INFORMATION AGE WARFARE QUARTERLY

Winter 2005, Volume I, Number 1

Table of Contents

ISSN 1554-0561

The **I**nformation **A**ge **W**arfare **Q**uarterly (ISSN 1554-0561) contributes to the solution of real world Information Age defense problems. The journal provides intellectual bridges among technologists, analysts and operators with interdisciplinary essays and analytical articles on the application of complex systems research to:

Military operational challenges
Defense innovation
Investment in future defense systems, or defense-related hardware
Human capital development.

A secondary purpose of the journal is to provide a means for researchers to share technical insights about complex systems and Information Age innovation.

Submission Guidelines: Unsolicited manuscripts are welcome. Manuscripts should be submitted via email to the editor, Dr. James F. Miskel at the following address: editor-iawq@alidade.net. The IAWQ uses the Naval War College style manual which is available at:

http://www.nwc.navy.mil/Academics/guides/stylemanual.pdf.

FROM THE EDITOR'S DESK:

This is the introductory issue of the Information Age Warfare Quarterly (*IAWQ)*, a journal dedicated to exploring the impact of new models of analysis and ways of thinking about contemporary and future military operations. *IAWQ* operates from the assumption that the Information Age is different from the Industrial Age, but that the implications of the differences have not been assimilated by many organizations in government, the private sector and the most conservative organization of all, the military.

The differences between the Information and Industrial Ages have been variously described and new differences will inevitably become apparent as Information Age technologies accelerate their propagation through society worldwide and smaller-faster-smarter-cheaper technologies continue to leap off the scientists' bench into the defense and commercial marketplaces. *IAWQ* will be less interested in precisely defining the things that make the Information Age different than it will be in examining ways in which Information Age developments can be better leveraged to meet the challenges of the future and in defining the mechanisms of advantage in the Information Age.

A particular emphasis of *IAWQ* will be on complex systems research and on the application of this research to military operational challenges, defense innovation, investment in future defense systems and defense-related hardware, and human capital development. Indeed the principal audiences envisioned for the journal are military planners, operations researchers, academics with interest in defense and military issues, war game designers, analysts interested in the application of theory to practical problems, and students of management, leadership and innovation.

Since the first humans charged off to war with stones or spears in their hands, individuals and small groups have been able to take autonomous action and self-synchronize their day-to-day behavior at the local level. However, contemporary technologies enable large numbers of widely-dispersed units to do what pairs of early humans could do in combat—self-synchronize martial behavior to achieve greater results. If wisely utilized, modern technologies enable large networks of small groups and individuals to learn from each other and adapt their behavior in real time without having to wait for formal, time consuming after-action evaluations by a headquarters staff and the issuance of new operating instructions. There is still a place for after-action analyzes, of course, but there is much to gain in the battlefield innovation that network behavior enables.

Perhaps more importantly, large organizations, such as the armed forces, can re-configure themselves as networks and thereby increase efficiency and effectiveness, reduce platform costs, and minimize exposure to counter-attack or terrorist assault. Finally, technological advancement has led to the creation of the tools that analysts need to quantify network effects, simulate alternative plans, and design network structures.

The allure of technology and the apparent success in some corporate settings of "technology push" approaches to innovation and the understandable desire to start making progress on innovation should not obscure the important, fundamental role of rigorous analysis in charting the course to new concepts of military operation and organizational designs. We hope that readers of *IAWQ* will find in its pages analyses that will help them better understand the implications of operating in the Information Age.

DISTRIBUTED ADAPTIVE LOGISTICS:
Transforming Supply Chains into Demand Networks

Jeffrey R. Cares

Abstract*: Prevailing wisdom from the Industrial Age holds that the best way to provide logistics to a force is with a highly optimized supply chain. Emerging logistics concepts suggest that application of Information Technology (IT) might enable supply chains to reach unprecedented levels of optimality. At the same time, however, Information Age warfighting concepts suggest fluid, self-organizing military forces. This paper describes a logistics concept that relies on IT-enhanced adaptation and learning, rather than optimization, to transform supply chains into demand networks that more effectively support combat operations.*

Introduction

Throughout the last decade, long-range planners in the defense industry have proposed concepts for Information Age Warfare, under the rubric of Network Centric Warfare, that use information technology to solve long-standing military challenges and to effectively address new ones. These challenges include destruction of time-critical targets, theater-wide search and surveillance, long-range power projection and access to contested littoral areas.[1] Many of these concepts are expected to result in fielded forces that are distributed, networked, highly robust and dynamic. Long-standing practices in logistics and supply chain management, however, work best in environments where there are high levels of stability and predictability. They are not designed to cope with the quickly evolving and adaptively *ad hoc* behaviors envisioned for future military forces. Many logistics systems proposed for this future merely apply Information Technology (IT) to improve existing processes and do not address the need – particularly at the tactical level – for Information Age logistics processes that are as robust and dynamic as the forces they would serve. This article introduces the Distributed Adaptive Logistics concept, a system of logistics management that, for the purposes of supporting distributed, networked forces in the most challenging operational and tactical environments, values flexibility, adaptation and learning over predictability, precision and optimization.

Logistics, by definition, is the "process of planning and executing the projection, movement, sustainment, reconstitution and redeployment of operating forces in the execution of national security policy."[2] Even under the most benign conditions, logistics systems are susceptible to poor information or imprecise prediction about consumption rates, transport delays or interruptions, high transportation costs, inter-modal bottlenecks, high warehousing costs (including force protection). Logistics operations are also adversely impacted by operational plan changes, inadequate information about transfer rates and the arrival of commodities out of sequence (e.g., perishables being delivered without storage equipment). Some of the solutions proposed to address these problems include better information and prediction about consumption rates, faster or cheaper transport, more efficient inter-modal transfer, reduced stockpiling, quicker delivery or shuttle platforms, better information and prediction about transfer rates, better visibility into critical items and better understanding of item sequencing.

Some of these solutions require improvements to the physical characteristics of the supply chain elements, yet most would be the result of improvements in an ability to cope with the "information conditions" in a supply chain, that is, the degree of operational and environmental uncertainty encountered by the system.

Focused Logistics is not Adaptive

The Joint Staff has proposed the application of IT to improve the information conditions in future logistics systems. Joint and Service future logistics concepts are centered on the idea of "Focused Logistics," which has been defined as the "fusion of logistics information and transportation technologies for rapid crisis response, deployment and sustainment, the ability to trace and shift units, equipment and supplies even while en route, and delivery of tailored logistics packages and sustainment directly to the warfighter." Focused Logistics is concerned with Joint deployment and rapid distribution of logistics, with an increased emphasis on movement velocity, time-definite delivery, reduced footprint, streamlined processes and centrally managed and fused information. Focused logistics concepts expect that an agile infrastructure, reliable information and accelerated cycle times will create "Lean Logistics," "Precision Logistics," or systems that rely mainly on "Velocity Management." Such systems are normally scoped for the theater level of war and claim the ability to provide a CINC with the capacity to centrally synchronize, prioritize, integrate and coordinate all supply chain efforts in theater. These concepts clearly place a high premium on optimizing the supply chain and use IT to dramatically improve optimization.[3]

The extent to which a supply chain can be optimized, however, depends on the complexity and predictability of the operations serviced by the supply chain. Some operations might be quite simple. An example is force buildup operations in a protected rear area. For such an operation, a highly optimized supply chain (such as that envisioned by Focused Logistics) will perform best. As operations become more complex, however, so must the supply chain.

Prototypical Industrial Age Warfare is characterized by limited communications, massed forces, centralized command, control and decision making, and information that is difficult to obtain and hard to share. The introduction of IT into military force structures is serving to change some important facets of warfare, and the new prototype is characterized by physical dispersion, distributed information, and decentralized cognition. These characteristics will increase the complexity of military operations in three ways. First, units are not compelled to act in tight formations or groups. Second, IT applications and networking can create connections and associations between elements of a force that heretofore might never have interacted. Third, the dispersed elements of an organization can task-organize themselves to adjust to unfolding opportunity or unexpected risk.

Distributed Adaptive Logistics

The Distributed Adaptive Logistics concept would rely on adaptation, flexibility, agility and responsiveness, all within a "learning," networked context to cope with these complexities. Distributed Adaptive Logistics relies on clever commanders using and sharing local information to improve logistics support rather than centrally collecting information, controlling processes and dictating local decisions. Distributed Adaptive Logistics aims to cope with complexity by translating global governing principles into local rule sets, by placing local coordination of modular units at a premium, by clearly articulating roles and responsibilities rather than directing behavior and by providing a deeper understanding of battle force dynamics. Distributed Adaptive Logistics achieves these aims by enabling self-synchronization via local coordination through IT systems, encouraging interaction, connection and recombination at the lowest echelon possible so that innovative teams can emerge to meet local challenges, closing feedback loops so that all levels and perspectives in the force can learn from each other, and by vigorous education and training in the most complex and challenging extremes of the operational spectrum.[4]

Distributed Adaptive Logistics is not an Information Age concept just because Information Technology is used – it is an Information Age concept because it exploits advantage from Information Age models of decentralization, adaptation and self-synchronization. Distributed Adaptive Logistics transforms supply chains to dynamically adaptive demand networks that more closely conform to unfolding battlefield conditions while remaining intimately connected to commander's intent, thereby enabling more fluid operations and creating an ability to seize local opportunities as they develop.

Optimization, Control, Complexity and Scale

Whether or not a supply system can be optimized depends not only on the stability and predictability in system itself, but also on the stability and predictability of the environment and of the other systems with which it interacts. Paradoxically, as stability and predictability decrease, too much efficiency can actually impair the ability of a system to function effectively. To see how this might happen consider the idea of "make-span" in production line fabrication. A piece of metal that proceeds through a milling process consisting of several machining steps, is the object of a process that literally "spans the making" of the piece. If a certain amount of time is required on each machine, then the total milling time plus all the transfer and set up time equals the make-span. If there is sufficient transfer time, then the entire process can tolerate the failure of one step, and, for example, work-arounds can be employed.[5] As the transfer time is shortened in the name of efficiency, however, the probability of failure in the entire process can increase dramatically.

The parallel with supply chains is direct: *if too much slack is removed from a supply chain, the entire chain becomes much less tolerant of change.* Of course, supply chain operations are much more complex than the process of production line fabrication and they incur additional complexity because they are inextricably connected to combat operations. Moreover, recent experience in Afghanistan and Iraq suggests that fluid, self-organizing military forces will ~~be~~ become the norm, particularly at the tactical level. It has been proposed that the primary source of advantage in distributed, networked forces arises from networked effects that are distributed in many dimensions throughout a force and can be summoned for use in the manner of advantage chosen by commanders based on evolving conditions.[6] Highly-optimized supply systems cannot provide effective logistics for such dynamic operations.

The concepts of *complexity* and *scale* bring the relationship of optimization to control into tighter focus. If one defines complexity as the number of ways a system can be described, then it is helpful to think of the scale at which useful descriptions can be found.[7] To illustrate, at the three-star level, a large amphibious landing might be described in terms of, say, ships, objectives, Marine Expeditionary Units (MEUs) and the total number aircraft sorties. From the perspective of the amphibious ship captain or the MEU commanding officer there is much more detail, including transit lanes, synchronized waves, landing zones, and flight schedules. In addition, there are some issues from the higher scale that are not relevant or useful (perhaps not even observable) at this scale. From the individual Marine's viewpoint, there is a host of detail that changes rapidly from one moment to the next, particularly while attempting to cross a hostile beach under fire or while egressing a transport helicopter in a contested landing zone.

