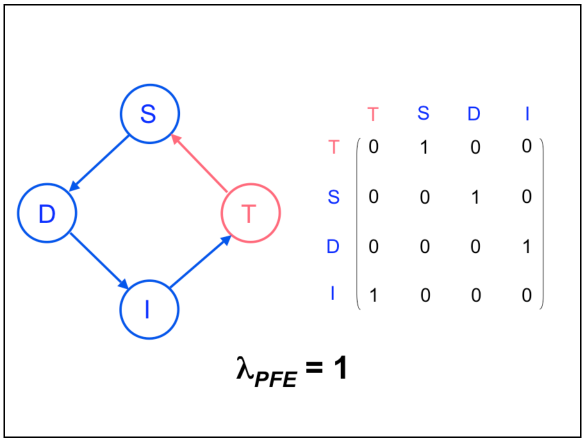
$$\lambda_{PFE} = 0$$

Figure 10 – Network with No Cycles

The adjacency matrices that describe the Information Age Combat Model 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.[41]

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 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 network structure over and above the simple cycle in Figure 11. Such additional links 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 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 (ACSs) because the additional structure creates feed-forward and feedback linkages that autocatalytically create networked effects.

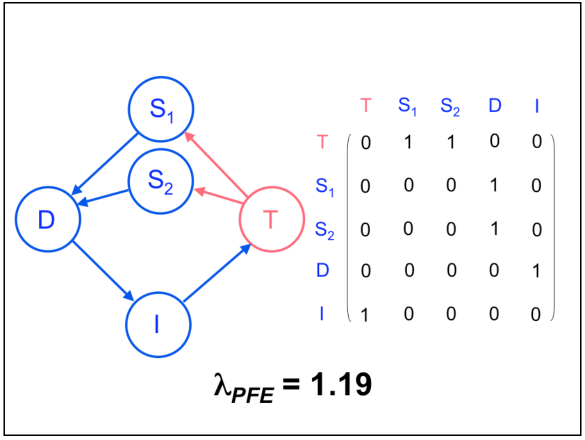


$$\begin{array}{c|cccc} & T & S & D & I \\ \hline T & 0 & 1 & 0 & 0 \\ S & 0 & 0 & 1 & 0 \\ D & 0 & 0 & 0 & 1 \\ I & 1 & 0 & 0 & 0 \end{array}$$

$$\lambda_{PFE} = 1$$

Figure 11 – Network with a Single, Simple Cycle

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 a link and a node to the basic structure in Figure 12 does not change the value of the PFE. The structure in Figure 12 is known as the "core" process of the network in Figure 13. A core is the set of links and nodes that contains all the mechanisms for networked effects in a network. Additional links and nodes that do not contribute to an increased PFE are called "peripheral" links and nodes. In larger networks, however, it is possible to have more than one core.

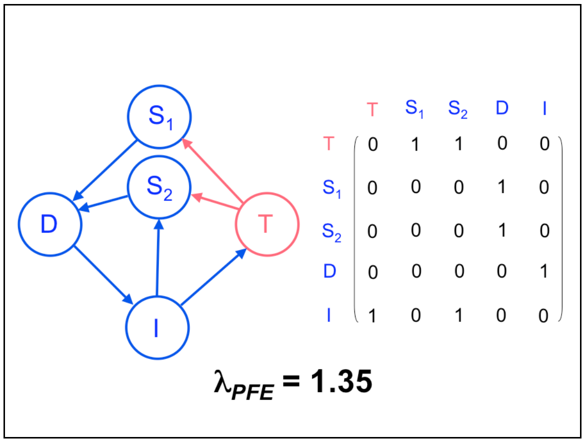


$$\begin{array}{c|ccccc} & T & S_1 & S_2 & D & I \\ \hline T & 0 & 1 & 1 & 0 & 0 \\ S_1 & 0 & 0 & 0 & 1 & 0 \\ S_2 & 0 & 0 & 0 & 1 & 0 \\ D & 0 & 0 & 0 & 0 & 1 \\ I & 1 & 0 & 0 & 0 & 0 \end{array}$$

$$\lambda_{PFE} = 1.19$$

Figure 12 – Network with an Autocatalytic Set (ACS)

Since the largest possible PFE for an N x N adjacency matrix is N, then the networked effects of networks of different sizes can be compared using the ratio PFE/N, which we define here as the Coefficient of Networked Effects (CNE). CNE ranges in value from 1/N to 1.

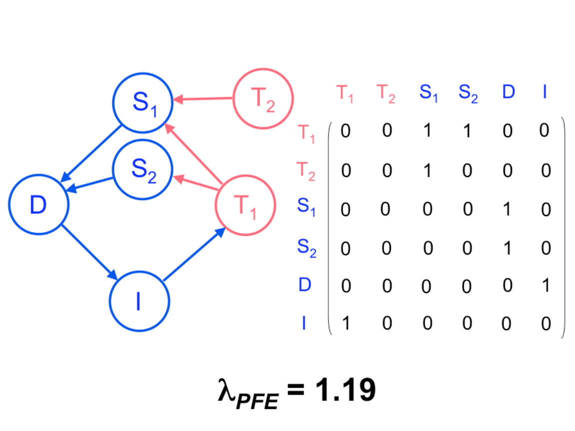


$$\begin{array}{c|ccccc} & T & S_1 & S_2 & D & I \\ \hline T & 0 & 1 & 1 & 0 & 0 \\ S_1 & 0 & 0 & 0 & 1 & 0 \\ S_2 & 0 & 0 & 0 & 1 & 0 \\ D & 0 & 0 & 0 & 0 & 1 \\ I & 1 & 0 & 1 & 0 & 0 \end{array}$$

$$\lambda_{PFE} = 1.35$$

Figure 13 – ACS with Additional Linkages

It is clear from the examples presented here that the characteristics of a network and its potential for improved performance increase as the network grows. The next section will discuss the importance of the long timescale dynamics of a network, or "network evolution."



$$\begin{array}{c|cccccc} & T_1 & T_2 & S_1 & S_2 & D & I \\ \hline T_1 & 0 & 0 & 1 & 1 & 0 & 0 \\ T_2 & 0 & 0 & 1 & 0 & 0 & 0 \\ S_1 & 0 & 0 & 0 & 0 & 1 & 0 \\ S_2 & 0 & 0 & 0 & 0 & 1 & 0 \\ D & 0 & 0 & 0 & 0 & 0 & 1 \\ I & 1 & 0 & 0 & 0 & 0 & 0 \end{array}$$

$$\lambda_{PFE} = 1.19$$

Figure 14 – ACS with a Peripheral Link and Node

5 EVOLUTION

As networks mature they grow in a way that is very unlike progressive improvement in most other systems. This section defines and describes how exploitable properties develop as a result of growth and evolution in complex networks. A type of rapid connectivity ubiquitous in networked structures will be explored, mechanisms of adaptation and learning will be defined, and convergence toward a set of descriptive statistics will be discussed. The potential for using these statistics to quantify combat network performance will be addressed.

5.1 Punctuated Growth in Complex Networks

One of the most important phenomena in network evolution is *punctuated growth*. This pattern of sudden connectivity occurs as a network matures (under competition, for purpose or in response to resource constraint) from a loose collection of a small number of nodes into a larger, more complex structure.

A simple thought experiment demonstrates the essence of this rapid growth. Imagine that there are 400 buttons and many pieces of string on a table. Imagine also that a button and a piece of string are randomly selected from the table, tied together and placed back on the table. Now imagine this process is repeated indefinitely. Eventually, a button might be selected that has a string and a button already tied to it; perhaps also a string will be chosen that was previously connected to a button. Soon the table will be populated with so many clusters of buttons and strings that at some threshold level, adding a very few additional buttons or strings will connect almost all the small clusters into one large collection (called the *giant component* of the network).

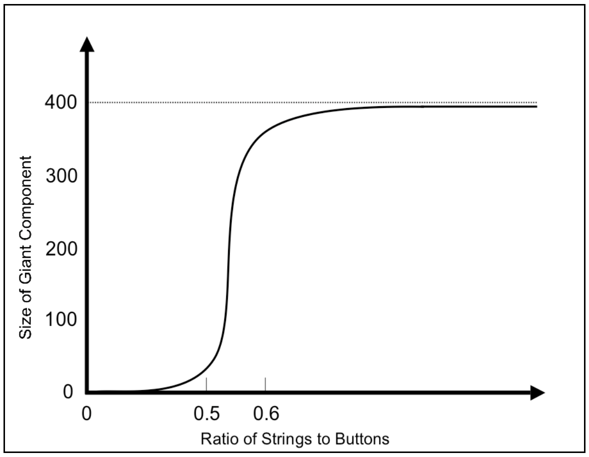


Figure 15 – Buttons and Strings

Plotting the size of the giant component against the ratio of strings to buttons more formally describes punctuated growth. The curve in Figure 15 shows that as the ratio of strings to buttons approaches 0.5, the connectivity of the buttons suddenly and dramatically increases. The curve flattens quickly after this ratio hits 0.6, 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 rapid transition from an unconnected group of nodes to a highly connected network.[42] Although the buttons and strings in this example were connected in a purely random process, other complex networks experience the same type of punctuated growth and the same "S-shaped curve is found in the growth profiles of all complex networks.

