United States Military Academy

The Network Science Center

Network Science Report

Vol. 1 No. 1 http://http://www.netscience.usma.edu

In this issue:

From The April Workshop

Network Science at the United States Military Academy

NS Notes

Introducing the Network Science Report, *Robin Burk* 1
Commander's Comments, *COL Eugene Ressler* 2
From the Director, *Dr. John James (COL USA Ret)* 3
Network Science Research at USMA, *Dr. Frederick I. Moxley* 4

From the April Workshop

A Contextual Multi-theoretical Multi-level (MTML) Model of Network Dynamics, *Contractor* 5
It's Ecological, Not Pathological: Mathematical Models of Counterinsurgency, *Drapeau, Hurley & Armstrong* 8
Tools for Automated Analysis of Networked Verbal Communication, *Foltz, Lavoie, Oberbreckling & Rosenstein* 19
Social Network Monitoring of Al-Qaeda, *McCulloh, Carley & Webb* 25
Information Sources for Improved Social Relationship Discovery, *O'May and Forester* 31

Undergraduate Research

A Methodology for Simulating Net-Centric Technologies: An Operations Research Approach, *Lospinosa* ... 35

Links and Upcoming Events 43

Recommended Reading 44

ISBN 978-1-934808-00-9 October 2007

The Network Science Report is a publication of the United States Military Academy's Network Science Center and is made possible by the support of the Director of Research within the Office of the Assistant Secretary of Defense for Networks and Information Integration. Publication of the USMA-ARI Workshop papers is supported by the Army Research Institute.

The views expressed in this report are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

Address correspondence to:

The Network Science Report
Network Science Center
607 Cullum Road
United States Military Academy
West Point, NY 10996

Volume 1 Number 1: ISBN-13: 978-1-934808-00-9
ISBN-10: 1-934808-00-8

Introducing the Network Science Report

Ms. Robin Burk, Editor

Welcome to the first issue of the Network Science Report. The Report is the first publication to come out of the new Center for Network Science at the U.S. Military Academy (USMA).

This issue of the Report introduces our Center to what we hope will be a growing community of interest for the emerging discipline of network science. The National Research Council's 2006 report challenged the Army to take a leading role in fostering this new discipline — and USMA has stepped up to that challenge.

As COL Ressler and Dr. James note, the Center has both internal and external goals. Internally, we are introducing network science topics into our curriculum and supporting network science-related research by faculty and students across all of the affiliated academic departments at the Academy. Externally, we are working with Army and DOD research proponents on a number of initiatives including specific research projects, invitational workshops and more.

Network science efforts are far from being limited to USMA. Military commanders, law enforcement agencies and public health officials are interested in network science. So too are researchers who bring skills in a wide range of domains where networked systems play a key role. Social, cognitive, information, communications, biological …. networks are all around us. Understanding the underlying principles that shape their creation, growth and behavior is an exciting intellectual challenge.

It's also one that has important applications to pressing needs today.

We hope the Report and other Center initiatives will contribute to the scholarly and practitioner discussion as the network science community coalesces. One way in which the Report can support that goal is by offering a place for shared dialogue among those already active in the discipline, along with an accessible place to start for those who are new to it. This issue begins that dialogue by offering several papers that were presented at our first invitational workshop last April.

Co-sponsored by the Army Research Institute, the April workshop addressed network science as applied to full spectrum military operations. The selected papers included here offer theoretical perspective, mathematical models, tools and an analysis of information sources in that domain. USMA faculty were among those who presented papers at the workshop, but in this first issue we've primarily focused on contributions from the wider network science community.

The Network Science Center is, as with all of our activities at USMA, intimately associated with the development of cadets as they grow to become Army leaders. In this issue we spotlight research done by Cadet Joshua Lospinosa. Currently a junior, he was a sophomore when he performed the research and wrote the award-winning paper we've included here. Cadet Peyton Hurley co-authored another of our papers during an internship with Rand Corporation and then-Cadet (now 2LT) Matthew Webb co-authored a third paper in this issue.

I'd like to invite each of our readers to consider contributing to future issues of the Report. Papers, short research descriptions, student activities, book reviews and network science news are welcome, as are letters to the editor. Let us know of activities, web sites and other information of interest to the wider network science community. These, and other comments, can be directed to me at the address below.

Network Science Center
Dept of EE&CS
US Military Academy
West Point, NY 10996
robin.burk@usma.edu

ISBN 978-1-934808-00-9

COMMANDER'S COMMENTS

COL Eugene Ressler

Head, Department of Electrical Engineering & Computer Science

Network Science: a visionary idea

That term - visionary idea - is badly overused. In some settings, it's just hyperbole for sound but unremarkable reasoning. In others, it's a euphemism for catchy marketing. Then again, "visionary" and "illusory" are near neighbors. With apologies to Samuel Johnson, the road to hell is probably paved with visionary ideas that really weren't.