This continuum from a broad description at the coarsest scale to a more detailed, yet still aggregated, description at medium scales to a great deal of rapidly changing detail at the finest scales is a property of complex systems. In the most complex parts of a system, fine scale descriptions provide the most useful information. In less complex parts of a system, coarser scale descriptions are sufficient. A graph showing the continuum of complexity and scale for littoral operations such as this notional amphibious operation is shown in Figure 1. It has a complexity-scale curve typical of systems with a great deal of complexity some parts and moderate complexity or simplicity in other parts.[8] The curve is "scale free": there is no single scale at which the all the important system behaviors can be described. Systems exhibiting such a complexity-scale profile are called scale free systems. These systems require "multi-scale representation" to show behaviors and structure at the scale at which they are most informatively displayed.[9]

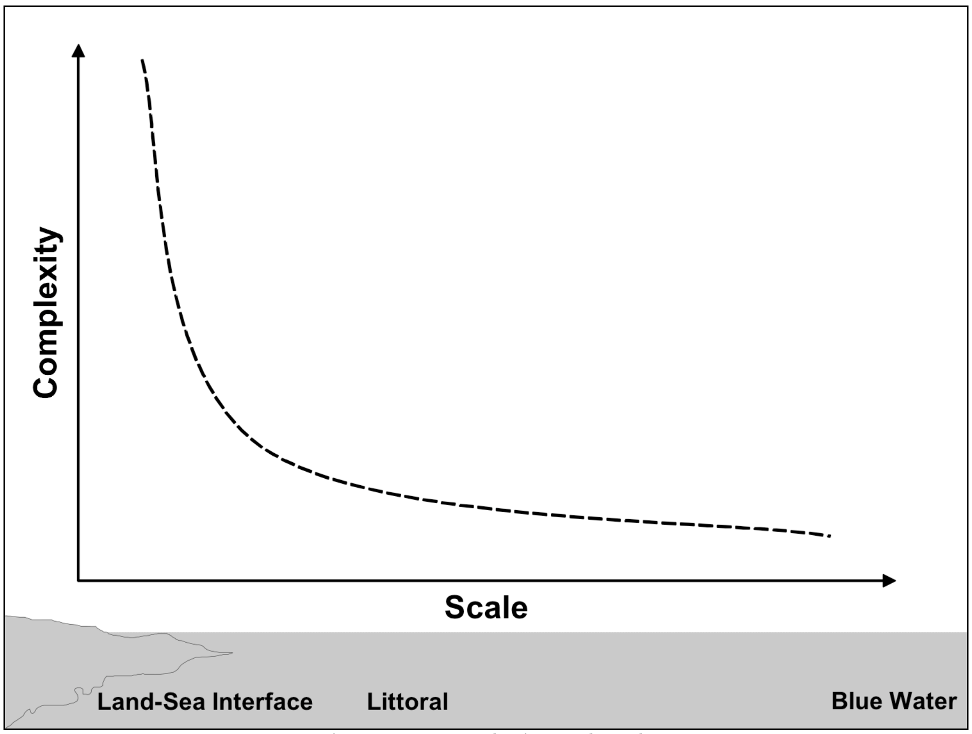


Figure 1 – Complexity and Scale

In the fields of Mathematics and Computer Science, optimization is a quantitative, analytical process for finding solutions in the shortest time possible. Researchers have recently derived what they call the "No Free Lunch (NFL) Theorem" of optimization, which says there are no universally best optimization routines. This theorem proves that all algorithms perform well on one type of problem at the expense of performance on other types of problems. The reason for is this that the success of an optimization routine depends on the extent to which the structure of the algorithm matches the structure of the problem.[10] Another way to say this is that the scale of the routine that performs best is the same as the scale of the problem. Therefore, there exists no universally efficient problem solving routine for scale free complex problems.

By defining the consumptive behavior of a force as a "problem" to be "solved" by logistics, one can propose a similar "No Free Lunch Theorem for Logistics": the best logistics system is one in which the complexity of the logistics process most closely matches the complexity of operations. What logistics structure, then, should be used for complex logistics operations? The answer to this question lies in a formal examination of the larger class of structures of which a chain is only one type: networks.

Network Structures and Diffusion Profiles

The word "network" is ubiquitous in Information Age discourse and is most commonly assumed to mean an IT system. What mathematicians formally call a network, however, is any kind of collection of arcs and nodes. A *connected network* is one in which every node is attached to the network by at least one arc. A *minimally connected network* is one in which the nodes are all connected with the minimum number of arcs possible (the minimum number of arcs nodes is one less than the number of nodes, if the number were lower than this the nodes could not constitute a single network). When a minimally connected network is laid out so that the collection of arcs and nodes resembles a string of pearls, then this network is called a chain. Chains are brittle, require many "hops" to get from one end of the chain to the other, are not very densely connected (in the jargon of networks, they are not very clustered), have a simple pattern, require simple control and operate at a single scale. Thus, a chain is not a good structure for solving a complex logistics problem.

At the other extreme is the maximally connected network. In this network, each node is directly connected to all other nodes. Maximally connected networks have more arcs and more possible subnets than any other type of network and are therefore very expensive. Maximally connected networks are robust (because of their extreme redundancy, snipping arcs will not cause catastrophic failure), require only one hop to get to any other location in the network, and are densely clustered. Since uncertain conditions would require every node to coordinate-with every other node,–a kind of "synthetic epilepsy" occurs in the system: nodes get stuck in conflicting coordination cycles and collective response is inhibited. This, maximally connected networks are not good candidates for a complex logistics system.

A mid-ground between the chain or the maximally connected network is the "regular" network, also known as a "lattice" or "grid." These networks have a standard number of nodes for each arc. A piece of graph paper with nodes placed at each intersection of the vertical and horizontal lines is an example of a lattice or grid network. Because there are four nodes for each square, it is a "regular network of degree four." These networks are robust, require many hops to navigate the grid, are densely clustered, retain a simple pattern and require simple control.[11] Because these networks are scaled they are poor candidates for a complex logistics system. Other scaled networks, such as the random network (in which arcs and nodes are randomly connected) or the Small World Network (a network with the features of both regular and random networks) are scaled and are likewise not good candidates.[12]

Recent research into the topology of the internet, collaboration networks of scientists, and the structure of other networked systems has led to the discovery of a new class of networks, "scale free networks."[13] They have very few nodes with a large number of arcs (these nodes are the networks' "hubs" and the arcs can also be thought of as spokes), a small number of moderately connected nodes and a large number of nodes with few arcs.[14] These networks are very robust, require only a few hops to get from one place to another in the network, are not very clustered, have complex patterns and require complex control. Best of all, these networks are scale free, which means their hubs of connectivity can be adaptively relocated by reconnecting only a small fraction of the network's links. This property makes scale free networks very good candidates for logistics networks in complex environments.

Scale free networks (like other complex networks) have an additional property that might be exploited by logistics networks. While chains typically diffuse at a fixed rate, scale free networks reach a "tipping point" where the rate of commodity diffusion suddenly and dramatically increases until the network reaches maximum capacity. The diffusion rate then hits another tipping point at which the rate of commodity flow starts to slow. This results in an "S" curve. The steepness of the curve and the takeoff point are related to the network structure and are affected by initial values, diffusion rates of the most important nodes and the average diffusion rate of the network. Scale-Free Networks have some of the steepest diffusion curves and hubs can appear very early in network formation. More interestingly, hubs and patterns can be created, disappear and then reappear by changing only a relatively few arcs.[15] If this property is applied to advantage in a logistics network, then scale free networks are not only good structures for logistics networks because they satisfy the No Free Lunch Theorem, but also because they are very adaptive and flexible.

How Distributed Adaptive Logistics Works

Having now reviewed the background, the concept of Distributed Adaptive Logistics can be presented. Figure 2 underscores the difference between supply chains and networks. The supply chain on the left is a prototypical hierarchy. This chain is brittle, has a long "Characteristic Path Length" (CPL, a measurement of the typical length of shortest paths in the network) and may require quite a bit of re-routing/retrograding to move commodities from one side of the chain to the other. In addition, its simplicity would be easy for an enemy to understand and disrupt. In addition, notice a particular feature of using such chains for logistics: the most important nodes – the ones nearest the enemy – are the least connected.

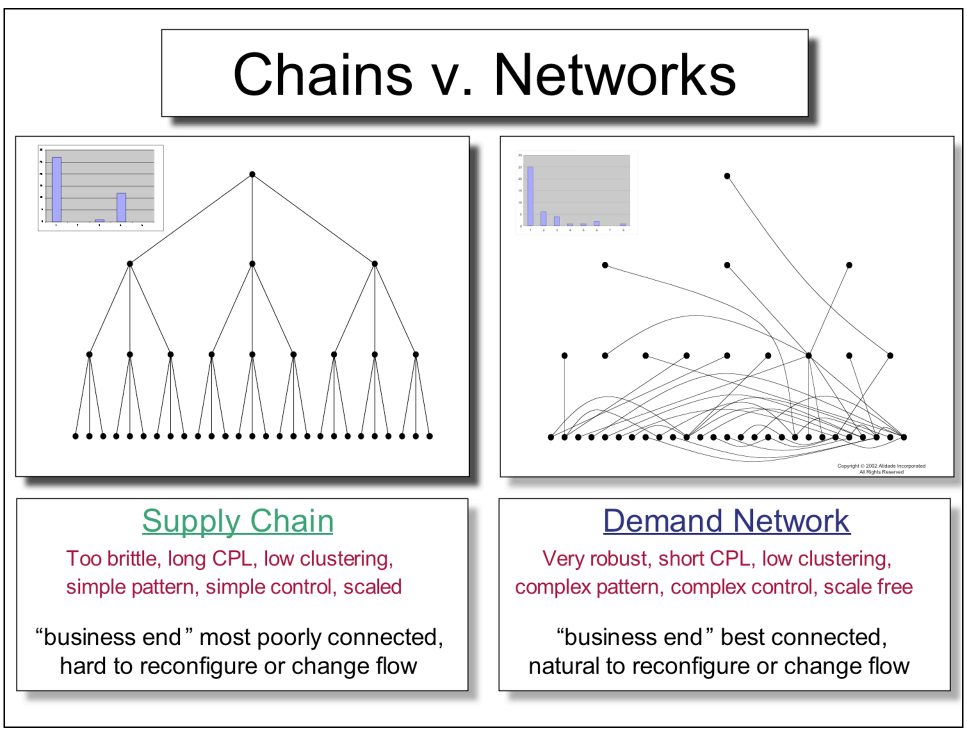


Figure 2

Contrast this with the network on the right. This scale free network is very robust and has a short average distance from one side of the network to another. Because it is scale free it can quite naturally adapt to changes in the competitive environment, and although its complex pattern requires complex control, the network is nonetheless more protected against efforts by an enemy to understand the intent behind its operations. Finally, note how the most important nodes in the network – those nearest the enemy – are very well connected.

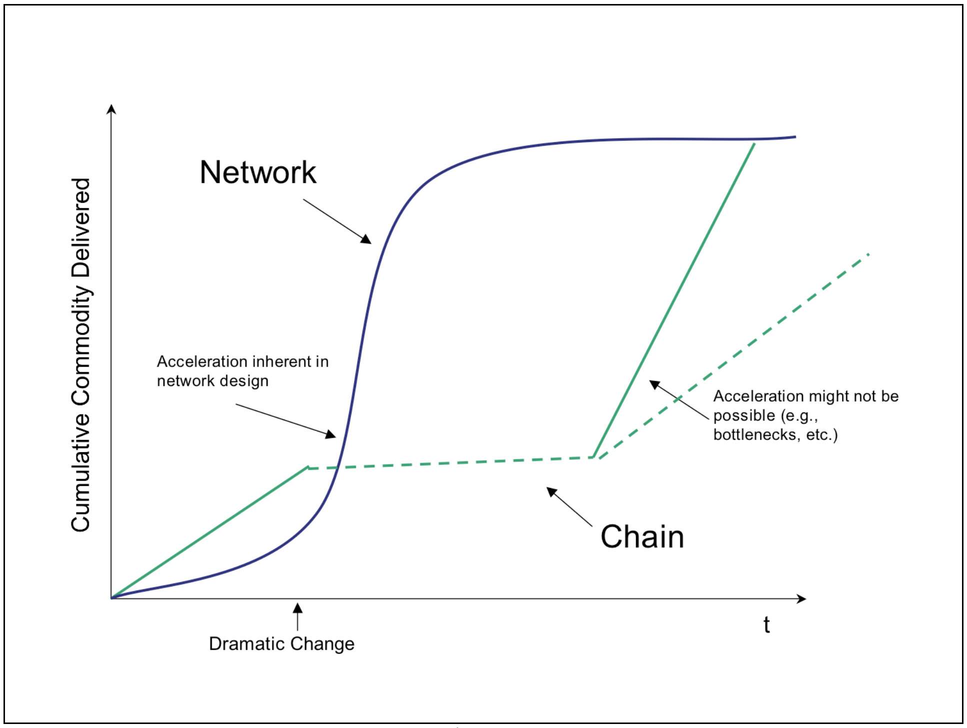


Figure 3

Figure 3, a graph of the accumulation of commodities over time, shows another important difference between chains and networks. While both the network and the chain appear to do well initially, the performance of each type of logistics system begins to diverge if operations experience dramatic change. Commodities in a supply chain accrue roughly linearly by design, limited by the throughput capacity of nodes. A dramatic change will require a substantial shift in flow, to possibly include retrograde and re-shipment down alternative paths. This causes the total rate of throughput to decelerate, as represented by the nearly horizontal dashed line. Only after the system is reconfigured can the supply chain attempt to accelerate delivery to match the theoretical delivery rate of a network. By contrast, the S-shaped curve of the network takes a shape opposite of the supply chain. By exploiting the ability to rapidly move hubs and spokes through the re-connection of a relatively few nodes, a network can deliver commodities more nimbly that a chain in response to changing demand.