5.2 Learning and Adaptation in Complex Networks

Readers familiar with calculus-based engineering problems might look upon the curve in Figure 15 and find it quite familiar. With this traditional view, they would be mistakenly assume that the important system behaviors were occurring at the "knees" of both curves (where the curves "tip") and at the mid-point of the "S." There is *latent* structure in the part of the connectivity curve to the left of the "tipping point" at 0.5, however, that is far more important than the tipping points themselves. This latent structure is contained in the smaller clusters of nodes that eventually connect at the tipping point, but the tipping point will not occur unless this latent structure is present. In some networks, latent structure may account for up to 95% of connectivity, yet this substantial level of connectivity would not be measured in Figure 15 until a very large giant component is formed.

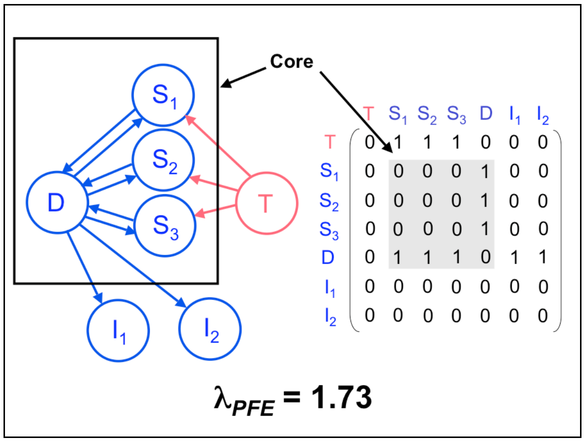
In complex networks this tail in the connectivity curve represents two distinct behaviors. The first behavior is a kind of learning, in the sense that the first small clusters of links and nodes inform the placement and connection of subsequent links and nodes (particularly in a combat network with sensors, but also in other networks that interact with the environment or a competitor). As additional links and nodes are added, the network evolves from one with no cycles to one with multiple simple cycles, and finally to one with ACSs and complex networked effects.[43]

The second behavior is adaptation. When the environment or competition changes substantially, the arrangement of links and nodes and, therefore, the networked effects can 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. While subtlety distinct from the first behavior, reactive learning, adaptation exploits the presence of latent links to help the network morph smoothly in response to environmental or competitive change. This adaptive re-configuration can be achieved in complex network with a re-wiring of only 5-10% of the links. A simple chain of links and nodes cannot be a complex network; a complex network, however, can invoke simple chains within it. Complex networks adapt, therefore by re-wiring simple chains with links selected out of latent structure. The latent structure is called "neutral" structure because it does not typically contribute to networked effects until it is incorporated into a re-wiring.

A measure of adaptability is the amount of latent structure – the amount of *neutrality* – in a complex network. This can be measured by subtracting the number of links in a simple chain of size N, N-1, from the number of links, l, in a network of size N. Dividing by N normalizes this calculation for network size and produces a statistic called the Neutrality Rating, $(l - \mathrm{N} + 1)/\mathrm{N}$.

5.3 Core Shifts in Complex Networks

Learning or adaptation profoundly affects the dynamical structure of complex networks, particularly the dynamic relocation of the cores of networked effects. In a “core shift,” the central mechanisms of networked effects move from one subset of links and nodes to another. An example of core shifts in the Information Age Combat Model follows. It portrays a combat network evolving from sensing a group of targets to attacking those targets.

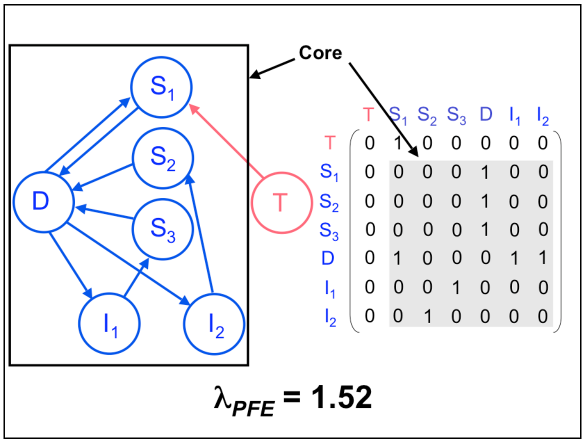


$$\begin{array}{c|ccccccc} & T & S_1 & S_2 & S_3 & D & I_1 & I_2 \\ \hline T & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ S_1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ S_2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ S_3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ D & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ I_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ I_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

$$\lambda_{PFE} = 1.73$$

Figure 16 – A Core of Sensors

Figure 16 shows a decision node controlling a group of sensors that detect a target. The core of the network is outlined by a box and the core portion of the adjacency matrix is highlighted by shading. The portion of the network outside the boxes and shading represents the presence of the two peripheral nodes (I_1 and I_2), as well as a target node (T).

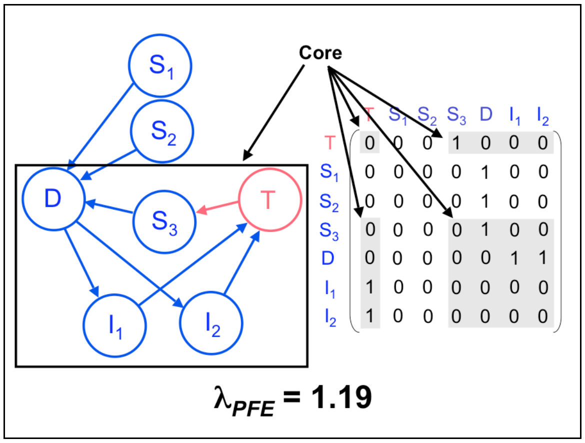


$$\begin{array}{c|ccccccc} & T & S_1 & S_2 & S_3 & D & I_1 & I_2 \\ \hline T & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ S_1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ S_2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ S_3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ D & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ I_1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ I_2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}$$

$$\lambda_{PFE} = 1.52$$

Figure 17 – A Core of Sensors and Shooters

Figure 17 shows the network adapting to sensors information by including two influencers in the coordination. Note that the core has expanded to include the influencers, and the PFE has changed as a result. Also note that this was accomplished by rewiring two control links from the sensors to the influencers and by invoking paths through two previously neutral links between the influencers and sensors. One sensor is now providing updated targeting information and the decision node has directed placement of the influencers.

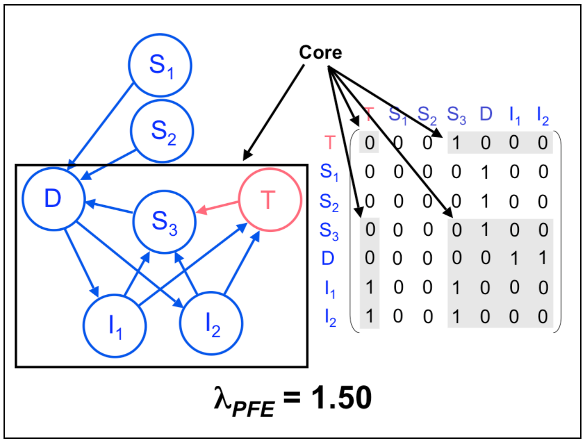


$$\begin{array}{c|ccccccc} & T & S_1 & S_2 & S_3 & D & I_1 & I_2 \\ \hline T & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ S_1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ S_2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ S_3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ D & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ I_1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ I_2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

$$\lambda_{PFE} = 1.19$$

Figure 18 – Attacking with a Core

In Figure 18, the network has initiated an attack on T. The core has shifted and is now represented in the lower right corner and along the top and left side of the adjacency matrix. Sensors S_1 and S_2 have been re-allocated to search for additional targets and longer have a role in the attack. S_1 and S_2 are now peripheral to the network but, most importantly, T is in the core. Again, the PFE has changed with this shift in the core.



$$\begin{array}{c|ccccccc} & T & S_1 & S_2 & S_3 & D & I_1 & I_2 \\ \hline T & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ S_1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ S_2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ S_3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ D & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ I_1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ I_2 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{array}$$

$$\lambda_{PFE} = 1.50$$

Figure 19 – Attack by the Core Continues

The attack continues in Figure 19: the influencers continue to engage T and their progress is reported by sensor S_3. S_3 communicates data to the decision node D, which in turn applies additional control measures 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.