Network Science, however, has none of these failings. Rather, it is a leap ahead, a badly needed fresh approach to the gaps and barriers that exist among current scientific discplines, where extremely important problems are lurking to be solved. It is founded on valid needs of our Army and modern society.

Moreover, the shared goals that are emerging from the nascent Network Science community are achievable, with good prospects for positive returns on investment within a reasonable period of time.

These returns are likely to include new ways to make soldiers safe and effective on the battlefield, to improve leadership and decisions at all levels of the military, government, and business, and to advance modern societies through fundamentally improved understanding of the world

Our Center for Network Science embraces these possibilities. No one is in a better position to advance Network Science and its application than Army leaders. We want cadets and faculty at the U.S. Military Academy to appreciate the possibilities and help make them real. And we will do that, not only within the Academy, but in cooperation with researchers and practitioners from other organizations as well.

Our intent is to contribute by fostering both the science itself and the community of enthusiastic people who share our goals. It's an inspiring challenge - one we accept with great anticipation.

The Department of Electrical Engineering & Computer Science hosts the Network Science Center at the U.S. Military Academy (USMA) . COL Ressler is a computer scientist who earned his PhD from Cornell University. His research interests include neural networks for image processing.

The Center has active participation from other academic departments and (as several papers in this issue demonstrate) draws on faculty and cadet research across many domains. Future issues of the Report will feature comments from leaders of the other USMA academic departments associated with the Center:

Department of Behavioral Sciences and Leadership

Department of Chemistry and Life Sciences

Department of Civil and Mechanical Engineering

Department of Mathematical Science

Department of Physics

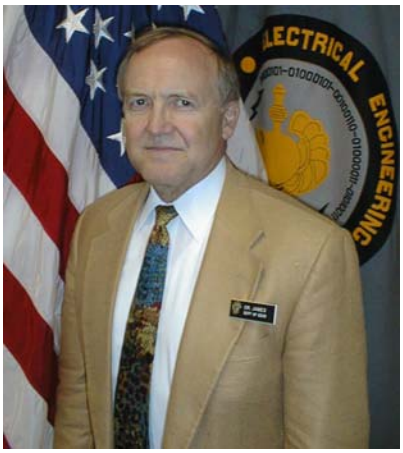
Department of Social Sciences

Department of Systems Engineering

FROM THE DIRECTOR

The Network Science Center

Dr. John James, Acting Director, USMA Network Science Center



A number of years ago a very successful scientist who also investigated solving military technical challenges related to me his conviction that "solving hard problems requires good science." The different academic, business, and government sponsors of network science research are certainly in the condition of having many hard problems to solve!

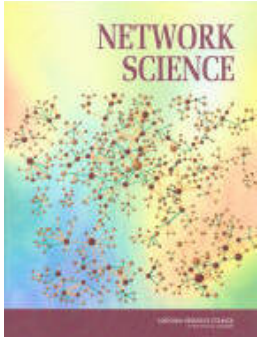
The set of United States Military Academy (USMA) academic departments which have come together the create the USMA Center for Network Science are focused on expanding the scientific base which will assist the Army in addressing the technical shortfalls in executing Net-Centric Operations.

The Army and Department of Defense sponsors of our local efforts have been very open in their intent to enable creation of a Network Science community which may be able to achieve cross-disciplinary results which will assist in addressing not only Army technical needs but also the nation at large.

We look forward to exposing the cadets and faculty to the new horizons being discussed by Network Science practitioners and to support those cadet and faculty educational endeavors which will add to the Network Science body of knowledge.

— John

Why a Network Science Center at USMA?



In 2006 the National Research Council of the National Academies of Science issued a report urging the Army to foster research into networked phenomena and the principles that underlie their behavior and growth.

From the preface to that report:

This study was an exercise in coping with complexity. The subject matter is complex. Important networks like the Internet and the power grid are becoming ever larger, encompassing up to hundreds of millions if not billions of nodes. They exhibit complex and often dynamic patterns of links between the nodes. Networks interact with one another and are recursive.

Social networks are built upon information networks which are built upon communications networks which in turn are built on physical networks. Moreover, this layered structure of interacting networks built on top of other networks is reflected directly in the diversity of communities that study networks: sociologists, management theorists, warfare strategists, economists, biologists, chemists, physicists, and a wide variety of engineers . . .

Networks lie at the core of the economic, political, and social fabric of the 21st century. The demand for structured knowledge that can be used to design, procure, and operate networks is ubiquitous and growing rapidly.

Moreover, social and communications networks lie at the core of both conventional military operations and the war on terrorism. Thus, ***investment in network science is both a strategic and urgent national priority****.*

Network Science. Committee on Network Science for Future Army Applications, National Research Council. ISBN: 0-309-65388-6.

FROM THE RESEARCH DIRECTOR

Network Science — A Field Whose Time Has Come

Dr. Frederick I. Moxley, Director of Research and Deputy Director

Some scholars indicate that the study of networks first began during the 18th century when the mathematical language known as graph theory came into being. Based on discrete mathematics, graph theory is used to describe the properties of diverse linkages and pathways - what we now refer to as *networks*.