Supply Chains v. Demand Networks

It is telling to note the prominence that the word "supply" has in the contemporary logistics community. The Defense Department has supply centers, units have supply officers and the Navy even has a Supply Corps. This focus on supply rather than demand is a perspective rooted firmly in Industrial Age logistics when the gap between consumption and re-supply could be many days, weeks or even months. The "supply system" focused on decreasing time or cost of delivery, and optimized supply chains became the ideal. Companies like Wal-Mart turned the supply chain into a high art using new technology to refine the chain via dis-intermediation (removing levels of hierarchy by rapidly informing suppliers of purchases right at the check-out lane) or finer optimization of an inflexible demand-supply reaction. As profitable and beneficial as such a system is, it is still a chain. As illustrated by the makespan case, this chain still has an upper limit of efficiency. This system would function poorly under the type of uncertainty, complexity and scales inherent in military operations.

By contrast, "demand" is a much better perspective for Distributed Adaptive Logistics than "supply." Demand is the true control signal in the logistics system, containing more information about local operational conditions than the classic aggregation of supply chits ever can. Demand for the tools of battle is intimately related to unfolding battlefield operations, including the uncertainties of combat, and is also quite closely tied to commander's intent. Legacy supply processes require great predictability, depend on the statistics of stability for efficiency and remain a lagging response to dramatic changes in battle conditions. Demand signals provide the best insight into required control methods for complex systems and allow Distributed Adaptive Logistics to adapt by learned response rather than planned reaction.

Conclusion

By turning supply chains into demand networks, Distributed Adaptive Logistics can provide a transformational capability to combat support. Units will no longer be at the far end of a delivery system – those in the main effort will become hubs for logistics support and the system itself can quickly configure to create, remove or reconstitute these hubs as situations warrant. The demand networks of Distributed Adaptive Logistics will more closely tie logistics to operations through commander's intent (perhaps even turn enemy units into receptor hubs for combat power) while obscuring friendly strategies in a distributed logistics train and operating without a centralized dump. Adaptive logistics will be a true Information Age capability as adaptive learning, networked advantages and distributed decision making replace reactive planning, mass and centralized control.

---

[1] "Future Warfare: America's Military Preparing for Tomorrow," http://www.dtic.mil/jv2020/.

[2] Joint Publication 4-0, Doctrine for the Logistics Support of Joint Operations, 6 April 2000, http://www.dtic.mil/doctrine/jel/new_pubs/jp4_0.pdf, accessed 01 Apr 2005.

[3] For example, see the Joint Vision 2020 concept at, http://www.dtic.mil/jv2020/jv2020a.pdf, accessed 01 Apr 2005.

[4] The inspiration for and most of the language used to describe Distributed Adaptive Logistics comes from Stephen H. Haeckel, *Adaptive Enterprise: Creating and Leading Sense and Respond Organizations*, (Harvard Business School Press, Boston, MA, 1999). Since, as Dr. Haeckel notes, "no complete exemplars of the sense-and-respond model exist," (p. xix), this paper comprises a pioneering effort to more fully and formally define the mechanisms by which an sense and respond system can provide extraordinary advantage over its traditional, Industrial Age counterpart. The fundamental ideas behind Distributed Adaptive Logistics are adapted from Jeffrey Cares and Linda Lewandowski, unpublished, undated DoD white paper, "Sense and Respond Logistics: turning Supply Chains into Demand Networks."

[5] For mathematical detail on and discussion of makespan, just-in-time manufacturing and the Toyota production system see http://www.toyotaproductionsystem.net, accessed 01 Apr 2005.

[6] Jeffrey R. Cares, Raymond J. Christian, Robert C. Manke, *Fundamentals of Distributed, Networked Military Forces and the Engineering of Distributed Systems,* NUWC-NPT Technical Report 11,366, 9 May 2002, NUWC Division Newport, 1.

[7] For a full mathematical treatment of complexity and scale in complex systems see Section 8.3 of Yaneer Bar-Yam, *Dynamics of Complex Systems,* (Addison-Wesley, Reading, MA, 1997).

[8] For a complete discussion of the impact of complexity and scale on littoral operations, see Yaneer Bar-Yam, "Multiscale Analysis of Littoral Warfare," CNO Strategic Studies Technical Paper, 2002.

[9] The concept of multi-scale representation has direct application to military command and control problems. For a short definition of this concept, see http://www.necsi.org/guide/concepts/multiscale.html, accessed 01 Apr 2005.

[10] David H. Wolpert and William G. Macready, "No Free Lunches For Search," Santa Fe Institute Working Paper 95-02-010, http://www.santafe.edu/sfi/publications/wpabstract/199502010, accessed 01 Apr 2005.

[11] As long as the degree is less than 5. Chaotic, uncontrollable behavior can emerge with 5 links per node or more. See Stuart A. Kauffman, *The Origins of Order,* (Oxford University Press, New York, 1993), 192-3.

[12] This newly defined class of networks is explored by Duncan Watts in *Small Worlds,* (Princeton University Press, Princeton, NJ, 2000). Networks in this class include the web of actors listed in the Internet Movie Database, which can be interactively explored at http://www.cs.virginia.edu/oracle/, accessed 01 Apr 2005.

[13] See Albert-Laszlo Barabasi, *Linked: The New Science of Networks,* (Perseus Publishing, Cambridge MA, 2002), for a review of the relevant research. In one way, it is misleading to say these networks were "discovered," since these structures are found in very many systems that have existed for centuries, if not millennia. As a tool for describing these structures, however, such networks have been known to researchers for only a very short time.

[14] Scale free networks are different from other types of hub-spoke networks, such as centralized networks with only one hub that connects all nodes in that the distribution of arcs among the nodes matches the complexity-scale curve found in Figure 2. In other words, the presence of intermediate sized hubs is a key feature of scale free networks.

[15] The literature on such diffusion curves is quite rich, including Thomas C. Shelling, *Micromotives and Macrobehavior,* (W.W. Norton & Company, New York, 1978), Everett M. Rogers, *Diffusion of Innovations, 4th Edition,* (Free Press, New York, 1995), Thomas W. Valente, *Network Models of the Diffusion of Innovations,* (Hampton Press, Cresskill, NJ, 1999), and Stuart A. Kauffman, *At Home in the Universe*, (Oxford University Press, New York, 1995).

THE ADAPTABLE FORCE: PRIVATIZATION AND THE PUBLIC MILITARY

Stephen G. Nitzschke
LtCol. USMC

***Abstract**: The government has not done all it should do to promote the development of a flexible, adaptive force through privatization. Revisions should be made in acquisition, licensing and contracting rules so that it will be easier to craft a public/private force mix that maximizes beneficial resource flows, produces quality feedback, elicits appropriate aggregate behavior and minimizes harmful nonlinear effects.*

"If we do not identify our vulnerabilities, fix what is broken, and establish processes to enable innovation and adaptability-if we do not transform-our enemies will surely find new ways to attack us." Admiral A.K. Cebrowski (November 2003)

Introduction

Marine Expeditionary Units (MEUs) consider the evacuation of U.S. civilians in war-torn regions one of its core competencies. Marines have rescued civilians in Liberia, Somalia, Rwanda, Sierra Leone, the Congo and Albania. One such Marine, hardly capable of recognizing the irony of his predicament, found himself in exactly the opposite situation in April 2004. That Marine was wounded during an attack on the Coalition Provisional Authority (CPA) headquarters in Najaf, Iraq. The attack itself was repulsed by civilians, eight commandos from a private security firm called Blackwater Security Consulting. As reported by Dana Priest in the *Washington Post*, the 3 ½-hour gun battle resulted in 4 casualties and required the re-supply and evacuation of *military* personnel by a *civilian* agency. [1] The Defense Department had outsourced CPA security responsibilities to Blackwater. The company used its own helicopter to rescue the wounded Marine. The incident illustrates a practical consequence of a growing Department of Defense trend towards outsourcing, moving traditionally public military capabilities to the private sector. It is just one aspect of the current transformation strategy designed to make the military more adaptable.

Themes on adaptation have permeated and permutated strategic thought in private corporations and public military institutions since the early 1990s, ever since James Glieck, M. Mitchell Waldrop, and John H. Holland published their new science theories on chaos and complexity.[2] Glenn James wrote in 1996 that, "The practical applications of Chaos [complexity] in military technology and strategic thought are so extensive that every military decision maker needs to be familiar with Chaos [complexity] theory's key results and insights."[3] Adaptation is a key feature in a variety of complex environments, including the battlefield environment. Accordingly, the U.S. military began a relationship with the Santa Fe Institute (SFI) in the 1990s to explore the science behind complex adaptive systems.

Adaptation became a recurring theme in a variety of military documents. The Marine Corps' Warfighting publication MCDP-1 states; "Each encounter in war will usually tend to grow increasingly disordered over time. As the situation changes continuously, we are forced to improvise again and again until finally our actions have little, if any, resemblance to the original scheme."[4] These constant improvisations (adaptations) represent the essence of a complex adaptive system. The 2001 *Quadrennial Defense Review* outlined a paradigm shift in force planning. This shift would, "…provide over time a richer set of military options across the operational spectrum than is available today and [would] ensure that U.S. forces have the means to adapt in time to surprise."[5] The United States' *National Military Strategy* (NMS) lists, "adaptable" as one of seven desired force attributes.[6] The NMS defined adaptable as, "…prepared to quickly respond with the appropriate capabilities mix."[7]

The business world was no less enthusiastic about the science of complex adaptive systems. Christopher Meyer, as the Director of the Center for Business Innovation between 1995 and 2002, founded Bios Group, Inc., "…a Santa Fe-based venture that invests in applications of complexity theory to business."[8] Today, as a business consultant, Meyer continues applying adaptive system theory to understand how businesses can cope in an economically volatile environment. Vadim Kotelnikov, the founder of an international web-based business development company called *Ten Cubed Ventures*, in his course, "Winning Organizations: How to Develop Institutional Excellence," lists *adaptability* as the number one organizational trait that determines success.[9] On January 20th 2001, Donald Rumsfeld became the 21st Secretary of Defense. In June, the former chief executive officer of two Fortune 500 companies established the Department of Defense Business Initiative Council (BIC).

The Business Initiative Council's purpose is to, "seek business practices focused on transforming the U. S. Military into a fighting force for the 21st century." Among the council's "quick hit" initiatives recommended in September 2001, was the "Manpower Mix Management Flexibility" proposal. The idea would change full-time civilian end-strength controls to allow DoD more efficient use of contract employees.[10] A fifth set of proposals in June 2002 recommended a series of "Pioneer Projects" that would utilize various sourcing arrangements, to include expanding privatization efforts, to transition the military's non-core competencies to the private sector.[11] The feeling in Washington as James Surowiecki described it was, "Washington fell for the era's biggest business fad: outsourcing. Do only what you do best, and pay someone else to do the rest."[12] Using private military companies (PMCs) to accomplish public military objectives is clearly a strategy designed to make the services more adaptable. The question today is whether the strategy is working.