5.4 Long Term Statistics of Complex Military Networks

The last three sections have detailed the three most important aspects of complex networks:

- Structure – the definition of links, nodes and connection rules

- Dynamics – the mechanisms by which networked effects are achieved

- Evolution – the behavior of the network as it adapts to its environment and to competitors

A great deal of recent study has identified a growing number of statistics that usefully describe important complex network characteristics. These statistics converge to certain ranges or distribution in the many other domains that this research has examined. Some of these statistical values can be used to determine adaptability, robustness, survivability and many other desirable properties that should be engineered into complex military networks. A more complete list of these statistics is contained in the appendix, but the most useful measures and their desirable values are listed here. These properties and their suggested values are offered 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 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 connectivity profile in Figure 15, for example, is partly a function of the number of buttons: the more buttons, the steeper the curve. One of the early, unsubstantiated claims of some network-centric military concepts was that "numbers count" – here is the evidence to support that claim.

Link to node ratio, l/N. Just as important as the number of nodes is the number of links, but NCW literature mandates that all nodes should be directly linked to all other nodes in a maximally connected network.[44] Such networks needlessly incur excessive overhead. Figure 15 shows that very good connectivity can be achieved with many fewer links than this. The lengths of paths in the network, local cohesion, survivability and adaptability also perform well in complex networks with far fewer links per node than N-1, the ratio found in maximally connected networks. As a general rule, complex networks should have about two links per node.

Degree distribution. The number of links per node, however, should not be uniformly distributed throughout a network. If a node's degree is the number of links connected to it, then complex networks should have a skew degree distribution. 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. This property is a direct result of cycles in complex networks. Skew degree distributions also are the source of remarkable property of complex networks: the largest hubs can appear, recede, and then re-appear in a different part of the network by re-wiring only about 5 to 10% of the links.

Size, connectivity of the largest hubs. A skewed degree distribution creates a very small number of very well connected nodes. The largest hub typically contains fewer than 100 links and the network can be engineered for survivability so that the largest hubs are not directly connected.

Characteristic path length. Although there can be a very large number of lightly connected nodes and only about two links per node in a complex network, the paths from each node to every other node are nonetheless relatively short. The characteristic path length measures this property, and is defined as the median (middle ranked value) of the mean of the lengths of all shortest paths in the network. This value grows only by the order of the number of nodes in the network. In other words, it takes on average only four links to reach any node from any other node in a network of 10^4 nodes.

Clustering Coefficient. Section 4 discussed the mechanism of networked effects in complex networks, cyclic compounding feedback. The best types of cycles in the Information Age Combat model are 3-cycles, because they represent shortcuts in 4-cycle T-S-D-I connections. 3-cycles also contribute to local cohesion, a very important tactical principle in military operations. Clusters of 3-cycle can be measured by the clustering coefficient, the proportion of a node's direct neighbors that are also direct neighbors of each other. The overall clustering coefficient of a complex network should be between 0.1 and 0.25, meaning that on average about 10-25 per cent of 3-node collections should be 3-cycles. The distribution of clustering coefficients among all nodes should be skewed, creating the condition that not all nodes in a cluster of mutually supporting nodes interact directly with nodes outside the cluster. In other words, many nodes have a high clustering coefficient, a moderate number of nodes have a moderate clustering coefficient, and a low number have a low coefficient. A skew distribution of clustering coefficients therefore defines the structure of adaptive hierarchy in a complex network.

Betweenness. Betweenness is a measure of a node's importance to dynamic behaviors in a complex network. Betweenness measures the proportion of shortest paths that pass through a node, but a node need not be the most well connected node (the largest hub) in order to have the highest betweenness. Betweenness 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. Complex networks should have a skew distribution of betweenness.

Path horizon. Path horizon is a measure of how many nodes, on average, a node must interact with for self-synchronization to occur. Only in very simple environments can each node successfully interact with all other nodes and clearly interacting with no other nodes prevents 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.

Neutrality Rating. Neutrality is additional structure in a complex network above the minimum for required for connectivity. Subtracting the number of links in a network of size N, N-1, from the number of links, *l*, in a given network of size N, and then normalizing to network size produces the Neutrality Rating, $(l - N + 1)/N$, which is a good measure of adaptavity Complex networks should have a neutrality rating of between 0.8 and 1.2.

Coefficient of networked effects (CNE). The coefficient of networked effects measures the amount of cyclic behavior per node and compares the potential for networked effects in networks of different sizes. CNE is the PFE from Section 4 normalized for network size, PFE/*N*. Complex networks should have a CNE between .1 and .25.

Property	**Range**	**Effect**
Number of Nodes, *n*	$n > \sim 100$	Networked effects unlikely to occur with $n < 50$
Number of links, *l*	$l < \sim 2n$	$l << 2n$, too brittle $l >> 2n$, too much overhead
Degree Distribution	Skewed	Adaptivity, Modularity
Largest Hub	< 100 links	Hub appears, recedes by reconnection 5% of links
Characteristic Path Length	log(*n*)	Short distances even for large networks (e.g., 10^4 nodes → Average Path Length = ~4)
Clustering	Overall: 0.1 – 0.25 Distribution: Skewed	Hierarchy, Organization
Betweenness	Distribution: Skewed	Highest: Most important nodes, bottlenecks Cascade Control
Path Horizon	log(*n*)	Self-Synchronization
Coefficient of Networked Effects (CNE)	0.1 – 0.25	Networked effects per node
Neutrality Rating	0.8 – 1.2	Increased adaptation; decreased susceptibility
Susceptibility	Low (random removal) High (focused removal)	Hubs should be kept obscure until needed, damage abatement/repair schemes

Table 1 - Thumb Rules for Analysis and Experimentation

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 by degradation of the previously listed properties. For example, the curve in Figure 15 works both ways: most of a network's connectivity can be lost with the removal of only 5-10 per cent of the network's most well connected nodes.

Table 1 summarizes these thumb rules for analysis and experimentation. Note that these are first approximations inferred from the study of adaptive networks in other domains. One topic for immediate study should be the validity of these thumb rules for military networks.

6 IMPLICATIONS

This paper has assessed the state of the art of military modeling, defined the elementary structure of a model of networked combat, identified mechanisms of networked effects in the model and described the model's long term evolutionary behavior. This research represents a significant new direction in combat modeling and has important implications for military modeling and simulation. The following sections present and discuss these implications.

6.1 Implications of Networked Structure

The Information Age Combat Model constitutes a dramatic change in military modeling because it mandates a substantial change in the structures we use to represent combat. If the structure presented in Section 3 is adopted, then two propositions logically follow.

IT is subsumed by process. The routers, computers, transmitters and other connected elements of hardware and software that make up military IT systems networks are only one of the dimensions in which a force can be networked. Metaphors and standards from the IT industry are appropriate for representing IT, but not necessarily useful for representing the totality of networked combat. Moreover, any model that does not employ graph theory (arcs and nodes) to represent networked combat cannot sufficiently represent the important processes and networked effects that make Information Age Warfare different from Industrial Age Warfare.

Networked warfare is ultra-dimensional. Section 3 discussed how even the most simple, complete model of networked combat must be represented in a high number of dimensions. If the trend toward greater numbers of robotic platforms and remote sensors continues, most real world, networked operations will also be conducted in many dimensions. Centralized coordination of a high-dimensional system is extremely difficult, yet much of the network-centric literature dictates centralized control. The defense community will need new concepts for decentralized control to operate their new, high-dimensional network-centric systems.

6.2 Implications of Networked Dynamics

The Information Age Combat Model describes the source of networked effects in networked warfare, as well as a method for measuring their presence or magnitude. If networks like those in Section 4 can be created, then the following implications must be addressed.

Networked warfare does not always require attrition. It is clear from Section 4 that a substantial amount of the total effort expended by a distributed, networked force is not expended on attrition. Networked warfare values the arrangement of assets over the number of assets. Superior competitive arrangements can be achieved by leveraging control cycles, catalytic control cycles and catalytic competitive cycles without necessarily resorting to combat cycles. Researchers should investigate the use of non-combat cycles as important sources of advantage in Information Age combat.

The dynamics of real-world distributed, networked forces are not well-known. Engineers and operators can infer from the Information Age Combat Model that network-centric programs that cannot formally or quantitatively express the source of their value must be suspect. This type of Information Age "Hippocratic Oath" prevents harm, but it does not inform the engineer about how to build a distributed, networked system or the operator about how to apply networked effects. For example, important questions about the relationship between the Coefficient of Networked Effects and performance in a combat network go unanswered. Future research should focus on answering these and other such performance-related questions.