It wasn't until the mid-20th century however, that graph theory spread to disciplines beyond the scope of pure mathematics. Used primarily for modeling purposes, it soon became apparent that graph theory could also be used as a tool for the analysis of empirical data. As a result, it eventually took hold across several fields of scientific endeavor. Most notable among these were the social sciences.

Graph theory is still in use today and is considered a viable tool when describing probability distributions. Even so, it has been noted that graph theory often falls short when applied to real-world concerns. In particular, it is limited in its ability to deal with both theoretical and empirical questions, presumes that networks are static, and does not provide the basis in which to comprehend their behavior. In other words, graph theory alone is incomplete and the existing void still needs to be addressed.

Military strategists have taken note of this gap and have indicated that the current fundamental knowledge about networks is primitive and that their behavior is not reliably predictable. Furthermore, what we need to know about networks to better benefit our society from an innovative and economically based perspective is insufficient.

To address these shortcomings, an interdisciplinary approach is necessary. One in which the framework to enhance our collective knowledge can be built. This requires a thorough examination of the field and the processes that presently exist in order to determine how we may expand our current perspectives regarding networks – in essence, a field that focuses on and proliferates research as it pertains to the establishment of a network *science*.

The resulting framework would help to fill the void that presently exists by enabling the practitioner with viable approaches and methodologies that are based on sound theoretical principles.

In support of the Defense Department's current Network-Centric paradigm, it is anticipated that the field of network science will be of great strategic and national interest. As a result, the U.S. Army has taken the lead in this area by first recognizing the need for an interdisciplinary field pertaining to Network Science, and secondly through its establishment of a Center for Network Science at the United States Military Academy.

The Army intends to further its stance in this area by consistently developing and enhancing its foundation curricula, as well as promoting the research that will aide in producing the interdisciplinary tools, applications and methodologies that are necessary to validate the net-centric concept DoD-wide and beyond.

The establishment of the Network Science Center at the United States Military Academy is a major step along this path and is leading the way in which we are educating and preparing America's future leaders.

As seen in the following articles and associated cadet projects, we are not only privy to efforts submitted by some of the worlds leading experts, but also the remarkable accomplishments and efforts put forth by future Network Scientists at the undergraduate level!

GO ARMY!

A Contextual Multi-theoretical Multi-level (MTML) Model of Network Dynamics

Noshir Contractor

ABSTRACT

This paper extends the multi-theoretical multi-level (MTML) model to study the creation, maintenance and dissolution of communication and knowledge networks. It begins by identifying the theoretical mechanisms that influence the dynamics of communication and knowledge networks in general. Next it proposes a contextual meta-theory to explain why actors' motivations are better explained by some sub-set of these theories depending on the goals of the community. The goals of a community could include exploring, exploiting, mobilizing, bonding or swarming. Finally, the paper provides an empirical illustration to illustrate how hypotheses derived from this contextually driven meta-theory can be tested using the networks of individuals playing the Massively Multiplayer Online (MMO) role playing game World of Warcraft.

OVERVIEW

To date, most network research has been limited by five major problems. First, it tends to be atheoretical, ignoring the various social theories that contain network implications. Second, it explores single levels of analysis rather than the multiple levels out of which most networks are comprised. Third, network analysis has employed limited theoretical insights from contemporary complex systems analysis and computer simulations. Fourth, it typically uses descriptive rather than inferential statistics, thus robbing it of the ability to make theoretical claims about the larger universe of networks. Finally, almost all the research is static and cross-sectional rather than dynamic. we propose solutions to all five problems (Monge & Contractor, 2003; Contractor, Wasserman & Faust, 2006). First, we have developed a multi-theoretical model that relates different social theories with different network properties. Second, our model is multi-level, offering a network decomposition that applies pertinent social theories at all network levels: individuals, dyads, triples, groups, and the entire network. Third, our model relies on a complex systems perspective, implementing *Blanche*, an agent-based network computer simulation environment, to generate and test theories and hypotheses. Fourth, our model utilizes the Exponential Random Graph Models (ERGM)/*p** family, a set of innovative tools for statistical network analysis, to provide a basis for valid multilevel statistical inferences. Finally, our model relates communication networks to other networks, enabling more sophisticated study of how dynamic organizational networks emerge.

This paper extends our theoretical framework by positing that not all theoretical arguments are equally influential in explaining the emergency of networks in all cases. Instead, we posit that the goals of the community will influence the motivations individuals use to create, maintain, and dissolve their network ties. Based on our current theoretical and empirical research, we have identified five such goals:

Exploration: This describes situations where the community is particularly interested in exploring new ideas and resources. These could be the case, for instance, when communities prioritize the quest for disruptive innovations.

Exploitation: In this case a community is more interested in exploiting existing resources and ideas within the network for efficiently rather than exploring new ideas into the network. This is often the case when a community seeks "incremental" rather than "disruptive" innovations.