Specifically, the Defense Department must determine if PMCs contribute to force adaptability. Although that young Marine in Najaf might argue the positive aspects of privatization, there is ample evidence to suggest an alternative view. To date, the Department of Defense has not achieved its goal of creating and maintaining a more adaptable force through privatization. In fact, there are instances which indicate the exact opposite has occurred. To improve adaptability through privatization, the U.S. Government must revise the International Trade in Arms Regulations (ITAR) and improve its contracting practices.

First Things First…

Revising policy to improve the regulation, oversight and legal shortcomings associated with using PMCs is not a new idea. The British House of Commons ordered a *Green Paper* on the subject in 2002, entitled, "Private Military Companies: Options for Regulation." Authors Peter Singer and David Isenberg have both written about oversight, employee vetting and legal loopholes.[13] Even industry leaders recognize some form of increased regulation is necessary. Doug Brooks, President of the International Peace Operations Association (IPOA), an industry trade organization, has published a PMC "Code of Conduct."[14] In response to the British *Green Paper*, Brooks claims, "Most regulations having to do with human rights and accountability will be readily accepted by the PMCs."[15] The U.S. Department of Defense recently initiated its own policy review. In a draft June 2004 Interagency Policy Memorandum entitled, "Contractor Security in Iraq," Deputy Secretary of Defense, Paul Wolfowitz proposed new guidance for all contractors working in Iraq.[16]

Although there is ample reason to suggest PMC policy changes to improve accountability and increase oversight, no one has yet considered policy designed specifically toward improving force adaptability. This paper will recommend policy changes designed to increase that attribute called for in the *National Military Strategy*, adaptability. Complex adaptive system (*cas*) theory will provide the basis for recommending changes to the ITAR and government contracting practices. These changes will reduce the contextual differences between the public and private environment, creating diversity, increasing system flows, and improving system feedback to reduce unwanted nonlinear effects, all in an effort to create a more adaptable force.

CAS Theory in Brief…

Before offering policy to improve force adaptation, it is first necessary to discuss adaptation's salient features within the context of a complex system. John Holland, in his book *Hidden Order: How Adaptation Builds Complexity* lists four general *CAS* properties; aggregation, nonlinearity, flows and diversity. In their most elementary form, complex adaptive systems are sets of nonlinearly interacting parts, agents or components that can adapt to a changing environment. Each agent typically exists within a nested hierarchy of agents within agents. In this case, within the Defense Department (an adaptive agent itself), there exist both military units and private military companies. The interaction between the two units creates an aggregate behavior that further influences agents inside and outside the system. These interactions can contribute to nonlinear behavior. That is to say the actions of one agent can produce disproportionate effects on multiple agents.[17] Take for instance the terrorist actions on 9/11 or those of a few civilian contractors and military personnel at the Abu Ghraib prison; in each case, these actions produced disproportionate effects in other agents.

In addition to aggregate behavior and nonlinear interactions, complex adaptive systems exhibit two other characteristics--flows and diversity. System flows represent the transportation of resources among agents through their connections (relationships). In an economic context flows may include products delivered by rail or the interstate highway system. Similarly during war, resources can be tangible commodities like weapons or logistic support, or less tangible items such as security, inspiration or the will to fight. Flows can improve the chances for survival of an individual agent or contribute to its demise. The resources Blackwater provided military personnel in Najaf clearly contributed to their survival. John Holland says that the persistence of an individual agent depends on the context provided by the other agents: "…each agent fills a niche defined by the interactions centered on that agent; if you remove one agent from the system--creating a hole--the system typically responds with a cascade of adaptations resulting in a new agent that fills that hole."[18]

This cascade of adaptations contributes to the last characteristic of a complex adaptive system, diversity. Diversity can be seen in the wide variety of species encountered in the rain forest, the large number of automobile companies in the economy, and in the different units of a military organization. PMCs have added diversity to the military's organizational structure in Iraq and Afghanistan, filling a niche and creating resource flows in security, logistics and linguistic services. Doug Brooks advocates PMCs fill a peacekeeping niche, a vacancy he says was created by nations unwilling or unable to allocate public military resources towards this end.

The Adaptable Force

To create an adaptable force, the military, as a complex adaptive system, must utilize feedback and alter internal structures (interactions) to confront novel situations. This feedback (a form of system flow) is used to restructure the agent's internal interactions, creating additional diversity and new aggregate behaviors both internal and external to the agent. Of course these new structures must produce the diversity, flows and behavior necessary for success within a given context, in this case, the context defined by human conflict.

It is intuitively obvious that designing policies to increase beneficial resource flows and improve feedback will alter internal structures more effectively, and therefore improve the agent's adaptive process. Kathleen M. Carley, in her work on organizational adaptability noted that the most successful organizations tend to be highly flexible. They hire more, they fire more, they re-assign and re-engineer more often.[19] Successful agents are those whose interactions produce behaviors best suited to achieve their purpose within a given context.

The Private Military Company

Private military companies are playing an increasing role in a wider variety of contextual settings, including contingency, stability, and combat operations. Today there are foreign and domestic PMCs operating in North America, South America, Africa, Asia, Europe and the Middle East. In the United States, the Department of Defense contracts logistics, military training, security and intelligence functions from private contractors such as Halliburton, MPRI, Blackwater, CACI International Inc. and Titan. A CPA report to Congress listed 60 PMCs operating in Iraq today. David Isenberg, in his report for the British American Security Information Council (*BASIC*) points out that "...during the Gulf War in 1991 for every one contractor there were fifty military personnel involved. In the 2003 conflict the ratio was 1 to 10."[20]

As active duty military forces remain engaged in major theaters like Iraq and Afghanistan, private firms have advanced U.S. interests in so-called "economy of force" theaters. Where the alternative is neglect, the U.S. employs PMCs to provide logistic support and train local militaries. PMCs are presently accomplishing both tasks in Africa, South America and the Balkans. Theresa Whelan, Deputy Assistant Secretary of Defense for African Affairs, in a November 2003 speech to the IPOA listed rapid response and reduced costs as two advantages of employing U.S. contractors in Liberia earlier that year. Often private firms hire local personnel to facilitate their operations. This provides advantages in understanding local customs and identifying important leaders. In many instances, PMCs have demonstrated significant flexibility.

Peter Singer argues that a PMC's "virtual nature" gives them a degree of innate adaptability. Many companies require little permanent infrastructure, rely on client provided hardware, and maintain a personnel database that provides instant access to hundreds of highly skilled former military personnel. They can tailor and task-organize a force specifically designed for a particular regional conflict. He says, "The virtual nature of the structure often provides the potential for a short but profitable organizational half-life. Companies can rapidly dissolve and recreate themselves whenever the need arises."[21]

Today, constructing a defense force with the right mix between public and private capability is more important than ever. The NMS calls for a seamless mix of active forces and contract workers.[22] Categorizing and classifying private defense related services helps government officials determine this mix. To increase adaptability, Defense Department and Department of State personnel must create a force mix that maximizes beneficial system flows, produces quality feedback and appropriate aggregate behaviors (interactions) that minimize harmful nonlinear effects.

International Traffic in Arms Regulations (ITAR)

Kathleen Carley admits, "Little is known about organizational adaptation, and even less about how organizations should change…Organizational performance is a function of many factors of which the various elements of design is only one component, but one over which the organization has some, albeit limited control."[23] Designing a public/private force mix that produces the correct resource flows, feedback and aggregate behavior requires a clear understanding of these characteristics in each organization, and a compensatory assumption of their combined behavior within the appropriate context. The government is familiar with public military organizations, but it often lacks similar knowledge of private military companies.

The private military company is an amorphous organization. Peter Singer describes PMCs in business terms as "boundary spanning."[24] Singer and Isenberg both recognize three basic types of PMC firms: military support, military consultant and military provider.[25] The military support firm is the most widely recognized and accepted type within the broader category. Contractors who offer advice and logistical support for operating and maintaining military equipment fall into this category (Northrop-Grumman, Raytheon, and General Dynamics). Consultants offering military advice on everything from training and organization to employment tactics fall into this second organizational type (MPRI, DynCorp and SAIC). Some of these companies have expanded their operations to include services offered by the last type, military provider firms. These firms may actively participate in direct combat. Some companies, like the South African firm Executive Outcomes (EO), offered a full array of military services, to include a combined arms capability. Although EO no longer exists, it shaped the outcome of conflicts in Angola (1993) and Sierra Leone (1995). Blackwater, the firm in Najaf City, falls under this third type. Many companies, however, are not easily classified into a single type. As Singer points out, "The proviso of any such typology…is that it is a conceptual framework rather than a fixed definition of each and every firm."[26] Moreover, these definitions do little to identify adaptive qualities within the organization.

Other "typologies" do less to define resource flows and predict potential behaviors. Doug Brooks, classifies PMCs into passive and active categories.[27] The more passive companies may provide advisors during actual conflict but do not engage in actual combat. MPRI reportedly provided this service to Croatia during *Operation Storm* in 1995.[28] Active companies actually replace or augment a nation's military forces during combat. The British firm, Sandline, was the catalyst behind the Papua New Guinea government's collapse in 1997. Prime Minister Julius Chan resigned during violent protests over his decision to use Sandline, rather than the Papua New Guinea Defense Force (PNGDF) to quell a Bougainville Island rebellion.[29] Typology such as "offensive" and "defensive" or the Defense Department's use of "core" and "non-core" skills means little in the realm of human conflict, where peacekeeping operations can become peace enforcement to full blown combat in a matter of minutes or in the space of a few city blocks. The solution is to ignore the company itself and define its services (capabilities). The vehicle most appropriate for this task resides within the State Department.

The U.S. Government must clearly categorize and classify defense related services. The President of the United States is given authority to control the export of defense articles and defense services under section 38 of the Arms Export Control Act (22 U.S.C. 2778). The President delegates the statutory authority to regulate these exports to the Secretary of State. The regulations are administered by the Deputy Assistant Secretary for Defense Trade Controls (DAS-Defense Trade Controls) and the Managing Director of Defense Trade Controls (MD-Defense Trade Controls). The MD-Defense Trade Controls uses federal regulations outlined in the

International Traffic in Arms Regulations (ITAR) to enforce exportation policy for both defense articles and defense services.[30] The State Department receives support from the Department of Defense, primarily from the Under Secretary of Defense for Acquisition, Technology and Logistics (USD AT&L).

Although the exportation of defense services is regulated under the ITAR, the document's primary focus is on defense articles, equipment and munitions. Part 121, entitled "The United States Munitions List," takes 23 pages to classify hundreds of defense articles into 20 separate categories.[31] Listed items include everything from rifle scopes to guided missiles. Items are categorized according to their impact on national security and foreign policy interests. Part 120.2 states, "Such designations are made by the Department of State with the concurrence of the Department of Defense."[32] Part 123 of the ITAR, "Licenses for the export of Defense Articles," outlines requirements, special controls and non-transfer clauses for defense articles. There is no similar section devoted to defense related services.

The State Department, using this new classification system, must also expand licensing criteria for private defense services. Currently the Office of Defense Trade Controls reviews individual license applications for service contracts in excess of $50,000,000.[33] Defense services under Part 120.9 are defined almost exclusively as military technical assistance and military training services. The DAS-Defense Trade Controls must now make licensing decisions for security, counterinsurgency and hostage rescue services. It must do so without a comprehensive list that classifies these services in relation to their impact on national security and foreign policy interests. Furthermore, the DAS-Defense Trade Controls has no document categorizing the potential impact a combination of defense services and/or defense articles may have on national security or foreign policy.[34]

Adding a "United States Defense Services List" and expanding ITAR licensing criteria to include these services would allow government officials to make better preliminary assessments regarding system resource flows and aggregate behaviors. DAS-Defense Trade Controls can then use licensing criteria to identify categories or category combinations as either acceptable or unacceptable based upon their assessment. In this manner, the Office of Defense Trade Controls can reduce the possibility for unwanted nonlinear effects.

For example, a PMC offering counterinsurgency training to a weak foreign government may benefit U.S. policy. However, if that company exported modern weapons and a counterinsurgency force of its own, in addition to the training capability, the result might be quite different. This was the general scenario in 1997, when the PNGDF objected to Sandline's involvement in the Bougainville rebellion. Categorizing defense related services also helps minimize contextual differences between public and private institutions.