We can know what networked warfare is not. Merely adding IT to an Industrial Age process does not necessarily create networked effects (and sometimes might even guarantee decreasing returns for IT investments). Preliminary analysis using the concepts from this paper shows that many existing military processes do not have the potential for networked effects. Using IT to increase the efficiency of supply chains, the Air Tasking Order (ATO) process or intelligence production are examples of existing Industrial Age structures masquerading as networked processes merely because IT is employed. Researchers should use the Information Age Combat Model to re-assess the potential for networked effects in these processes.

We know very little about how networks compete. Many of the figures in the paper represent two-sided competition between networks. One might expect that some in the scientific community have a sense for how networks actually compete. In fact, an Internet search on the topic produces almost no relevant literature.[45] Future research should place a high priority on exploring this important subject.

6.3 Implications of Network Evolution

Section 5 described the long-term evolution of networked warfare, provided a set of metrics to quantify this evolution and proposed the values to which these metrics should converge. If this evolutionary behavior is sufficiently accurate, then the following implications must be addressed.

Punctuated growth is a unifying theme. The research in Section 5 shows how small clusters of networked elements can be quickly combined into a composite force, a fundamentally different behavior than in traditional, Industrial Age force build-up. Not only could punctuated growth constitute a new concept for force deployment and employment, but it can also be a unifying theme for engineering and acquisition. The US Navy's FORCEnet Engagement Packages (FEPs, subsets of networked capabilities) and Fleet Readiness Program (FRP, an asynchronous deployment concept) are the types of programs and concepts to which the Information Age Combat Model can add analytical rigor.

Development of Information Age Operational Art. Existing Operational Art relies heavily on machine metaphors and Industrial Age concepts like applying *mass* and *force* to *centers of gravity*. Service colleges and the military concept development community should develop a new Operational Art that invokes networked behaviors and characteristics such as clustering, core shifts, punctuated growth and tipping points. The Information Age Combat Model can imbue the concepts and terminology of a new Operational Art with an intellectual pedigree.

Thumb Rule Validation. The Thumb Rules were derived from the characteristics of adaptive networks in non-military domains. Although early research shows that some of the Thumb Rules appear valid, a much larger set of data must be examined before the rules can be confidently adopted, modified or refuted. Until such time, the Thumb Rules represent a starting point for the engineering of distributed, networked systems and analysis of operational experiments with distributed, networked forces.

7 CONCLUSION

The model introduced in this paper shows why a closed form set of equations – the traditional format for a combat model – is inappropriate and insufficient to describe Information Age Combat. A formal notation is provided to help understand the character, behavior and dynamics in distributed, networked warfare. The model provides a point of departure for other types of representations, including simulation. A reader familiar with graph theory or real-world networks will note one important weakness in the Information Age Combat Model: real links have many other values other than the simple on/off representations provided here. The Information Age Combat Model is merely a rudimentary model of the topology of networked combat. Although the model might usefully describe the long-term statistical topology of complex military networks, it cannot fully evaluate military networks. A more mature model would include values other than "0" and "1" in its adjacency matrix and may have different values than the Thumb Rules presented in Table 1.

A better tool for further study of these networks is an *agent-based model*, which can translate a graph theory model into a dynamic, evolving simulation to achieve and explore more robust interactions. In an agent-based model, small pieces of software act interdependently in exactly the way the simple two-dimensional diagrams in this paper suggest, but they can do so in far many more dimensions and with a greater variety of parameters than the current state of Information Age Combat Model development allows.

It is a fundamental conclusion of this paper, then, that further mathematical development of this model is not as useful as instantiating the Information Age Combat Model in an agent-based model. It is with this first step that subsequent research into networked competition, networked effects and validation of Thumb Rule values can be achieved.

8 APPENDIX: COMPLEX NETWORKS

The research supporting this paper included an extensive examination of network flows and graphs, including very recent research into complex networks, much of which is still developing. This section is a primer that presents the findings of this research most relevant to understanding distributed, networked military forces.

8.1 Network Theory

What is commonly called a *network* is more technically described as a *graph*. A graph is a simple collection of *links* and *nodes*. When values are assigned to the links and nodes, a system with its own logic is created. This system is more properly called a *network*. Networks are typically used to mathematically model flows, analyze network circulation or evaluate costs in a dynamic, distributed system. For the purposes of this primer the values can be removed, greatly simplifying the discussion without loss of validity. Properties that characterize the performance of networks include:

- Link/node Ratio: Compares the link densities of different size networks.

- 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 through a network without passing through a high number of nodes.[46]

- Diffusion Rate: Describes the rate at which commodities proliferate throughout a network.

- Clustering: A measure of local cohesion in a network. The clustering coefficient, γ, is the ratio of the number of actual links between neighbors to the number of possible links between neighbors. In a social context, this would be a measure of how many of one's friends are also friends of each other. Highly clustered networks tend to have pockets of connectivity, which can increase the connectivity and redundancy of the whole network.[47]

- Scale: A measure of the distribution of links 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*. A scale free network has links 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*.[48]

The following examples show how the characteristics describe distinctly different behaviors in different networks.

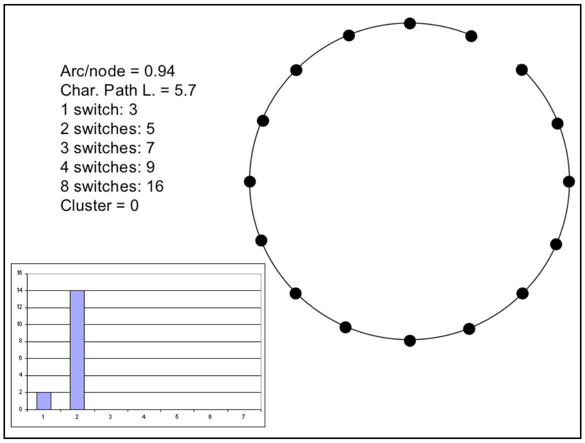


Figure 20 – Minimally Connected Network

Minimally Connected Network. A connected network is one in which every node, *n*, is attached to the network by at least one link. A minimally connected network, also known as a chain, is one in which the nodes are all connected with the minimum number of links possible, i.e., $n - 1$ links. Figure 20 shows a minimally connected network with 16 nodes and 15 links. In general, a minimally connected network contains:

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

different sub-networks, that is, each new node adds n - 1 sub-networks to the cumulative total of sub-networks (a third node adds two sub-networks to an existing two-node sub-network raising the new cumulative total to three sub-networks; the fourth node brings the cumulative total to six, the fifth brings the cumulative total to ten, etc.). The number of subnets in Figure 20 is 120. Minimally connected networks have fewer links 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 represented by the entries in Figure 20 listing the average number of nodes reachable from each node in *n* "switches" (which also represents the diffusion rate). 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 links attached to a node (the *degree* of the node, horizontal axis) and the number of nodes in each category (vertical axis). This graph defines the *scale*, or *degree distribution* of the network, which in this case is very close to two, because the majority of nodes are connected with only two links. Note also that the clustering coefficient is zero, which indicates that there is very little local network structure in this type of network.

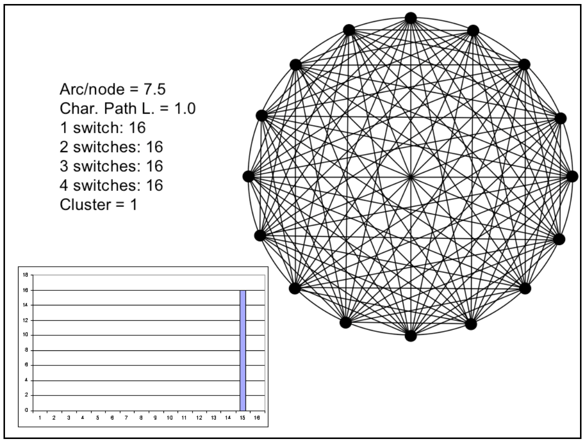


Figure 21 – Maximally Connected Network

Maximally Connected Network. A maximally connected network is one in which every node is directly connected to every other node by one link, i.e.,

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

links, that is, each new node adds n - 1 links to the cumulative total of links (the third node adds two links to the previous cumulative total of one link raising the new cumulative total to three links; the fourth node brings the cumulative total of links to six, the fifth brings the cumulative total to ten, etc.). Figure 21 shows a maximally connected network with 16 nodes and 120 links. A maximally connected network contains n! different sub-networks.[49] The number of subnets in Figure 21 is over 20 trillion. Maximally connected networks have more links and more subnets than any other type of connected network and are therefore the most expensive and complicated 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 21 requires over 20 trillion calculations). The scale is fixed at n – 1 = 15, and the network is maximally clustered.