Mobilizing: In some cases, the focus of a community is not exploring or exploiting existing resources but to mobilize for new resources or standards. Examples would include lobbying on behalf of a collective interest or agreeing to new technical standards and protocols.

Bonding: In many cases the focus of a community is simply to build social support and trust. This process of bonding is often an end in itself but is also a means towards other ends.

Swarming: Finally, there are instances where the goal of a community is to be prepared as a latent network that coalesces into action (or "swarms") at very short notice and after accomplishing their task returns to a latent state.

These goals are by no means mutually exclusive, nor are they exhaustive. Instead, they represent a starting point for the development of a meta-theory that provides a more sophisticated and refined understanding of how the goals of a community might shape the motivations individuals have to create, maintain, and dissolve network links. The table below demonstrates how these goals map onto the various multi-theoretical multilevel motivations.

	Exploring	Exploiting	Mobilizing	Bonding	Swarming
Theories of Self-Interest	+		--		
Theories of Collective Action		+	+		+
Theories of Cognition	+	+			+
Theories of Balance	--		+	+	
Theories of Exchange		+		+	
Theories of Contagion	+		+		
Theories of Homophily	--			+	
Theories of Proximity	--			+	+

As shown in this table, communities that are interested in exploring new ideas and resources, the motivations are explained by Theories of Self Interest (where they choose links that maximize their self interest), Theories of Cognition (where they are driven to create links with people who have expertise in the areas they are interested in developing expertise), and by Theories of Contagion where they create links with those who are already well connected with others. On the other hand, their motivations are less likely to be explained by Theories of Balance (talking with friends of your friends are not likely to yield many novel non-redundant ideas), Theories of homophily (you are not likely to learn many new things from networking with people who are similar to you), or Theories of Proximity (you are less likely to learn about new ideas and resources from people proximate to you than those who are at a distance and thus exposed to different information sources.

We illustrate the utility of this approach by investigating the multi-theoretical multi-level motivations for the creation of network links in one community – World of Warcraft. World of Warcraft (or WoW) is by far the largest Massively Multiplayer Online (MMO) role-playing game that has over 7 million players world wide. In this game members belong to guilds and develop a wide variety of skills necessary in engaging in warcraft (making weapons, developing healing potions, etc.). Members of the WoW community are primarily interested in carrying out or responding to a "Quest" (a rapid response attack). However an important motivation for the community is to build community and trust in the process. Hence, we posit that the goals of this community are: exploiting resources (necessary for a quest), bonding (to build trust among members within the guild), and the ability for swarming (the agility to coalesce rapidly. Based on the table above, we posited the following hypotheses:

1. *Social Exchange Theory*: Individuals are more likely to reciprocate communication ties with those who have created ties with them previously.
Reciprocity/Mutuality

2. *Balance Theory*: Individuals are more likely to create ties with people their contacts communicate with.
a. Increase Balance
Reduce Actors at Distance Two

Cognitive theories: Individuals are more likely to create ties with people who they perceive to be experts

Data were collected from all 184 individuals who belonged to 16 guilds at 3 points in time. 21.7% of the participants were female. The ethnic composition was Caucasian (79.3%), Asian/ Pacific Islander (15.2%), African American (2.2%), Hispanic/Latino (1.1%), and Native American (1.1%)

We asked the question *"How often do you ask <guildmember> for WoW advice or information about ..... Your Character's Class?"* We used SIENA - *Simulation Investigation for Empirical Network Analysis for the* Statistical estimation of models for longitudinal social networks according to the dynamic, actor-oriented model of Snijders (2005).

We found that there was a baseline cost for creating a WoW link with a random member of the network. However, this cost was mitigated by benefits that were derived from motivations consistent with theories of social exchange, balance, and cognition. Specifically we found that the cost-benefit for creating a link in this network was given by the following equation:

-1.08 (cost of creating a link)
+ 0.29 (benefit of reciprocating) [Social Exchange]
+ 3.07 (benefit for being a friend of a friend) [Balance theory]

+ 0.04 (benefit of connecting to an expert) [Theories of Cognition]

This illustration shows the empirical viability of extending the MTML approach initially proposed (Contractor, Wasserman, & Faust, 2006; Monge & Contractor, 2003) by developing a contextually driven meta-theory for explicating how the goals of a community influence which theoretical motivations might be more influential in a given context. While this empirical illustration applies to individual actors, the theoretical and empirical approaches discussed here are equally applicable to networks where actors might be groups, organizations, nation-states, or non-human agents such as knowledge repositories.

AUTHOR

Noshir Contractor is the Jane S. & William J. White Professor of Behavioral Sciences at Northwestern University, where he also holds professorships in Industrial Engineering & Management Science (McCormick School of Engineering), Communications Study (School of Communications), and Management & Organizations (Kellogg School of Management). He is also the Director of the Science of Networks in Communities (SONIC) Research Laboratory, an affiliate of the National Center for Supercomputing Applications, University of Illinois at Urbana Champaign.