There is an inherent conflict between public and private interests. Actions taken by a publicly supported military are assumed to revolve around the public good and are perceived to support national objectives. The public has a voice through Congress and the ballot box on the use, regulation and oversight of public military forces. Military personnel are rewarded through promotions and prestige from accomplishing missions that serve the public's interest. PMCs, however, are limited by the scope of their contract. National interests are often considered secondary to the corporate well-being. Individuals are promoted for their contributions to the company, not the country. Singer describes this conflict of interest in his book, *Corporate Warriors: The Rise of the Privatized Military:*

> Private firms operate in gray areas where national interest is not clear and thus more easily contorted to private advantage, even unconsciously. Private companies have distinctly different motivations, responsibilities, and loyalties

> than those of the public military. No matter their background, while in a private company, employees are directly responsible to the corporation and its executives.[35]

What Singer describes here is a different environmental context for adaptation between the public military and private industry. Government officials are unlikely to eliminate this difference completely, but they can revise government contracting practices to minimize the disparity.

Government Contracting

Creating contract policy to minimize contextual differences is a key element to improving military adaptability. Lacking a similar context, each agent is left to alter internal structures based on feedback from different environments. The result may be conflict rather than cooperation among the relevant agents. The U.S. Government must revise federal contracting practices to increase joint training between military forces and private firms, improve the transparency in public/private relationships, establish common lines of authority, and eliminate legal disparities between uniformed military personnel and private employees. These reforms reduce contextual differences by increasing constructive resource flows (doctrine, standard operating procedures, rules of engagement), improving the fidelity and periodicity of feedback (intelligence, situation and after action reports), and helping produce desired aggregate behaviors.

A striking example, illustrating a need for such reform, is the prisoner abuse scandal at Abu Ghraib. The U.S. Government employs CACI and Titan contractors to provide linguistic support for U.S. Forces in Iraq. According to David Isenberg's *BASIC* report, CACI and Titan together provide over 4,400 linguists to U.S. forces.[36] Under their contract, and contrary to Army policy, some of these linguists were also performing prisoner interrogations.[37]

Secretary Rumsfeld testified before Congress that some 37 civilian interrogators had been assigned to Abu Ghraib, where prisoners were allegedly humiliated and tortured.[38] Major General Antonio M. Taguba discussed contractor participation in his report on the Abu Ghraib abuses. Excerpts from the report published on-line indicate that civilian contractors either, "allowed and/or instructed MPs, who were not trained in interrogation techniques, to facilitate interrogations by 'setting conditions' which were neither authorized and [sic] in accordance with applicable regulations/policy."[39] Referring to U.S. civilian contractors, third country nationals and local contractors, the report stated, "During our on-site inspection, they wandered about with too much free access in the detainee area. Having civilians in various outfits (civilian and desert camouflage) in and about the detainee area causes confusion and may have contributed to the difficulties in the accountability process…" [40] When asked how the chain of command worked at Abu Ghraib between her unit and civilian contractors, Brigadier General Janis Karpinski replied, "We have no control over them at all."[41]

The method by which CACI received its initial contract illustrates the difficulty behind identifying appropriate relationships, command or otherwise. As part of an effort to reinvent government in the 1990's, the Clinton-Gore administration initiated a "National Performance Review (NPR)." The NPR era procurement reforms allow the U.S. Government to purchase new articles and services under existing indefinite delivery/indefinite quantity (ID/IQ) contracts.[42] CACI actually received a no-bid opportunity to provide the Army's linguistic services from a company it inherited (Premier Technology Group) that already had a "blanket purchase agreement," awarded in 2001, by the Department of the Interior.[43] ID/IQ contracts and corporate subcontracting practices obscure relationships needed to provide resources, and blur the chain of command required to deliver feedback. Procurement officials must provide transparency and designate clear lines of authority in each contract. Both objectives reduce the contextual differences between public and private operators. The alternative is additional uncertainty and increased risk of potentially harmful nonlinear effects. Different legal standards also skew the context between military members and civilian contractors.

Unlike active duty military personnel, contract employees are not subject to the Uniform Code of Military Justice, and therefore they cannot be charged under Article 92 for a failure to obey a lawful order. Instead they face a hodge-podge of potentially contradictory regulations that fail to fully align public and private interests. A status of forces agreement (SOFA) or bi-lateral arrangements may include legal options for contractors employed by the Department of Defense. Host countries may assert their right to enforce local laws, or the United States can attempt to enforce federal laws under the 1996 War Crimes Act.

In his BASIC report, Isenberg lists other legal options to hold contractors accountable, from the international criminal courts to a new "Convention on the Use of Armed Non-Military Contractors by an Occupying Force."[44] The most promising in terms of creating a common legal framework is the Military Extraterritorial Jurisdiction Act (MEJA) of 2000. The act applies to criminal offenses committed by persons employed or accompanying the Armed Forces. Regarding the act, Isenberg stated (September 2004) the following:

> …the Pentagon has not yet formalized or signed the implementing regulations for the 2000 law. On February 10, 2004 the Department of Defense issued its first proposed rules for MEJA implementation. The rules, however, were limited by the statutory constraints of MEJA, preventing DoD from clarifying the outstanding questions about civilians contracted by agencies outside the DoD.[45]

Michael Wynne, acting Under Secretary of Defense for Acquisition, Technology and Logistics said before the House Armed Services Committee in June 2004, "Currently, the procurement regulations do not have a standardized approach for addressing most issues that deal with contractors accompanying the forces engaged in contingency, humanitarian, peacekeeping or combat operations outside the United States."[46] Until a broader policy is in place, procurement officials must include contractual obligations that hold civilian employees legally accountable, with standards comparable to military law. Contract officials must also include training requirements to increase interoperability between the military and the private sector.

Training works "muscle groups," improving flows and feedback to benefit internal structures. Training also provides a common foundation of knowledge and understanding. Unfortunately, the military does not maintain extensive doctrinal publications guiding public/private training evolutions. At the tactical level, Army publications include FM 100-10-2, *Contracting Support on the Battlefield* and FM 100-21, *Contractors on the Battlefield*.[47] Singer notes that the field manuals fail to address today's relevant issues.[48] Isenberg lists numerous doctrinal publications covering contractors in his BASIC report, but with the singular exception of an Air Force publication, *Deploying with Contractors: Contracting Considerations*, all were written prior to March 2000. In its report, *Detainee Operations Inspection*, the Army's Inspector General said, "Of the contract interrogators in Operation Iraqi Freedom (OIF), 35% (11 of 31) had not received formal training in military interrogation techniques, policy and doctrine."[49] A lack of relevant, standardized procedures only increases the contextual uncertainties adaptive agents must confront to modify their structures and change behaviors. Even locally generated standard operating procedures and rules of engagement must be learned on the job unless contracts mandate appropriate prior training.

Conclusion

To create an adaptable force, the military must constantly utilize feedback, altering internal structures to confront novel situations. These structures must produce the diversity, resource flows, aggregate behavior and nonlinear effects that contribute to its success. Successful adaptations occur more often when agents share a common environmental context. Finally, complex adaptive system theory highlights the importance of not only the individual agents, but the interactions between agents and their resulting aggregate behaviors.

The Defense Department has not yet achieved its goal of creating an adaptable military force through privatization. To do so, it must craft a public/private force mix that maximizes beneficial resource flows, produces quality feedback, elicits appropriate aggregate behavior and minimizes harmful nonlinear effects.

The U.S. Government must revise the International Trade in Arms Regulations (ITAR) and improve government contracting practices. The government should categorize and classify defense related services according to their impact on national security and foreign policy. It should establish a licensing policy to identify appropriate defense article and/or defense service combinations. Government contracts should include mechanisms to minimize the contextual differences between public and private force components. These mechanisms must mandate training, improve transparency, define lines of authority, and reduce legal disparities between public military members and private employees. These revisions will give government officials the tools to assess and create appropriate diversity, resource flows, aggregate behaviors and nonlinear effects. The result will be a more adaptable military force.

---

[1] Dana Priest, "Private Guards Repel Attack on US Headquarters," (Washington Post, April 6, 2004), 1.
[2] James Gleick, Chaos: Making a New Science (New York: Viking Penguin Inc., 1987); John H. Holland, Adaptation in Natural and Artificial Systems, 4th ed. (Cambridge, MA: MIT Press, 1995.); M. Mitchell Waldrop, Complexity: The Emerging Science at the Edge of Order and Chaos, (New York: Simon and Schuster, 1992).
[3] Glenn E. James, "Chaos Theory: The Essentials for Military Applications," Newport Papers Number 10, (October 1996.), 15.
[4] United States Marine Corps, Warfighting, MCDP-1 (Department of the Navy: Washington, D.C. June 1997) 19.
[5] Department of Defense, Quadrennial Defense Review Report, (Washington, DC: 30 September 2001), 17.
[6] Joint Chiefs of Staff, National Military Strategy of the United States of America, (Washington, DC: 2004), IV.
[7] Ibid., 14.
[8] Chris Meyer, nerve website, on-line at < http://www.gotnerve.com/biography.html/ > 1 [25 Feb 2005]
[9] Vadim Kotelnikov, "Winning Organizations: How to Develop Institutional Excellence," Ten Cubed Ventures 2004 on-line at < www.1000ventures.com/founder_msg.html/ > [3 October 2004]
[10] Edward C. Aldridge, Jr., Department of Defense Memorandum, Department of Defense Business Initiative Council. 19 Sept. 2001.
[11] Edward C. Aldridge, Jr., Department of Defense Memorandum, Department of Defense Business Initiative Council. 12 Jun. 2002.
[12] James Surowiecki as quoted in David Isenberg, *A Fistful of* Contractors: The Case for a Pragmatic Assessment of Private Military Companies in Iraq, (British American Security Information Council research report, September 2004), 16.
[13] David Isenberg, A Fistful of Contractors: The Case for a Pragmatic Assessment of Private Military Companies in Iraq, (British American Security Information Council research report, September 2004), 69-71; Peter W. Singer, Corporate Warriors: The Rise of the Privatized Military Industry, (Ithaca, NY: Cornell University Press, 2003), 214.
[14] International Peace Operations Association on-line at < http://www.ipoa.org/ > [28 September 2004]