Random Network. Minimally and maximally connected networks represent the extremes of network connectivity. For most warfare network applications, neither of these two extremes are useful. For comparison, Figure 22 shows a randomly connected network.[50] The ratio of links to nodes in this network is 2 (that is, there are 32 links, about twice as many as the minimally connected network in Figure 20 yet only about a quarter of the links in the maximally connected network in Figure 21). 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 links and subnets is dramatically lower than the maximally connected network. Two drawbacks arise from the random connection of links and nodes. The first is that the network is *irregular* in the sense that CPL 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 clustering coefficient. Irregular path lengths and clustering 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 property of random networks: the links are distributed with a Normal distribution with the network scale defined by the peak of the resulting bell curve.[51]

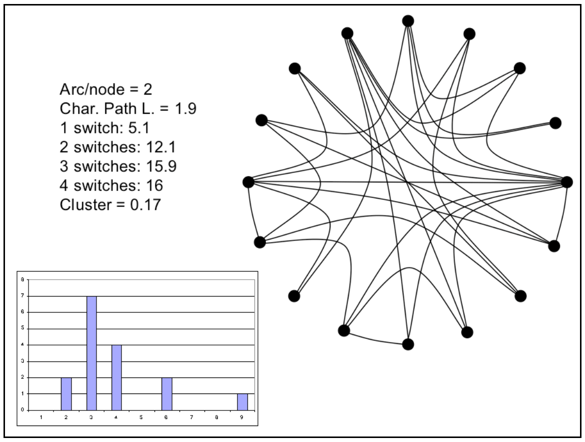


Figure 22 – Random Network

Regular Network. Figure 23 shows a regular network (otherwise known as a "lattice") that has the same ratio of links to nodes as the irregular random network. Although the clustering of this network is uniform, and therefore more regular than the random network, the characteristic path length increases significantly (although it also becomes more regular). The scale of this network is set at 4.0. Note that the minimally and maximally connected networks are special cases of a regular, lattice networks. Note also the dramatic difference in link distribution between the regular and random networks, although the number of links and nodes is identical.

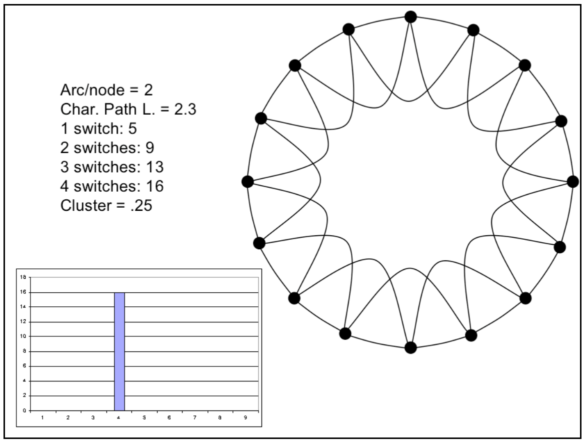


Figure 23 – Regular Network (Lattice)

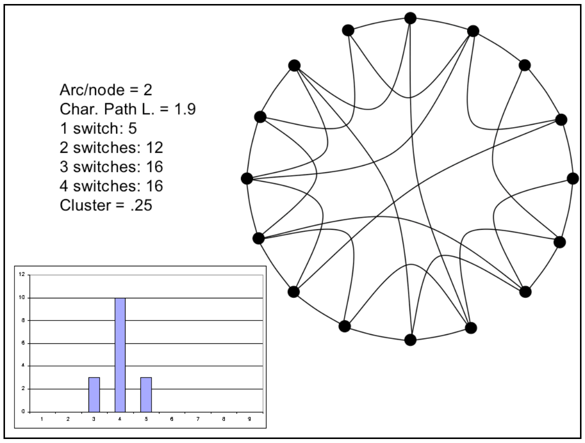


Figure 24 – Small World Network

Small World Network. A minor "re-wiring" of the regular network can create a "Small World" network that is very regular and has good clustering and short 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 24 shows how the regular network in Figure 23 can be re-wired to create a Small World network.

Random Network with Growth. For many decades, graph theory research depended on two assumptions that ultimately became 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 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 25 shows what happens when network structure 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 old nodes have more opportunities for connection.[52] In other words, the very first node in the network has *n* - 1 opportunities to connect by the time the *nth* node is added. This dynamic, known to economists as a type of *network externality*, has been used to explain "first mover advantage" in the Information Age marketplace. Note that the network is about as clustered as the random network, yet the scale has started to become less defined (this network, in fact, has two distinct scales: degree 1 and degree 2). Also note that although this network has 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 per cent.

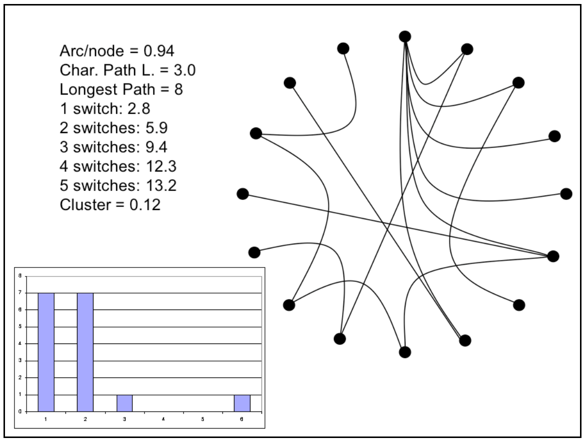


Figure 25 – Random Network with Growth

Scale Free Network with Preferential Attachment. If one removes the constraints of both assumptions so that the connection of nodes is biased and the network is grown, then a class of networks is created that represents many real world networked structures. The network in Figure 26 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 another type of Information Age process that constitutes a network externality. It is also the type of attachment mechanism that mimics the distribution of routers connections on the internet, the distribution of links to web pages on the world wide web, and a host of other adaptive, dynamic network topologies.[53] The statistics of this network are quite different than the previous examples (the network is not be as well clustered as the others and the CPL is almost as long as the lattice) but it has one beneficial property that marks it as a very adaptive network – it is a *scale free* network. The degree distribution is represented by a skewed curve like the one approximated above the histogram in Figure 26. One generic form of the equation defined by these curves is the "Power Law," but other skewed distributions can represent connections in a scale free network.[54] A scale free distribution of links defined by a skewed distribution has very many nodes with a very small degree, a moderate number with a moderate degree and a very few with a very high degree.

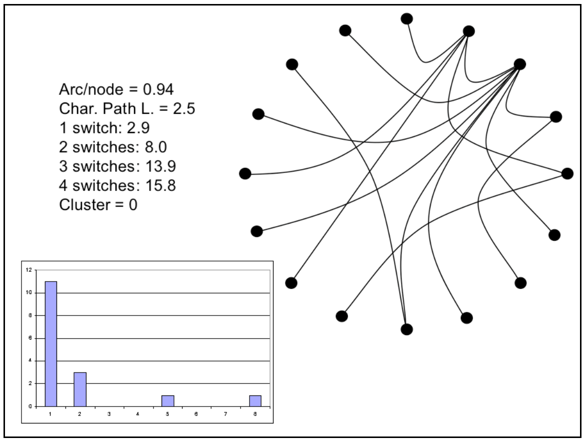


Figure 26 – Growth and Preferential Attachment

Network	# of Links	# of Nodes	Links / Node	CPL	1 Link (Nodes)	2 Links (Nodes)	3 Links (Nodes)	4 Links (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 2 – Network Comparison

8.2 Network Comparison

Table 2 is a summary of the statistics from the networks described in Section 8.1. These statistics are the number of links, the number of nodes, the ratio of links to nodes, the CPL, the average number of nodes reached by traversing some number of links (or the number of "switches", listed for 1 to 4 links) and the clustering coefficient, γ.

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

Random connection of links and nodes with a link-node ratio of 2 can connect all nodes in only about 3 switches, CPL is low (1.9) and clustering is also better. Although the random network provides better 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. The standard deviation of γ listed in Table 2 for the random network means that some nodes may have values of γ similar to the minimally connected network.

Arranging the same number of links and nodes in a more regular network, however, reduces the irregularity γ but the CPL gets more irregular. The regular network also has a longer CPL (that is, commodities proliferate much more slowly in the network in Figure 20).

The Small World network uses the same ratio of links to nodes as the random and lattice networks, but retains regularity and clustering 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 in CPL and local cohesion.

The preceding analysis demonstrates that the arrangement of links 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 8.1 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 2 suggests that Small World and Preferential Attachment networks, both in a class called complex networks, are simpler, perform better and require lower overhead than other networks.