QUOTES WORTH PONDERING

"Problems worthy of attack prove
their worth by fighting back."
— Paul Erdos (1913-1996)

"It is not enough to do your best:
You must know what to do,
And then do your best."
— W. Edwards Demming

Knowledge, then, is a
system of transformations
that become progressively adequate.
— Jean Piaget

All truths are easy to understand
once they are discovered.
The point is to discover them.
— Galileo Galilei

Mathematicians stand
on each others shoulders.
— Carl Friedrich Gauss

It's Ecological, not Pathological: Mathematical Models of Counterinsurgency

Mark D. Drapeau, Peyton Hurley and Robert E. Armstrong

ABSTRACT

The climate of conflict during the early 21st century has lent itself to a reexamination of techniques and tactics used in counterinsurgency [1]. The complexity inherent to warfare and other complex systems and networks can be modeled in similar ways. The interaction of competing and cooperating groups having differing goals, tendencies, and talents lends itself to mathematical analyses, which often result in predictions of ways to perturb systems to reach desired outcomes. These predictions are occasionally unintuitive.

The field of network science is defined by the idea that there are general, cross-disciplinary "laws" of networks and complex systems. Here, we apply this to explore the notion that ecological modeling of species interactions might approximate the interactions found in counterinsurgency. First, we found that relatively simple models of predation, parasitism, and mutualism were inappropriate because of over-simplicity, violation of critical assumptions, or both. Second, we discovered that models of interspecific competition for resources approximated the struggle between insurgents and counterinsurgents for military and political control over a host nation's population. Third, this set of models implies that various aspects of a counterinsurgency campaign – fighting insurgents, controlling crime, and winning popular support – are probably and perhaps favorably inseparable.

This paper represents a theoretical thought experiment about using biological models and metaphors for predictive purposes in warfare. It is important to note that modeling of this sort can only provide insight – not answers. Using the initial framework outlined here, more extensive analysis, modeling, and simulation could be used to derive historical insights about past COIN campaigns and aid in planning future ones.

Biology as a Mindset

Biology is more than a laboratory science; it is a way of thinking about the natural world. Biological metaphors provide powerful ideas about how the natural world functions, and many parallels between natural and man-made systems have been drawn in technical, policy, and popular literature [2]. Within the field of network science, one powerful idea is that there may be general "laws" of networks. Therefore, the study of one type of network might bear fundamentally on one which seems superficially different.

Within the field of military and war studies, biological metaphors are often used to convey powerful ideas about human behavior. For example, a very influential recent article by David Kilcullen uses the terms "adaptation," "evolution," "competition," "ecosystem," and "environment" to describe various things occurring during a counterinsurgency (COIN) campaign [3]. Notably, these words are all from the same subspecialty of biology.

The study of this subspecialty – commonly called ecology, evolution, and animal behavior or "EEB" – is more than merely observational. It is also mathematical and can sometimes be predictive. In practice, empirical and theoretical work is often performed simultaneously by one or more investigators in order to shine greater light on nature's mysteries. Depending which comes first, experiments can be performed to test models, or new data can be used to inform new mathematical theory. This quantitative approach has been highly successful since the beginning of modern biology a century ago and continues in cutting-edge fields such as bioinformatics and genomics.

The similarities between biological ideas and observations of warfare raise the question: Might mathematical models of biological processes be useful for understanding – and perhaps predicting – certain aspects of warfare? Here, we investigate whether a number of ecological models might be relevant to the study and practice of COIN.

How the weak win wars

It has been posited that powerful modern nations – the U.S., the USSR, Great Britain, France – have only been beaten in battle or driven to stalemate via insurgent tactics. These include guerrilla warfare and terrorism, and typically have a large psychological operations (PSYOP) component. The general success of insurgencies warrants study. However, since the Vietnam era, relatively little intellec-

tual or academic work has been performed within military/defense circles [4].

What is "counterinsurgency"? What academics typically term COIN cannot exist without an initial insurgency; academics are typically on the side of the counterinsurgency. Generally speaking, COIN involves a rebellion ("R" – the insurgents) against an authority ("A" -- the counterinsurgents) for control of a population ("P" – everyone else) [5]. The rebellion or the authority may be from the area of operations (AO) or from outside it (e.g., a NATO peacekeeping force).

The literature has various definitions of what insurgency and counterinsurgency are. Below are three modern definitions [6]:

> *"Counterinsurgency: those military, paramilitary, political, economic, psychological and civic actions undertaken by a government to defeat a subversive insurgency"*
>
> *"An insurgency is a struggle for power (over a political space) between a state (or occupying power) and one or more organized, popularly based internal challengers."*
>
> *"An insurgency is a struggle for control over a contested political space, between a state (or group of states or occupying powers), and one or more popularly based, non-state challengers."*

The first key point, in all three definitions, is that an Authority in the AO is defending its right to control a territory against a Rebellion. The Rebellion is implicitly assumed to be smaller and less powerful, else they would be the governing Authority. The second key point, in the second and third definitions, is that the Authority and Rebellion are fighting over *political space*, which includes control of the "hearts, minds, and acquiescence of the general population" in the AO. This is to be distinguished from battles over what is merely *physical space*, territory itself – a key distinction between this particular form of irregular warfare and traditional conventional warfare [7]. Inherent in this is that PSYOP and other non-kinetic techniques are at least as valuable as - if not more than - traditional kinetic techniques in winning these battles. Finally, the third and most inclusive definition takes into account the transnational nature of some contemporary insurgencies, noting that one or more states (Authorities) may battle one or more external or internal challengers (Rebels). This last definition, by David Killcullen, is probably the most useful.