[15] Doug Brooks, "Protecting the People: Comments and Suggestions for the UK Green Paper on Regulating Private Military Services," (25 July 2002), 4. On-line at, < http://www.ipoaonline.org/ > 4. [3 October 2004]
[16] David Isenberg, A Fistful of Contractors: The Case for a Pragmatic Assessment of Private Military Companies in Iraq, (British American Security Information Council research report, September 2004), 43.
[17] *Effects Based Operations* and terrorism exploit the nonlinear properties of a complex adaptive system to the advantage of one or more agents. For a complete discussion of complex adaptive system characteristics and properties see, John H. Holland, *Hidden Order: How Adaptation Builds Complexity*, (New York: Addison-Wesley Pub., Co., 1995)
[18] John Holland, Hidden Order, (New York, NY: Addison-Wesley Pub. CO: 1995), 127.
[19] Kathleen M. Carley, 1998 "Organizational Adaptation," Annals of Operations Research 75: 25-47.
[20] David Isenberg, A Fistful of Contractors: The Case for a Pragmatic Assessment of Private Military Companies in Iraq, (British American Security Information Council research report, September 2004), 7.
[21] Peter W. Singer, Corporate Warriors: The Rise of the Privatized Military Industry, (Cornell University Press, Ithaca NY: 2003), 75.
[22] Joint Chiefs of Staff, National Military Strategy of the United States of America, (Washington, DC: 2004), 23.
[23] Kathleen M. Carley, 1998 "Organizational Adaptation," Annals of Operations Research 75: 1-6.
[24] Peter W. Singer, Corporate Warriors: The Rise of the Privatized Military Industry, (Cornell University Press, Ithaca NY: 2003), 75.
[25] David Isenberg, A Fistful of Contractors: The Case for a Pragmatic Assessment of Private Military Companies in Iraq, (British American Security Information Council research report, September 2004), 15.
[26] Peter W. Singer, Corporate Warriors: The Rise of the Privatized Military Industry, (Cornell University Press, Ithaca, NY: 2003), 91.
[27] Doug Brooks, "Protecting People: The PMC Potential," (International Peace Operations Association: 25 July 2002), 3. on-line at , < http://www.ipoaonline.org/ > [3 October 2004]
[28] Peter W. Singer, Corporate Warriors: The Rise of the Privatized Military Industry, (Cornell University Press, Ithaca NY: 2003), 126.
[29] Peter W. Singer, Corporate Warriors: The Rise of the Privatized Military Industry, (Cornell University Press, Ithaca, NY: 2003), 192.
[30] 22 CFR Parts 120-130., International Traffic in Arms Regulations (ITAR) Defense Trade Controls-Reference library. Government Printing Office, 1 Apr 2004. Online at < http://pmdtc.org/reference.htm/ >
[31] Ibid., Part 122
[32] Ibid., Part 120.2
[33] Ibid., Part 123.15(a)
[34] While the ITAR does address some traditional PMC services, it does not adequately confront licensing criteria for companies actively engaged in the application of force, psychological operations, information warfare etc…
[35] Peter W. Singer, Corporate Warriors: The Rise of the Privatized Military Industry, (Cornell University Press, Ithaca, NY: 2003), 154.
[36] David Isenberg, A Fistful of Contractors: The Case for a Pragmatic Assessment of Private Military Companies in Iraq, (British American Security Information Council research report, September 2004), 37.
[37] Ibid., 54
[38] Ibid., 51
[39] Antonio M. Taguba MajGen,"Article 15-6 Investigation of the 800th Military Police Brigade,"(February 2004) 34. On-line at < http://scoop.agonist.org/annex/taguba.htm > [11 Oct 2004]
[40] Ibid., 20.
[41] David Isenberg, A Fistful of Contractors: The Case for a Pragmatic Assessment of Private Military Companies in Iraq, (British American Security Information Council research report, September 2004), 61
[42] John Berlau, "Democrat Attacks on Contractors," Insight, (2 February 2004),1. On-line at http://www.insightmag.com/news/2004/02/17/national/Democrat.Attacks.On.Contractors-593359.Shtml/ [10 October 2004]
[43] David Isenberg, A Fistful of Contractors: The Case for a Pragmatic Assessment of Private Military Companies in Iraq, (British American Security Information Council research report, September 2004), 51.
[44] David Isenberg, A Fistful of Contractors: The Case for a Pragmatic Assessment of Private Military Companies in Iraq, (British American Security Information Council research report, September 2004), 72.

[45] Ibid., 65

[46] Jim Wolf, "US Lacks Standardized Rules for Iraqi Contractors," ABC News, (24 Jun 2004), on-line at <http://www.abcnews.go.com/wire/US/reuters20040624_514.html,accessedhttp://www.abcnews.go.com/wire/US/reuters20040624_514.html,accessed > [2 Oct 2004]

[47] Department of the Army, Contracting Support on the Battlefield. FM 100-10-2, (Department of the Army, 15 April 1999; Department of the Army, *Contractors on the Battlefield,* FM 100-21. (Washington: Headquarters, September 1999) On-line at < http://www.army.mil/usapa/doctrine/100_Series_Collection1.html/ >

[48] Peter W. Singer, Corporate Warriors: The Rise of the Privatized Military Industry, (Cornell University Press, Ithaca, NY: 2003), 124. Singer also points out that the Army's Training and Doctrine Command (TRADOC) hired MPRI to develop and write the manuals. In essence, "a private company wrote the rules that govern how the Army would interact and manage other such companies."

[49] Department of The Army, The Inspector General, Detainee Operations Inspection, op. cit., pp 87-89 as quoted in, David Isenberg, A Fistful of Contractors: The Case for a Pragmatic Assessment of Private Military Companies in Iraq, (British American Security Information Council research report, September 2004), 59.

Southwest Airlines and Network-Centric Operations

Michael I. Bell
24 August 2005

Abstract: *The network defined by the passenger routes served by Southwest Airlines is examined as a case study of potential interest to designers of small tactical networks for military or homeland security applications. Evidence is found that this network grew by a process involving selective attachment of new nodes to existing ones with large numbers of connections (hubs). Somewhat surprisingly, the Southwest network is found to be much more resistant to disruption by the deletion of such hubs than are the scale-free networks produced by growth and preferential attachment and widely studied in the technical literature. The implications of this result for network-centric operations and warfare are discussed briefly.*

Introduction

The concept of network-centric warfare (NCW)[1] and the closely related themes of network-centric operations (NCO) and network-enabled capability (NEC) have gained such rapid acceptance that it is easy to assume that any major technical issues associated with implementing these ideas have been resolved. Re-enforcing this impression, recent advances in our understanding of complex networks[2] have enabled us to describe quantitatively the structure and behavior of physical and social networks with unprecedented accuracy and completeness. Nevertheless, the networks of communication, command and control, collaboration, and logistics that will support highly coordinated, distributed systems delivering NCW capabilities have yet to be built and tested. Our theoretical ideas concerning the design and performance of such networks also remain untested. The purpose of this note is to examine briefly one example of an existing network that very effectively provides a service relevant to NCW (transport) while contradicting significant findings of recent theories of complex networks.[3] The goal is neither to cast doubt on the feasibility of NCW nor to question the validity of the theory but simply to serve as a warning that we are entering onto new territory where we may well encounter surprises.

Network Structure

It is well known that many networks of practical interest exhibit a scale-free structure characterized by a power-law degree distribution. That is,

$P(k) \sim k^{-\gamma}$,

where $P(k)$ is the probability that a node has degree (number of connections) equal to k. For a wide range of models and real-world networks, the exponent γ has been found to lie in the range

$2 \leq \gamma \leq 3$. Examples have been found in information technology (the Internet, the World Wide Web, and e-mail networks), in social behavior (collaboration, problem solving, and sexual contacts), and in natural systems (neurological networks, food webs, and biochemical systems). It has been shown[4] that if a network evolves by a process of growth and preferential attachment, with new nodes tending to connect to nodes that already have many connections, the result is a power-law degree distribution. There is no conclusive evidence that the networks mentioned above are produced by growth and preferential attachment, and there may be other mechanisms that lead to a power-law degree distribution, but the concept has proved to be a fruitful starting point for investigation.

The Southwest Airlines Network

An important and widely cited observation is that scale-free networks tend to be highly resistant to random node failure but vulnerable to attack, that is the selective removal of nodes with high degree, together with all their links.[3] Against this background, it is instructive to examine a small network that is potentially representative of the tactical communications, transport, and collaboration networks we will deploy in future operations. This network shows evidence of having resulted from growth and preferential attachment, but it proves to be far more resistant to attack than the scale-free networks studied to date. This analysis began as an example to be used in an informal tutorial on graph and network theory for Naval officers.[5] The goal was to examine a familiar network that was large enough to be interesting but small enough to visualize and to examine with simple tools. This report expands somewhat on that work, but uses only the data available at that time.

The network chosen was based on the flight schedule of Southwest Airlines.[6] Each airport is a node (vertex, in the language of graph theory), and links (edges) represent one or more non-stop flights between the airports. (The links are regarded as bi-directional, since every city pair served by non-stop flights has such service in both directions.) The Southwest Airlines network (SWAN) defined in this way can be studied by the formal methods of graph theory or network analysis.[7] As of January 2000, when the data for this study was first collected, Southwest served 55 cities using 56 airports.[8] Non-stop flights connected 294 city pairs. It would be useful to examine subsequent expansion of the network, and we do this briefly for cities added during 2000, but this is not likely to affect the main conclusions of this study.

Connectivity data extracted from the Southwest Airlines schedule was entered into the UCINET[9] network analysis program. UCINET and its companion program NetDraw were used throughout the analysis. The SWAN is shown in Fig. 1, with its nodes identified by the standard three-letter airport codes. A fully connected network of $n = 56$ nodes would have $n(n\text{-}1)/2 = 1540$ links, so the SWAN is sparse, with the number of edges closer to n than n^2. Figure 2 shows the degree distribution, that is, the number of vertices n_k for each value of k. The average value of k is 10.5, and the median is 8. The existence of nodes with very high degree ($k > 20$) is perhaps not surprising, since the airlines have favored the so-called "hub and spoke" architecture, especially since deregulation. The result is remarkable, however, in two other respects. One is the sharp peak in the distribution at $k = 5$. There is no reason to anticipate a strong preference for any particular number of non-stop connections, and five is not a number likely to arise as the residue of a regular lattice structure or other obvious mechanism. Second, rather than exhibiting a continuous decrease with increasing k, the distribution n_k has a number of secondary peaks. In fact, it is possible to imagine that the peaks in Figure 2 occur at intervals of five, except at $k = 30$. This suggests a hierarchy of hubs, "mini-hubs" and "super-hubs," possibly arising from the same mechanism that produces the $k = 5$ peak. These questions are beyond the scope of the present study, although some related observations are made in the closing discussion.

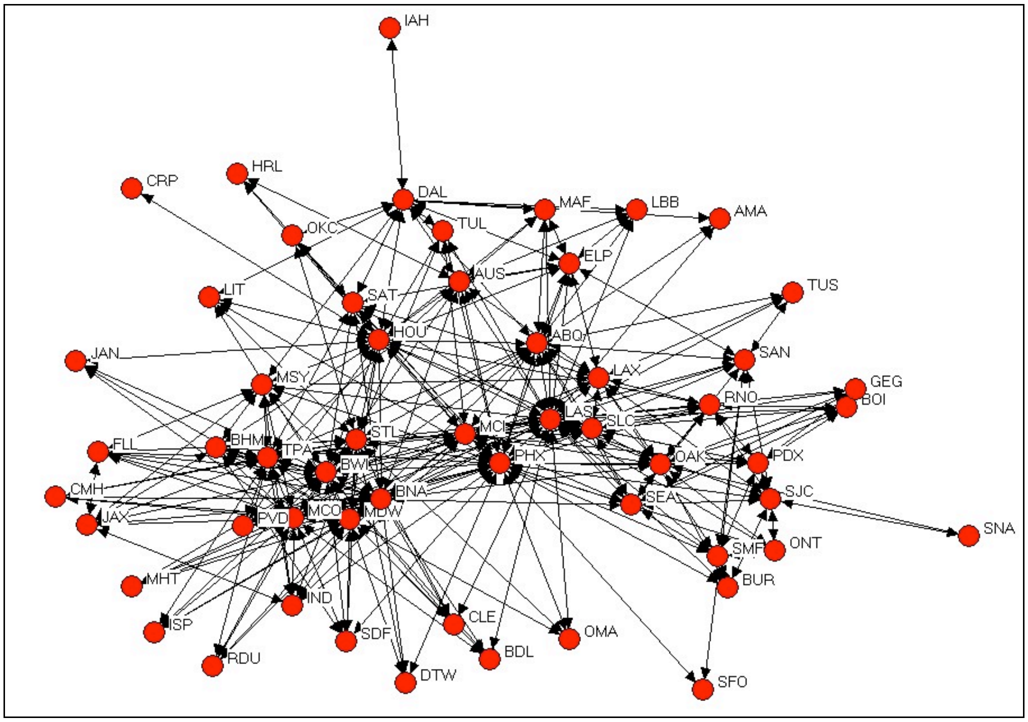


Figure 1. Southwest Airlines network (January 2000).

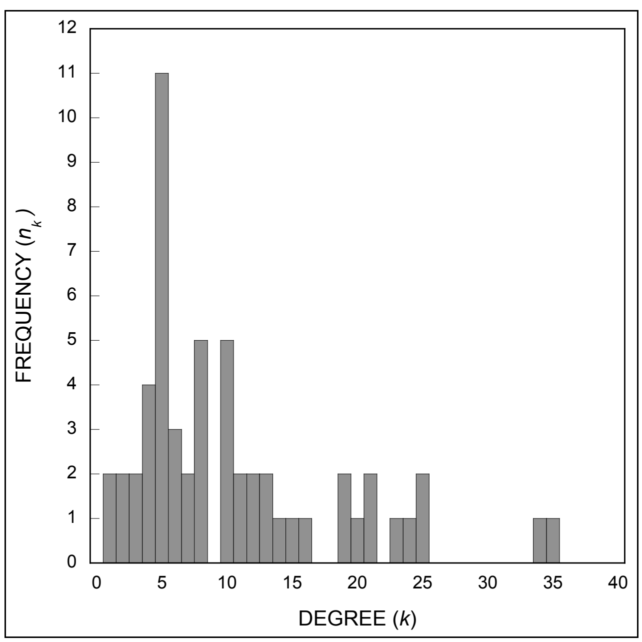


Figure 2. Node count as a function of degree.