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 rationale behind the design is derived from organizational principles and organization theory. The best configuration for a network should therefore 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 allowable connections. Based on the statistics presented in Table 2, the following comparisons can be made between the networks in Section 8.1:

- Minimally Connected Networks are brittle, but have long CPLs, poor clustering and definite scale

- Maximally Connected Networks are robust and have the shortest CPLs possible, but they are too clustered (each node is a neighbor of every other node) and have too many links per node. They have definite scale

- Regular Networks are robust but have long CPLs. They are highly clustered and have definite scale

- Random Networks are brittle but have short CPLs. They have low clustering and have definite scale

- Small World Networks are robust, have short CPLs and high clustering and are less scaled

- Random Networks with Growth are less brittle and have short CPLs. They have low clustering and are less scaled

- Networks with Preferential Attachment are robust, with short CPLs and low clustering. They are scale free

8.3 Desirable Network Properties

Most current research on complex networks focuses on discovering the statistical properties of existing complex networks such as the World Wide Web or a sociological data set. 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? The following section defines some of the more useful network properties and prescribes their values for combat networks.

Node and Link Types. A combat network will have many different types of nodes and links.

Flow. Combat networks should capitalize on the existence of cycles and the properties of autocatalysis and neutrality. Such networks will be directed, where the links may be outgoing, incoming, or both.

Number of Nodes. Many of the more important and exploitable networked effects are difficult to achieve unless a network contains at least about 100 nodes. Networked effects become increasingly difficult to achieve as combat networks get smaller.

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 - 1 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 coordination overhead (as well as the overhead required for protection of links) without adversely affecting performance. Combat networks should therefore have about two links for every node.

Degree Distribution. One way to represent the connection pattern of a network is by the degree distribution, which shows the number of nodes with specific degree. Most adaptive, re-configurable and resilient networks have a skew degree distribution (such as is found in a scale free network). These networks have very many nodes with very few links, a moderate number of nodes with a moderate number of links, and very few nodes with very many links. Skew-degree networks contain powerful hubs that can be adaptively reconfigured. Combat networks should have skew degree distributions.

Maximum Degree. In skew-degree networks, the maximum degree is roughly proportional to square root of the number of nodes. The Figure 27 plots maximum degree against number of nodes for a combat network with a skew degree distribution.

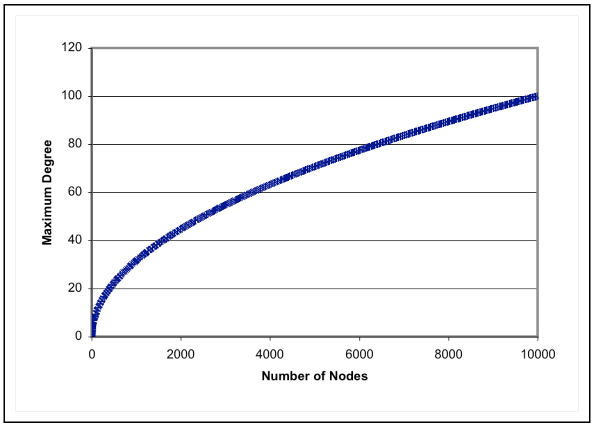


Figure 27 – Maximum Degree in Scale Free Networks

Betweenness Centrality. Betweenness centrality is a measure of the number of shortest paths that travel through a node, as well as its importance to dynamic behaviors in a complex network. Betweenness centrality can identify the most popular nodes and locate bottlenecks in a network. Research shows that betweenness should have a skewed distribution so that there are not a large number of well-traveled nodes. Also, the nodes of highest betweenness should not be directly connected to each other. This slows the proliferation of pathogens, viruses or cascading damage.[55]

Path Horizon. Path horizon measures the number of nodes on average that a node must interact with for constructive self-synchronization to occur. A path horizon of 1 means that a node must coordinate with all its nearest neighbors for self-synchronization to occur. A path horizon of 2 means that coordination should extend to all the nearest neighbors of a node's nearest neighbors, etc. Research shows that self-synchronization occurs when the path horizon is the logarithm of the number of nodes.[56]

Characteristics Path Length. Figure 28 lists the CPL of different networks. The legend in the figure refers to lattices of degree 1-5 (e.g., Lat1), random networks of degree 2-5 (e.g., Rnd3), and Small World and Scale Free Networks (SmlWrldSclFree). The CPL of lattices grows on the order of n/4*k*, where n is the number of nodes and *k* is the mean degree. The CPL in random graphs grows proportional to log n/log *k* and in Small World and Scale Free networks the CPL is proportional to log *k* or slower. Combat networks should therefore have characteristic path lengths 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.[57]

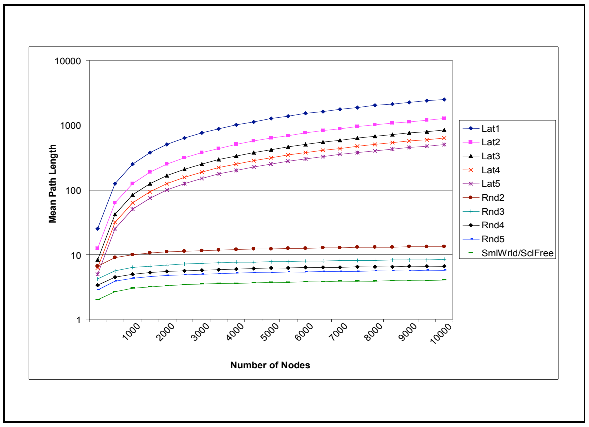


Figure 28 – CPL for Selected Networks

Component Sizes. Since no node should be isolated during military operations, the size of the smallest clusters in a network should be greater than one. Service specific operations in a joint environment or independent special operations would comprise larger sub-components, but to keep the ultimate network configuration obscure to an adversary, the giant component in combat networks should not be fully constituted until a large-scale operational is ready to be executed.

Neutrality. Complex networks require latent, *neutral* structure for adaptation. This allows for the creation, removal and re-emergence of hubs by rearranging only about 5-10 per cent of the total number of links in a network. One can always turn a complex network into an optimal (non-adaptive) chain by choosing a particular minimally connected path through the network, but a chain cannot be turned into a complex network without the addition of the adaptive (sub-optimal) neutral structure. The Neutrality Rating is obtained by removing from a complex network the number of links in a minimally connected network and then calculating the link to node ratio. Combat networks should have a neutrality rating of between 0.8 and 1.2.

Clustering Coefficient. Clustering is one way to measure cohesion in a network. The clustering coefficient is the fraction of node triples in a network that have their third edge filled to complete a triangle. If a network has a high clustering coefficient then there is tight cohesion in the network (many triangles). The overall clustering coefficient is calculated globally over an entire network but individual nodes can have a clustering measurement as well. Skew-degree distribution networks have good clustering properties in the localities of the largest hubs but low clustering away from hubs of high activity. This local clustering provides the type of cohesion and mutual support that military operations require. Collections of nodes with low activity, however, are not needlessly expending collaboration effort. For this reason, combat networks, like other adaptive networks, should have a skew distribution of clustering coefficients as well.[58]

Robustness. Robustness measures the extent to which a network can avoid catastrophic failure as links or nodes are removed. Robustness is usually determined by analyzing how network properties such as the size of the giant component, characteristic path lengths or betweenness, change with removal of nodes or links. The opposite of a "robust network" is a "brittle network."[59] For example, Figure 29 shows the size of the giant component in a military e-mail network with skew degree distribution plotted against the number of nodes removed from the network. Random removal results in an almost horizontal line (meaning the giant component stays connected), whereas removal by degree rank (highest first) shows a rapid disconnection. This is intuitive because there are many more low-degree nodes in a complex network than high-degree nodes, so a random selection of nodes should favor low-degree nodes over those with high degree. Combat networks should therefore be extremely resilient to random attack but can be very susceptible to focused attack. This will be true as long as adversaries are allowed to know the detailed structure of a network. Since skew distribution networks have a great deal of neutrality, it is a fundamental operational consideration of such networks that their detailed structure should remain obscure until it is configured for use.