In order to possibly use ecology models to understand COIN, at least one large generalization is necessary. That is, there are similarities that exist across most COIN environments. This assumption is particularly germane in light of recent discussions about the new "global insurgency" and its similarities and differences with "classical insurgencies" [8]. To some extent, there has been a paradigm shift in how insurgencies operate in the modern age. Communications have improved; financing is different. However, this does not mean that the "essence" of insurgency, or fighting it, has been significantly altered. If this is true – if there are generalities about COIN that we can understand at a fundamental level despite adaptational differences over the decades – then we can ask, is there a set of ecological models that addresses these similarities, and thus has the utility to be applied to different insurgencies in the past, present, and future? If so, what are those models?

Simple models: Us versus Them

The interaction of insurgents and counter-insurgents on an asymmetric battlefield resembles the perennial struggle between predator and prey . Mathematical models of predation are some of the oldest in the field of ecology and evolutionary biology and date back nearly a century to seminal work resulting in the influential Lotka-Volterra equations [9].

On the surface, the simple metaphor of predator-prey interactions is appealing. Predators are suited in style to kill prey, and prey, in turn, are quite often adept at escaping their common predators [10]. When observed in nature, these "arms races" have resulted in at least a temporary equilibrium; where they have not, no interaction can be observed, and the prey have gone extinct. The symbolism is obvious.

Furthermore, observations from nature suggest numerous overt mechanisms by which prey avoid extinction [11]. They can reduce the kill rate by decreasing local prey density (therefore increasing predator search time) or increasing "handling time" (time taken to kill a prey item). Prey can also utilize strategies such as occupying territory within which predators can't hunt (small rodent prey can burrow, for example) – prey can always persist at low densities in such spatial refuges. There may be a victim "carrying capacity" – a maximum number

of kills per day (predators having eating limitations). Waning prey populations can be reinforced by immigrants from populations not being preyed upon. All of these scenarios have counterparts in human warfare.

The excellent verbal metaphor begs the question: Do mathematical models of predator-prey interactions among animal species have any relevance for understanding interactions during a counterinsurgency campaign?

Imagine a pyramid describing categories of people in the AO of a COIN campaign. At the base of the pyramid is the general population – people who just want to go about their lives. The middle contains, in far lesser numbers, the criminal element of the population. These people are most likely not part of the Rebellion, but rather take advantage of a weak or distracted Authority in order to better themselves. Finally, at the top of the pyramid are the insurgents, or Rebellion. Historical data puts this group at about 0-1% of the population in the AO.

In theory, one could separate these three groups with regard to counterinsurgency operations. That is, one group from the Authority could concentrate on political affairs (targeting the general population), another group could conduct policing (targeting criminals), and a final group could perform "hunter-killer" operations (against the Rebels). This is in contrast to single individuals/units performing a mixture of these three basic COIN functions. In this framework, a simple predator-prey model may be valuable for simulating what takes place during COIN at the top of the pyramid. An historical example of this would be Operation Phoenix during the Vietnam War .

Population models such as those used to describe systems of predator- prey interactions are systems of differential equations. The most widely influential predator-prey models are those originally constructed by Lotka and Volterra [12]. In essence, the Lotka-Volterra predation model is a system of 1st-order differential equations describing the interaction between predator and prey. This interaction is commonly symbolized as (+, -) because the effect of the prey on the predator is positive (+), and the effect of the predator on the prey is negative (-).

The Lotka-Volterra "growth" equations for Authority and Rebellion describe how predator and prey populations change in size based on natural birth and death rates and the interaction between predator and prey [13] . The notion of predator and prey fighting to "win" is attractive on its surface. The key question is: Does this biological model accurately depict the interactions and relationships between Authority and Rebellion in a COIN ecosystem?

Numerous assumptions accompany the Lotka-Volterra predation model [14] . Some are non-negotiable while others can be accounted for by making adjustments such as adding new variables. Five key assumptions are:

- Prey population growth is limited only by predation
- Predator is a specialist that can persist only in presence of prey
- Individual predators can consume an infinite number of prey
- Random encounters occur in an homogenous environment
- There is a closed system with no migration

In natural systems of animal predators and prey, these assumptions often hold true - at least insofar that their violation does not severely disrupt the outcome of the system. However, in COIN, the actors (Rebellion and Authority) most likely violate these assumptions to the point of the model not being effective. For example, the Rebellion population is probably limited in size by more factors than the Authority kill rate. Furthermore, the Authority population does not receive a genuine positive (+) benefit from killing Rebels (with regard to population size/growth) and indeed can persist without the Rebellion. There is most likely some degree of migration for the Rebellion and Authority in and out of the AO (although this particular situation can be alleviated by modifying the model to account for this). Finally, the environments within which Rebellion and Authority encounter each other are always heterogeneous, and encounters are often non-random. To summarize, the ecological predation model framework is probably oversimplified and not very useful for understanding COIN.