The SWAN is too small to permit reliable conclusions about the frequency of high-degree nodes. In particular, it is impossible to determine whether or not $P(k)$ has power-law behavior. There is strong evidence, however, for preferential attachment of nodes, one of the two proposed requirements for the construction of a scale-free network. Figure 3 shows, as a function of the degree of each node, the average degree of the nodes to which it is linked. The line of slope one indicates the point where a node and its average neighbor have the same degree. Clearly, nodes of low degree are linked to nodes of high degree. It is worth noting that there is no evidence for the inverse relationship, that is, high-degree nodes linking preferentially to low-degree ones, although this is sometimes regarded in the literature as an expected consequence of preferential attachment. In the present case, all but the two nodes of highest k-value could attach preferentially to nodes with k at or below the median value of 8, and even these two could link, on the average, to nodes with k less than the mean value of 10.5. Figure 3 shows clearly that this is not the case.

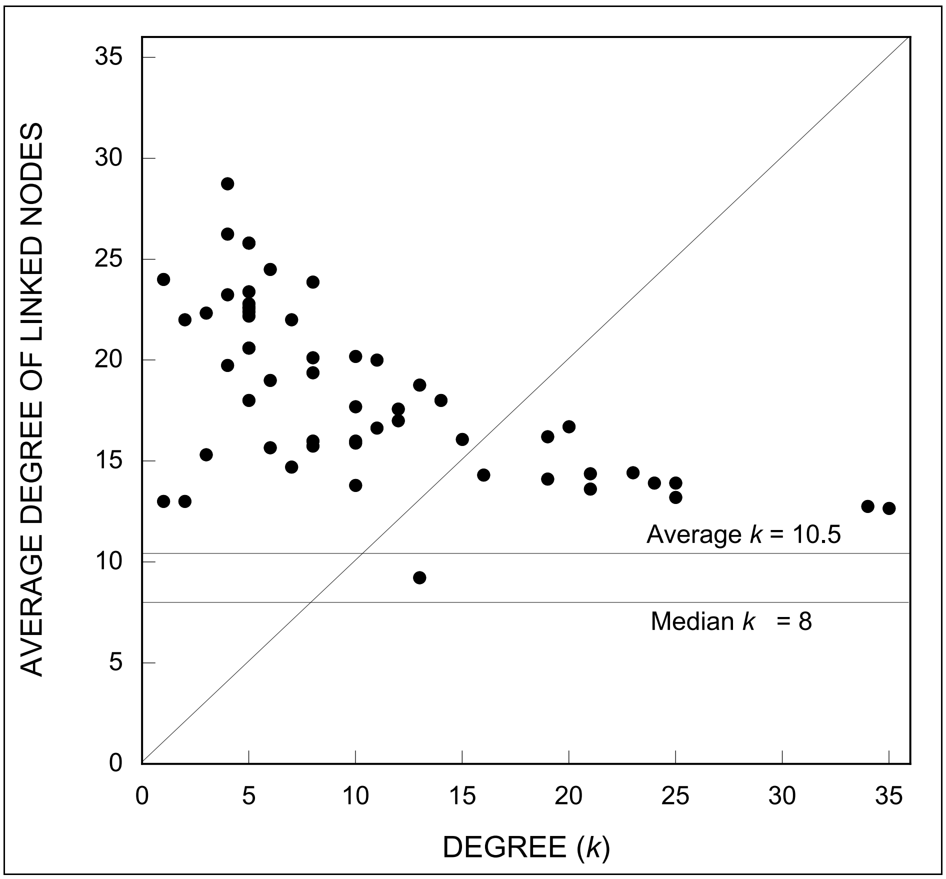


Figure 3. Average degree of first neighbors as a function of node degree.

Vulnerability of the Network

This evidence of preferential attachment, together with the possibility that further growth might produce a scale-free structure, raises the question of how vulnerable the SWAN or other network with similar structure would be to selective attack on its most highly connected nodes. In fact, airline networks are frequently cited as prime examples of the peculiar resistance to failure and vulnerability to attack characteristic of scale free networks. In the words of a leading researcher, the vulnerability of the Internet arises "because there are a couple of very big nodes and all messages are going through them... if someone maliciously takes down the biggest nodes you can harm the system in incredible ways. You can very easily destroy the function of the Internet." Airline networks have "exactly the [same] situation [as] on the Internet: there are a couple of hubs that are crucial to the system."[10] In the complex network literature (see footnote 3), removal of a relatively small fraction of the highest-degree nodes from a scale-free network resulted in a dramatic loss of connectivity as measured by the size of the largest surviving connected component. This fragmentation of the network occurs abruptly at a critical value of the fraction of nodes removed. This literature reported on three scale free networks: a model generated by growth and preferential attachment, the Internet, and the World Wide Web, and the critical fractions were found to be roughly 18%, 3%, and 7%, respectively. In contrast, the SWAN exhibits significantly less vulnerability to attack.

Figure 4 shows the fraction of nodes remaining in the largest component of the SWAN as nodes are deleted in order of their degree in the original network. (It would be possible to delete nodes in order of their degree in the *degraded* network, but the differences are insignificant in the present case.) Not until more than 25% of the nodes are removed does the SWAN begin to lose its connectivity, breaking into two components, one roughly three times larger than the other. Even then, the largest surviving component contains 34% of the original nodes. This is in striking contrast to the critical fractions reported in the literature (Footnote 3), which it should be remembered represent removal fractions which produce essentially complete fragmentation of the network.

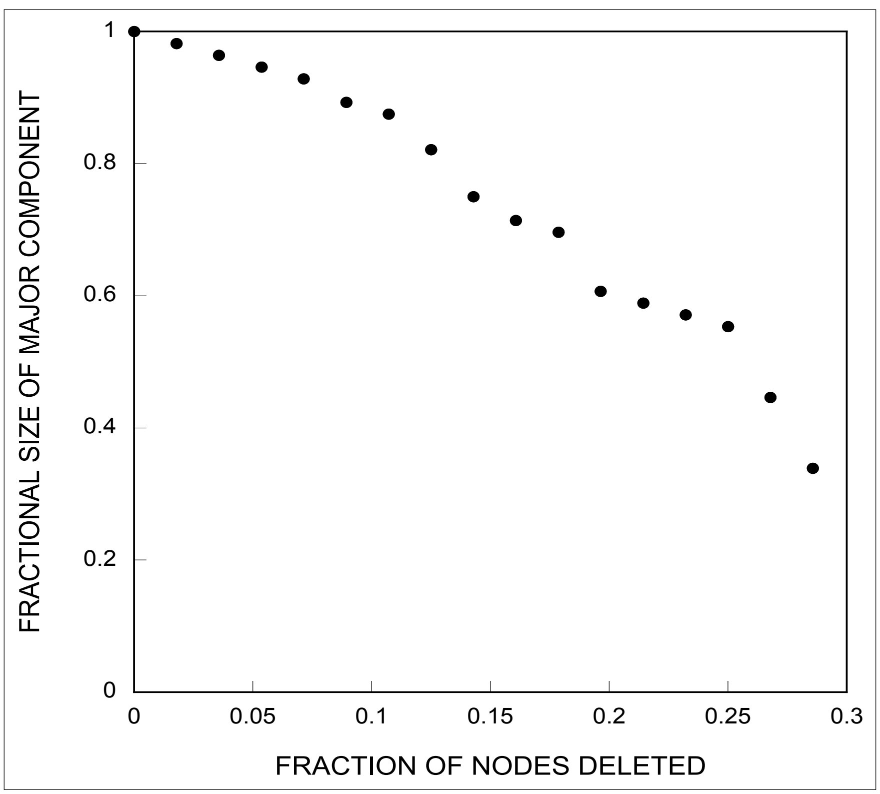


Figure 4. Response of the Southwest Airlines network to removal of high-degree nodes ("attack").

One source of this resistance to attack can be found by examining the adjacency matrix of the network. The rows and columns of the adjacency matrix are labeled by the network nodes, and the matrix contains a one where a link exists between the relevant pair of nodes and a zero otherwise. Figure 5 is a pictorial representation of the adjacency matrix of the SWAN, where ones have been replaced by solid black squares and zeros by white ones. The nodes have been arranged in order of degree, decreasing from left to right and top to bottom. The result shows clearly that the network structure is not strictly hub-and-spoke but rather core-and-periphery.[11] The central "hub" is actually a fully connected component, or clique, consisting of the six nodes of highest degree (LAS, PHX, MDW, BNA, HOU, and BWI) plus the 9th-ranked node, MCI. There are in fact eight other seven-member cliques within the core, involving 16 cities, including all ten of the highest-degree nodes. The exact definitions of the core and the periphery are subject to interpretation, but even by the most restrictive definition[12] almost 40% of the nodes lie in the periphery.

Figure 5. Graphical representation of the Southwest Airlines network adjacency matrix, sorted by degree.

Inspection of Figure 5 suggests that a more flexible definition would place between 20% and 30% of the nodes in the densely connected core and the remainder in the periphery. The results of Figure 4 could then be explained, at least qualitatively, in terms of the fact that since the core is almost fully connected it must be nearly completely destroyed before the connectivity of the network is threatened. Individual nodes become disconnected, but a single major component persists until 16 (29%) of the nodes have been removed.

Origin and Evolution of SWAN Network Structure

Without access to detailed, possibly sensitive planning information from Southwest Airlines, it is possible only to speculate on the origin of the observed structure of the SWAN. Clearly, the evolution of the route network was subject to economic and logistical constraints that cannot be captured in a simple graph-theoretical analysis in which all nodes and links are of equal significance. While robustness to failure of critical (high-degree) hubs may well have been a factor in creating many links among the high-degree nodes, there is another, less obvious consideration. An airline network is very different from networks such as the Internet where the value of a connection is nearly independent of the number of edges traversed. Routes of length greater than two are of very limited value. The Southwest schedule lists a number of two- and even three-stop flights, but these cannot be very popular with their passengers. In adding a new city to the network, it is clearly desirable to provide a large number of relatively short connections. Since the links are bidirectional, this not only gives customers in the new city a wide choice of destinations, it also makes the new city accessible to many others on the network. It is realistic to consider a connection "short" if it involves no more than one stop. Using that definition, Figure 6 shows the number of destinations that can be reached by short connections from a node of given degree. Once a city has direct connections to at least three others ($k = 3$) it can reach (and be reached from) at least half the network by non-stop or one-stop flights. At $k = 5$ this rises to about 80%, and somewhere between five and ten direct connections gives a city access to essentially the entire network. The significance of the peak in the degree distribution at $k = 5$ may be related to this behavior, but distinguishing between cause and effect will require further analysis.

Having an adequate number of links to the network may not only increase the number of short connections available but also reduce the need for long (multi-hop) routes. All of the 21 city pairs connected by routes of length four (three stops) involve just two airports, Houston Intercontinental (IAH) and Orange County (SNA). Significantly, these two airports have only one (IAH) or two (SNA) non-stop connections to the network.

At this point we might note that when service to Albany International Airport (ALB) was introduced on 7 May 2000, non-stop service was provided to three cities: Baltimore-Washington (BWI), Orlando (MCO), and Las Vegas (LAS). The average degree of these three nodes is 26, and this allowed Southwest to schedule direct or connecting service[13] to 31 additional cities, for a total of 33 short connections, in good agreement with the trend shown in Figure 6. When service was introduced to Buffalo Niagara International Airport (BUF) on 8 October 2000, the service included four non-stop connections to nodes with an average degree of 28, generating 27 one-stop connections for a total of 31 short connections, again in good agreement with Figure 6.