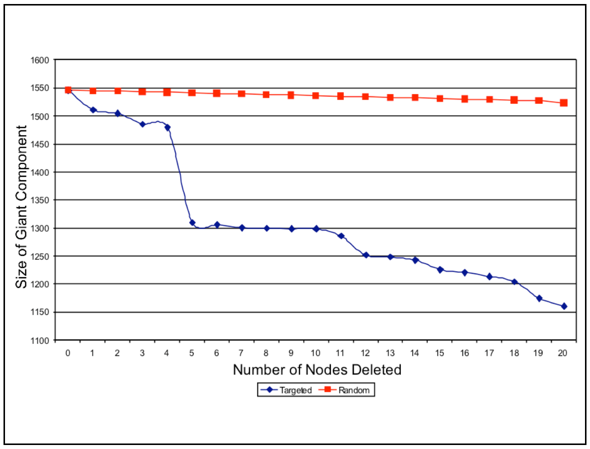


Figure 29 – Robustness in a Complex Network

Diffusion Rates. A network's diffusion rate is average number of nodes reachable by traversing exactly *l* links. Figure 30 compares the diffusion rates of all the networks listed in Table 2. The fastest rate, of course, is found in the maximally connected network because each node is directly connected to every other node. The slowest rate occurs in the minimally connected network, since this network contains no short-cuts. Between these upper and lower bounds is the rudimentary shape of diffusion patterns typical of complex networks (the curves in Figure 30 would be more pronounced if the networks had more links and nodes). Autocatalysis and neutrality contribute to the "S" shape of these diffusion curves. Figure 31 shows how the 400-node network from Figure 15 would have different diffusion curves for different connection probabilities (that is, larger numbers of strings attached at each turn). The curves get steeper as connection probabilities increase. Figure 32 shows that reducing the number of nodes by an order of magnitude requires an increase in the connection probability by an order of magnitude to achieve the same diffusion rates. Figure 33 shows how more nodes increase the diffusion rate for the same connection probability. All of these diffusion curves show how numbers have a non-linear effect on network diffusion rates.

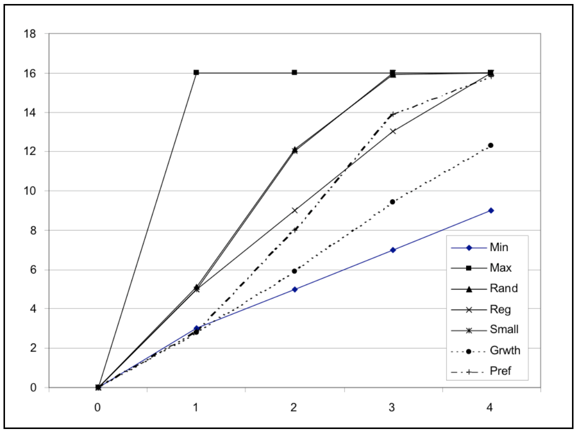


Figure 30 - Generic Diffusion Profiles: Complex Networks

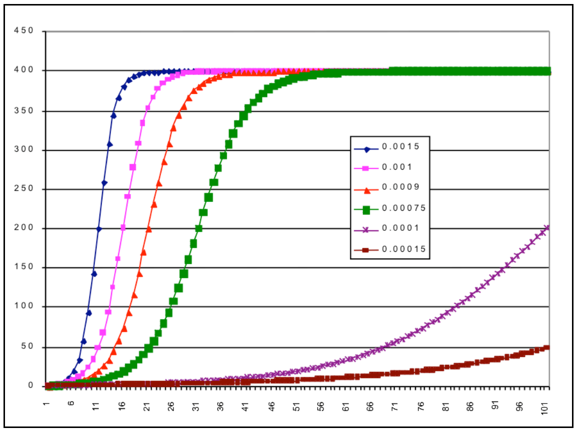


Figure 31 - Diffusion Rates, 400 Node Network

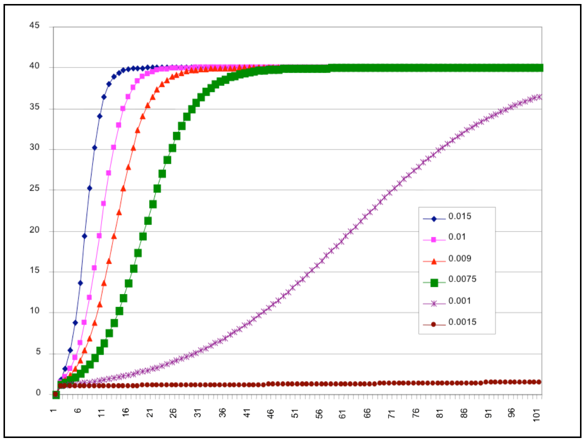


Figure 32 - Diffusion Rates, 40 Node Network

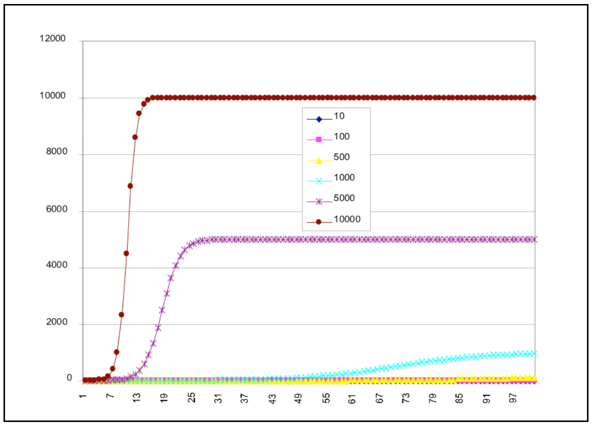


Figure 33 - Diffusion Rates, P(Connection) = 0.001

[1] Cares, Jeffrey R. and Gregory E. Glaros, *Wolf PAC – Real Options for Defense: Architectural Choices for Distributed Operations*, 1-2, draft manuscript, 2004.

[2] Cares, Jeffrey R., Raymond Christian and Robert Manke, "Fundamentals of Distributed, Networked Forces and the Engineering of Distributed Systems," NUWC-NPT Technical Report 11,366, 9 May 2002.

[3] Ito, T., Chiba, T., Ozawa, R., Yoshida M., Hattori M., and Sakaki, Y., "A Comprehensive Two-hybrid Analysis to Explore the Yeast Protein Interactions," *Proc. Natl. Acad. Sci. USA,* 98, 4569-4574 (2001); H. Jeong, Mason, S., Barabasi A.-L. and Oltvai, Z. N., "Lethality and Centrality in Protein Networks," *Nature,* 407, 41-42 ((2001); Maslov, S. and Sneppen, K., "Specificity and Stability in Topology of Protein Networks, *Science,* 296, 910-913 (2002); Sole, R. V., and Pastor-Satorras, R., complex Networks in Genomics and Proteomics," in S. Bornholdt and H. G. Shuster (eds.), *Handbook of Graphs and Networks,* 145-146, Wiley-VCH, Berlin (2003); and Uetz, et. al., "A Comprehensive Analysis of Protein-Protein Interactions in *Saccaromyces Cerevisiae*," *Nature,* 403, 623-627 (2000).

[4] Broida, A., and Claffy, K. C., "Internet Topology: Connectivity of IP Graphs," in S. Fahmy and K. Park (eds.) *Scalability and Traffic Control in IP Networks,* No. 4526 in Proc. SPIE, 172-187, ISOE, Bellingham, WA (2001); Chen, Q., et. al., "The Origins of Power Laws in Internet Topologies Revisited," in *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies,* IEEE Computer Society (2002); and Faloutsos, M., Faloutsos, P., and Faloutsos, C., "On Power Law Relationships of the Internet Topology," *Computer Communications Review,* 29, 251-262 (1999).

[5] Adamic, L. A., "The Small World Web," in *Lecture Notes in Computer Science,* Vol. 1696, 443-454, Springer, New York (1999); Albert, R., Jeong, H., and Barabas, A.-L., "Diameter of the World Wide Web," *Nature*, 401, 130-131 (1999); Broder, A., et. al., "Graph Structure in the Web," *Computer Networks,* 33, 309-320 (2000); Flake, G. W., Lawrence, S. R., Giles, C. L., and Coetzee, F. M., "Self-Organization and Identification of Web Communities," *IEEE Computer*, 35, 66-71 (2002); Kleinburg, et. al., "The Web as a Graph: Measurements, Models and Methods," in *Proceedings of the International Conference on Combinatorics and Computing,* No. 1627 in Lecture Notes in Computer Science, 1-18, Springer, Berlin (1999); and Kumar, et. al., "Stochastic Models for the Web Graph," in *Proceedings of the 42nd Annual IEEE Symposium on the Foundations of Computer Science,* 57-65, IEEE, New York (2000).

[6] Price, D. J. de S., "Networks of Scientific Papers," *Science,* 149, 510-515 (1965); Redner, S., "How Popular is Your Paper? An Empirical Study of the Citation Distribution," *Eur. Phys. J. B,* 4, 131-134 (1998); and Selgen, P. O., "The Skewness of Science," *J. Amer. Soc. Inform. Sci.,* 43, 628-638 (1992).