The overarching problem with the relatively simple predation, parasitism, and mutualism models is that they do not include the major aspect of COIN that distinguishes it from conventional warfare: the role of the general Population in the success or failure of the Authority and Rebellion. A successful COIN campaign is not won when the most Rebels are killed; rather, it is won when the most "political space" is controlled. The Authority does not "grow" when a Rebel is killed as the predation "growth" equations maintain. Both Authority and Rebellion can grow in some sense when they win the hearts, minds, and acquiescence of a member of the general Population. This individual will effectively "join their side" and increase their population size.

Another class of ecological models, competition models, take this into account and may be more

useful for describing the complex conflict ecosystem of COIN.

Competition models: Parts of the whole

COIN is more than killing insurgents . Killing the enemy is not the primary objective; rather, it is to out-compete challengers to control political space made up of the general population's hearts, minds, and acquiescence (Figure 2). The Authority can be viewed as a coalition of Security Forces, Government Infrastructure that supports the Authority, and persons in the Population that firmly support the Authority. Similarly, the Rebellion can be seen as the group containing actual Insurgent Combatants, the Auxillary forces that directly support them, and Indirect Supporters in the Population make up the "Underground" movement that opposes the Authority but does not directly fight. In the middle are the undecided general Population.

Hence, access to and control of the general Population in the center of Figure 2 is what the competition between A and R is about. Luckily, there is another class of ecological models which may in fact be relevant and useful, however: models of interspecific competition for resources .

Ecological competition models can be seen through the prism of COIN as more "inclusive," taking into account not only the insurgents and counterinsurgents but also the larger civilian Population within the area of operations (AO). Calculations based on historical COIN data suggest that insurgents and counterinsurgents as a percentage of the AO population is very small . Typically, reliable data from COIN is hard to come by, but, where information is available, insurgent combatants have comprised 0-1% of the overall population, and counterinsurgents or security forces amounted to 1-2% of the population . Hence, by ignoring 97% of the persons in the AO – among other reasons - simple ecological models like those describing predator-prey interactions lose much of the realism contained within the unconventional warfare of COIN.

Competition in nature comes in a number of forms, and ecologists have developed different mathematical competition models to describe them. One example is "exploitation competition," described as the negative (-,-) interaction of two (or mdirectly fight. In the middle are the undecided general Population.

Hence, access to and control of the general Population in the center of Figure 2 is what the competition between A and R is about. Luckily, there is another class of ecological models which may in fact be relevant and useful, however: models of interspecific competition for resources .

Ecological competition models can be seen through the prism of COIN as more "inclusive," taking into account not only the insurgents and counterinsurgents but also the larger civilian Population within the area of operations (AO). Calculations based on historical COIN data suggest that insurgents and counterinsurgents as a percentage of the AO population is very small [15]. Typically, reliable data from COIN is hard to come by, but, where information is available, insurgent combatants have comprised 0-1% of the overall population, and counterinsurgents or security forces amounted to 1-2% of the population . Hence, by ignoring 97% of the persons in the AO – among other reasons - simple ecological models like those describing predator-prey interactions lose much of the realism contained within the unconventional warfare of COIN.

Competition in nature comes in a number of forms, and ecologists have developed different mathematical competition models to describe them. One example is "exploitation competition," described as the negative (-,-) interaction of two (or more) species over a limited resource within the environment. The species *indirectly* "harm" each other by using non-renewable resources that the other species needs . In nature, for example, this resource might be food – an item that can ultimately constrain the local population growth rate of each species. However, this common form of competition in nature does not accurately describe what occurs between the Authority and Rebellion during an insurgency, because the numbers of opposing forces do not grow in direct relation to how many "hearts and minds" are won over. Furthermore, the "Competitive Exclusion Principle" of competition states that (in a simple system with two species competing for a single resource in a homogenous environment with no other interactions) two species cannot compete for the same limiting resource for a long period of time.

A simple extension of exploitation competition is more realistic and applicable. Termed "interference competition," it occurs when species seeking a resource harm each other when gathering it, even if it is not in limited supply . Here, there is indirect competition for a limited resource and direct competition between the competitors for access to the resource (the interference). A simple and amusing human analogy is a competition between a couple on a date sharing a milkshake with two straws. In an exploitation competition, the winner drinks more of the milkshake. In an interference competition, both people drink, but one person pinches the other's straw [16].