Finally, it is possible to think of the network growth shown in Figure 6 and the attack depicted in Figure 4 as inverse processes. Since newly added nodes require a minimum number of links to become well connected to the network, it might be reasonable to expect that the nodes that become disconnected during an attack are those with low initial k-values. This turns out to be essentially, but not completely true. Of the 16 isolated nodes that become disconnected during the attack of Figure 4, all come from the lower half of the degree distribution. The average initial k-value of the disconnected nodes is 4.1. On the other hand, two nodes with initial values of $k = 2$ remain connected to one of the surviving components, as do four of the six nodes of lowest degree. Two preliminary conclusions can be drawn. The good correspondence between the value of k needed to establish many short connections and the value that places a node at risk during an attack reflects the selectivity of the attack and the preferential nature of the attachment process.

In contrast, the survivability of very low-degree nodes may depend on specific details of the attack and of their connection to the network. Since the network core is virtually destroyed in the attack, it may be advantageous for a low-degree node to attach to nodes of intermediate degree at the edge of the core rather than to the highest-degree nodes. There is some evidence visible in Figure 5 that this is the case in the SWAN. The result is a trade-off between having short connections when the network is intact and the risk of disconnection if multiple hubs are lost in the core.

Conclusion

There remain important questions to be answered concerning the structure and evolution of the SWAN. A key issue is whether the growth mechanism involves preferential attachment in a way that would eventually lead to a power-law tail in the degree distribution and whether this would affect the resistance to attack described here. Understanding the growth process will almost certainly require some consideration of the cost and value of establishing particular links, making the results more directly relevant to practical network management problems. It might even be necessary to consider costs and benefits not directly attributable to particular nodes or links, such as the centralization or decentralization of maintenance or administrative facilities. Parameters such as network diameter or average path length could be used to measure the effect of attack and compared with the component size measure used here. Finally, the core-periphery structure of the SWAN is clearly a key to its resistance to attack, but the exact structure and behavior of the many interlocking cliques that compose the core-like region of the SWAN have yet to be explored.

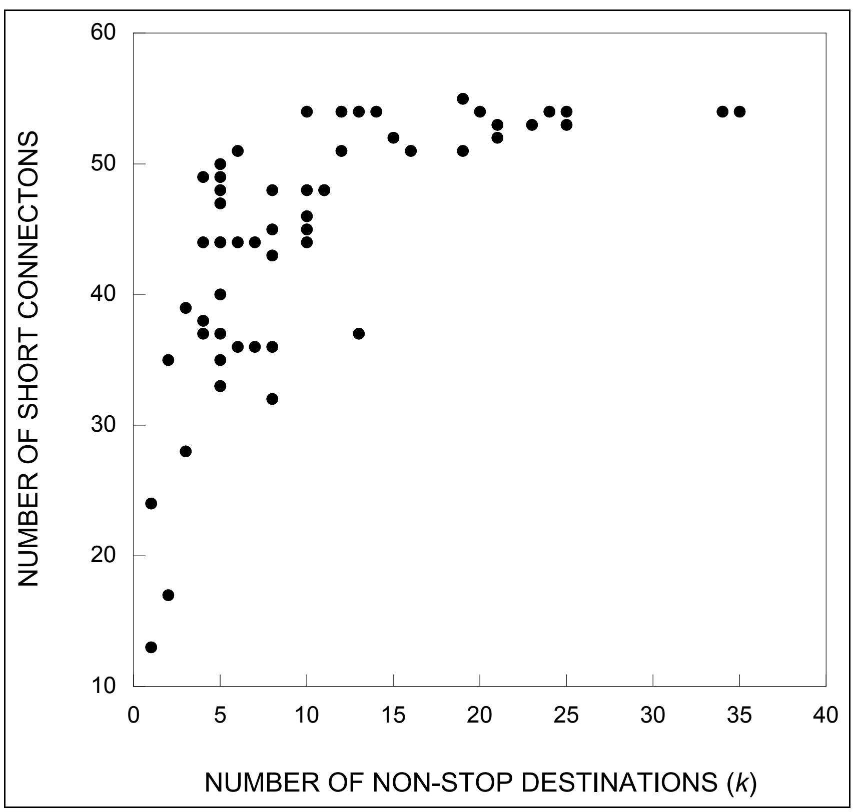


Figure 6. Number of destinations reached by short (non- or one-stop) flights from nodes of a given degree

The focus of this study has been on the structure and resistance to attack of a small, real-world network. This is not entirely satisfactory from a theoretical point of view, since the conclusions may lack generality and clear connection to some of the powerful ideas emerging from recent studies. On the other hand, in approaching the development of logistics or communications networks for military applications, especially small *ad-hoc* or expeditionary networks, it is very valuable to have examples that perform well in the real world and illustrate some of the design requirements that we will need to satisfy. In particular, it is reassuring to have examined a case in which preferential attachment does not appear to produce vulnerability to attack. Preferential attachment appears to be an inherent process in systems that self-organize in response to local influences or to the inhomogeneous distribution of desired resources. It would be unfortunate if we were forced to avoid it completely in order to reduce vulnerability. In particular, control of the degree distribution of a network by imposition of a hierarchical structure would run exactly counter to the assumptions underlying most discussions of network-centric operations. The "universality" of scale-free networks and the widely-discussed results demonstrating robustness to failure and vulnerability to attack in such networks have led some to conclude that this "robust yet fragile" behavior is to be expected in virtually any network structure allowed to evolve under conditions promoting selective attachment of new nodes. The results presented here for the Southwest Airlines route network suggest that this may not be the case and offer hope that rules for network construction and growth can be found that provide stability against both failure and attack.

---

[1] Cebrowski, A. K. and J. J. Garstka (1998). Network-Centric Warfare: Its Origin and Future. United States Naval Institute Proceedings. **124:** 28.

[2] See, for example, Albert, R. and A.-L. Barabási (2002). "Statistical mechanics of complex networks."Reviews of Modern Physics **74**(1): 47-97 and Newman, M. E. J. (2003). "The Structure and Function of Complex Networks." SIAM Review **45**(2): 167-256.

[3] Albert, R., H. Jeong and A.-L. Barabási (2000). "Error and attack tolerance in complex networks." Nature **406**: 378.

[4] Barabási, A.-L. and R. Albert (1999). "Emergence of Scaling in Random Networks." Science **286**: 509-512.

[5] M. I. Bell, Chief of Naval Operations Strategic Studies Group, Newport, RI, 8 Nov. 2000.

[6] http://www.southwest.com/

[7] See, for example, Trudeau, R. J. (1993). Introduction to Graph Theory. New York, Dover.

[8] Both Houston Intercontinental (IAH) and Houston Hobby (HOU) serve the Houston, TX area.

[9] Borgatti, S. P., M. G. Everett and L. C. Freeman (1999). UCINET 6.0 Version 1.00. Natick, Analytic Technologies.

[10] Reuters interview with Albert-Lázló Barábasi reported 26 July 2000, see http://archives.cnn.com/2000/TECH/computing/07/26/science.internet.reut/

[11] Borgatti, S. P. and M. G. Everett (1999). "Models of core/periphery structures." Social Networks **21**: 375–395.

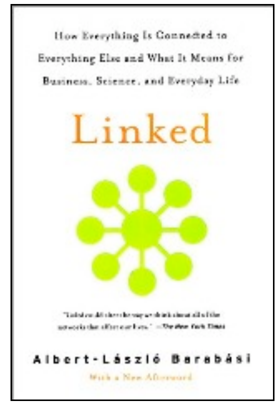
[12] The most narrow definition requires that the core be fully connected and that nodes in the periphery have connections only to nodes in the core.

[13] Direct service implies a one-stop flight with no change of aircraft or flight number. Connecting service requires a change. No distinction was made in this analysis.

BOOK REVIEW

David A. Jarvis

Albert-László Barabási
Linked: How everything is connected to everything else and what it means for business, science, and everyday life
New York: Plume, 2003.
294pp. $14.00
ISBN 0-452-28439-2
(Paperback edition)



Networks are everywhere. *Linked* attempts to explain where to find them, why they are important, and how it is that so many of them have similar characteristics. A network can be defined as a large collection of interconnected parts (nodes and links) arranged for a purpose. Barabási finds these networks everywhere: from protein interactions in cells to the Internet and World Wide Web to economies, terrorist groups, airline routes and the spread of diseases. It is a convincing read that uses a plethora of real-world examples to illustrate fairly complicated mathematical principles that have been advanced over the last decade. *Linked* was one of a number of books that were published in the late nineties and first few years of the new century that dealt with the emerging scientific discipline of complex networks and complexity theory. These popular books included *Small Worlds* (1999) and *Six Degrees* (2003) by Duncan Watts, *Nexus* (2002) by Mark Buchanan and *Emergence* (2002) by Steven Johnson.

The author of *Linked*, Albert-László Barabási, is the Emil T. Hofman Professor of Physics at the University of Notre Dame. A native of Transylvania, this is Barabási's first work of popular scientific literature. When *Linked* was first released, it received a substantial amount of press and was named one of the best business books of 2002 by *strategy+business* magazine. However, as with any popular science book, the difficulty lies in balancing technical information with easily understandable examples that can transform the technical principles into something that can be understood by a broad audience. Barabási's credentials are unquestioned and he has been instrumental in creating part of the foundation for complex network theory. The book does not run short of examples and there is enough technical material for a those readers who have a scientific background but are unfamiliar with the topic. However, it does lack specific applications of the principles. His theories can describe why complex networks work the way they work, but what does that mean? This is a problem with the field in general and it is up to the next generation of researchers to begin applying the principles more practically. The field is not mature enough to be passed from the scientist to the engineer quite yet.

The first few chapters of the book have Barabási tracing the history of network theory from Euler's famous seven bridges of Königsberg problem from 1736 to the present day. Through Euler's answer to the bridges problem the branch of mathematics known as graph theory was created, the precursor to network theory. Barabási states that what this simple problem taught us is that, "The construction and structure of graphs or networks is the key to understanding the complex world around us." Analyzing network topology is the first step in decoding complex networks. He goes on to explore the work of Erdös and Rényi (random network theory), Milgram (six degrees of separation), Granovetter (strength of weak ties in networks), and Watts and Strogatz (small world networks).

One of the key contributions that Barabási has made to the field of complex networks is that, with the help one of his collaborators Hawoong Jeong, he determined that the World Wide Web is a scale-free network. What this means is that there is a very few nodes in the Web that have a majority of the links (these nodes are known as hubs). The hubs on the Web are a select group of websites that a large number of other websites link to (e.g. Google, Yahoo). This same fundamental structure was evident in many of the other networks that they researched. This discovery led Barabási to write that hubs "determine the structural stability, dynamic behavior, robustness, and error and attack tolerance of real networks." He goes on to discuss how networks evolve and grow through preferential attachment, how the robustness and vulnerability of networks can be determined, how viruses and fads spread on networks, and the application of his research to genomes, protein interactions and economics. Each topic builds upon the prior one, evolving, not unlike a network.

For a military audience involved with "Network-Centric Warfare" or more generally, command and control, this should be one of the first books that are read. The lessons that Barabási highlights from the 1997 National Security Agency war game "Operation Eligible Receiver", where coordinated groups of hackers proved that they could take down military and other communication systems fairly easily, should serve as a wake-up call to the importance of complex networks in defense systems. This book is the perfect primer and lays the foundation for how future military systems should be designed, defended and operated.

Barabási's examples run the gamut, from how Paul spread Christianity to the proliferation of Windows and the spread of AIDS. If you aren't careful, by reading this book you might start developing the opinion that networks *are* truly everywhere. Some people may take the concepts in the book too lightly, thinking *Linked* is just another novel science/business book. They might find the network similarities very interesting and quaint, but more a curiosity than anything else. There will be others that ask how they can apply any of this to what they are doing? The point of Barabási's book, however, is not how to apply complex network theory to problems. He is really advocating a different mindset in approaching complex challenges. This mindset is a move away from reductionism and towards holistic views of systems and a greater emphasis on multi-disciplinary research.

Note: For a more technical view of the principles introduced in *Linked*, see Barabási's and Réka Albert's paper "Statistical mechanics of complex networks" (Reviews of Modern Physics, Volume 74, January 2002).