[7] Dunne, J. A., Williams, R. J., and Martinez, N. D., "Network Topology and Species Loss in Food Webs: Robustness Increases with Connectance," Santa Fe Institute Working Paper 02-03-013 (2002) and Martinez, N.D., "Artifacts or Attributes? Effects of Resolution on the Little Rock Lake Food Web", *Ecological Monographs,* 61, 367-392 (1991).

[8] Solé, R. V. and Valverde, S., "Hierarchical Small Worlds in Software Architecture," Santa Fe Institute Working Paper 03-07-044 (2003).

[9] Adamic, L. A. and Huberman, B. A., "Power Law Distribution of the World Wide Web," *Science,* 287, 2115 (2000); Amaral, L. A. N., Scala, A., Barthemely, M., and Stanley, H. E., "Classes of Small World Networks," *Proc. Natl. Acad. Sci. USA,* 97, 11149-11152 (2000); Newman, M. E. J., Strogatz, S. H., and Watts, D. J., "Random Graphs with Arbitrary Degree Distributions and their Applications," *Phys. Rev. E,* 64, 026118 (2001) and Watts, D. J., and Strogatz, S. H., "Collective Dynamics of 'Small World' Networks," *Nature,* 393, 440-442 (1998).

[10] Newman, M. E. J., "The Structure and Function of Complex Networks," SIAM Review 45, 167-256 (2003).

[11] See https://www.dmso.mil/public/transition/vva/ (accessed 01 Oct 2004) for a review of the US DoD VV&A program. In practice, funding for VV&A is almost never included in defense analysis contracts.

[12] Attributed to the statistician George E.P. Box. See http://en.wikiquote.org/wiki/George_E._P._Box, accessed 01 Oct 2004. Thanks to Major Alistair Dickie, Royal Australian Army, for chasing down the source of this Operations Research "street wisdom."

[13] Some models attempt to represent as much detail as computationally possible. These "virtual models" are more useful as simulators than simulations, that is, they are more useful for generating simulated experience (such as for pilot training) than for analysis.

[14] Shpak, M., Stadler, P. F., Gunter, P. W., and Hermisson, J, "Aggregation of Variables and System Decomposition," Santa Fe Institute Working Paper 2003-04-25, April 2003, http://www.santafe.edu/research/publications/wplist/2003, accessed 30 Sep 2004.

[15] See, for example, James J. Schneider, "The Exponential Decay of Armies in Battle," Theoretical Paper No. 1, U.S. Army School of Advanced Military Studies, 1985.

[16] Liebholz, S. W., "Twenty Questions," in Wayne P. Hughes, Jr., (ed.), *Military Modeling,* Arlington, VA, Military Operations Research Society, 1984, 344-345.

[17] In other words, the Central Limit Theorem applies. See http://mathworld.wolfram.com/CentralLimitTheorem.html, accessed 30 Sep 2004.

[18] These equations were first derived by a US Navy Lieutenant, J.V. Chase, in 1902. They remain attributed to Lanchester because Chase's work was classified until 1972. See Bradley A. Fiske, *The Navy as a Fighting Machine* (rev. ed.), (Annapolis: United States Naval Institute, 1988), 375-376. They were also derived independently by the Russian mathematician Osipov in 1913.

[19] See Bracken, J., Kress, M, and Rosenthal, R. E. (eds.), *Warfare Modeling*, (Danvers, MA, Wiley and Sons, 1995) for a listing and discussion of Lanchester variants.

[20] See https://www.jointmodels.mil/index.cfm?id=TACWAR/index.cfm for a description of TACWAR, accessed 01 Oct 2004.

[21] See http://www.metsci.com for a description of NSS, accessed 01 Oct 2004.

[22] See http://www.eadsim.com/EADSIMBrochure.html for a description of EADSIM, accessed 01 Oct 2004.

[23] See http://www.msiac.dmso.mil/spug_documents/JWARS_Overview_Brief.ppt for an overview of JWARS, accessed 01 Oct 2004.

[24] 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), 121-143.

[25] Michael Johns, "Heterogenous Salvo Model for the Navy After Next, Master's Thesis," Operations Research Department, Naval Postgraduate School, 2000.

[26] Kieth J. Ho, Captain, Singapore Army, "An Analysis of Distributed Combat Systems," Master's Thesis in Systems Integration, 2001.

[27] See http://www.airpower.maxwell.af.mil/airchronicles/aureview/1977/mar-apr/porter.html (accessed 01 Oct 2004) for a discussion of the dogmatic use of Correlation of Forces by the Soviets.

[28] Arthur K. Cebrowski, and John J. Garstka, "Network-Centric Warfare: It's Origin and Future," *US Naval Institute Proceedings,* January 1998.

[29] 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). Available online at http://www.dodccrp.org/NCW/NCW_report/start.htm. All sites accessed 01 Oct 04.

[30] J. V. Chase, a Lieutenant at the Naval War College, created "Lanchester's" Equations in 1902 out of frustration wrought by hand-waving and imprecise language that often accompanied discussions of the virtues of massed fires. The modern reader will note that Chase's disdain for "glittering generalities" would seem appropriate for NCW discussions today. See Bradley A. Fiske, *The Navy as a Fighting Machine* (rev. ed.), (Annapolis: United States Naval Institute, 1988), 375-376.

[31] Alberts, et al, 250-256.

[32] James Crutchfield and Yuzuru Sato, "Coupled Replicator Equations for the Dynamics of Learning in Multiagent Systems," SFI Working Paper 02-04-017, 2002 and Robert Axtell, "Non-Cooperative Dynamics of Multi-agent Teams," Brookings, 2002, are two counterexamples to NCW self-synchronization claims.

[33] See Jeffrey R. Cares, "The Fundamentals of Salvo Warfare," Operations Research Department, Naval Postgraduate School, 1990, for a treatment of combat entropy that depends on the arrangements of assets, not Information Age attrition.

[34] See www.dtic.mil/doctrine/jel/jfq_pubs/1620.pdf, accessed 30 Sep 2004.

[35] Richard Darilek, Walter Perry, Jerome Bracken, John Gordon, and Brian Nichiporouk, *Measures of Effectiveness for the Information-Age Army*, (Santa Monica, CA: RAND, 2001); 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).

[36] David Ronfeldt and John Arquilla (Ed's.), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, (Santa Monica, CA: RAND, 2001).

[37] Moffat, James, *Complexity Theory and Network Centric Warfare,* (DoD Command and Control Research Project, National Defense University, Washington, DC, 2003)

[38] Indeed, it has been long known that combat performance is better represented by skewed, rather than regular, distributions. See Joseph Bolmarchic, "Who Shoots How Many," Proceedings, MORIMOC II, Military Operations Research Society, 1988.

[39] In this paper, the word "network" refers to graph theoretic (links and nodes) representation of systems, not necessarily to information technology (IT) network structures.

[40] See http://mathworld.wolfram.com/Eigenvalue.html, accessed 30 Sep 2004.

[41] Jain, Sanjay and K. Sandeep, "Graph Theory and the Evolution of Autocatalytic Networks," http://arXiv.org/abs/nlin.AO/0210070, accessed 30 Sep 04. As with any multi-variant mathematical problem, there can be more than one eigenvalue that represents the value of a matrix.

[42] Kauffman, Stuart *At Home in the Universe,* (New York, Oxford University Press, 1995), 54-7.

[43] Jain and Sandeep, 19-22.

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

[45] The reader can check independently at www.google.com using "networked competition" or a similar word string.

[46] Watts, Duncan, *Small Worlds,* (Princeton University Press, New York, 1999).

[47] Watts, *Small Worlds*.

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

[49] $n! = n(n - 1)(n - 2)(n - 3) \dots (1)$. $n!$ (spoken, "n factorial") is one of the highest level of "computational complexity" in network mathematics.

[50] To be technically accurate, this network is actually pseudo-random, since it was created with a computer and true random sequences cannot be guaranteed by computer algorithm.

[51] Barabasi, Chapter 11.

[52] Barabasi, Chapter 6.

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

[54] 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.

[55] Stefan Wuchty and Peter F. Stadler, "Centers of Complex Networks," Santa Fe Institute Working Paper, 2002-09-052, September 2002.

[56] Sergi Valverde and Ricard V. Solé, "Internet's Critical Path Horizon," Santa Fe Institute Working Paper, 2004-06-010, June 2004.

[57] M. E. J. Newman, "The Structure and Function of Complex Networks," SIAM Review 45, 167-256 (2003).

[58] Newman, M. E. J., Strogatz, S. H., and Watts, D. J., "Random Graphs with Arbitrary Degree Distributions and their Applications," *Phys. Rev. E,* 64, 026118 (2001).

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