For our purposes, there are three "species" or actors involved – Authority (A), Rebellion (R), and Population (P). A preys on R, and both compete for access to P (a precursor to winning support: a means to an end). Such "competition for access" to P can be considered predation for the purposes of this model [17]. This three-actor "food web" is based on Okuyama and Ruyle's diagram [18].

Generally speaking, the interference competition model is more realistic than others we have considered and dismissed because while simplified two-species models have definite and constant effects - like competition (-,-), mutualism (+,+), and predation/parasitism (+,-) - situations are often more complicated. In interference competition, species are not classified strictly as a "competitor" or a "predator" but rather can play multiple roles across time and space. This is most likely the rule, not an exception [19] .

Unfortunately, from the standpoint of COIN, interference competition can allow, and even promote, coexistence of competitors on a shared resource. This is in contrast to exploitation competition, where in theory the Competitive Exclusion Principle would hold and one of the competing species would go extinct. In fact, with interference competition, assuming that the Competitive Exclusion Principle operates and that one species (Authority) is the "top predator" over the other competitive species (Rebellion) in order for coexistence to occur, the Rebellion must be better at competing for the resource. This is what we tend to see in COIN campaigns that lead to stalemate or loss for the Authority. Obviously, if the Authority is better at preying on the insurgency and is equally good at competing for the Population, the Authority will win.

There are some additional assumptions made in order for these types of interference competition models to work [20] . One is that the resource being competed for is in limited supply; else, there would be no competition. This is a reasonable assumption for COIN, particularly when viewed at a smaller-than-nation scale (e.g., a district). Another assumption is that "competition coefficients" and other components of the model are constants [21], but they may in reality be functions. This can make the model more difficult to wield, but data-based adjustments can be performed.

Another assumption of the competition models is that density dependence is linear, meaning that adding an individual to the A or R groups decreases in a linear manner the growth rate of the group. In fact, this assumption may be wildly violated and suggests that a different approach may be valuable (see section on Adaptive Dynamics, below). However, like many assumptions, if the effect is different (nonlinear or complex), this mainly makes interpretation, visualization, and prediction difficult and does not mean the model in itself is useless.

A final simplifying assumption of these competition models is that there is a "closed system". (This is an assumption of most every simple model.) In other words, the Authority and Rebellion receive no exogenous support. This is most likely violated in a majority of cases. Indeed, it has been wagered that rarely does an insurgency survive without exogenous support [22]. Such "migration effects" are also common to animal systems and can generally be accounted for with additional variables/factors (*i.e.*, migration rate of R in and out of the system) in the primary sets of equations. Migration, if it occurs, may not matter if its rate is low. It may also occur in some parts of the AO and not in others, allowing the model to be more accurate in some provinces than in others.

The reality of counterinsurgency – for example, the current war in Iraq – can certainly involve multiple actors (*i.e.*, multiple simultaneous Rebellions). Although outside the scope of this paper and more mathematically intensive, the three-way interaction outlined above (Figure 3, with A, R, and P) can be extended to *N* groups using matrices and can incorporate additional features [23].

The above scenario relies on the simplifying assumption that the Authority preys on the Rebellion unidirectionally. This assumption is perhaps reasonable if we suppose that Authority manpower is easily replaced (or substantially more easily replaceable than that of the Rebellion). If this assumption is relaxed - if we allow the Rebellion to *substantially* prey on the Authority - the model becomes more complex. Of course, each "predator" cannot prey on the other equally, and thus one must be better. Hence, in this model, one could then normalize predation such that R predation on A is equal to 0, and therefore, Authority is forced to be the predator over R [24].

It is important to note that there can be benefits or costs to successful A predation on R. The key point is that in this competition model, the goal is to obtain access to the resource (P); A predation on R is only beneficial inasmuch as it increases access to P. Looking at Figure 3, there can be direct and indirect feedback to A due to direct predation on R.

The fact that interference competition may be asymmetric between Authority and Rebellion (*e.g.,* A may be better at preying on R) means it can also be accounted for by the correction terms in the original equations.

All things considered, interference competition models from ecology are a relatively simple quantitative approach to modeling, understanding, and perhaps predicting COIN at a very simple, fundamental level. However, in order to make a more realistic model, many factors need to be changed or added, and it is still not clear that some of the fundamental assumptions (*e.g.*, logistic growth rates) are realistic or meaningful. In addition, all of the detailed mechanism of *how* predation and competition occur have been left out!

Luckily, some ecologists have felt the same way about their systems of study and have pondered the same issues, even though the Lotka-Volterra competition framework has been generally useful for decades. There is another more advanced and more newly developed class of ecological models that may be useful for COIN based in game theory.

Fight or Flight: Adaptive Dynamics

The analysis of interference competition is complicated in comparison to exploitative competition, and although many studies have observed interference competition in nature, formal models are still relatively rudimentary. One issue is that the individual behaviors that underlie the interference are quite varied and complex [25]. Ecological population models, like the ones discussed above, do not take this array of behaviors into account.

These individual-level behaviors may have important influences on group behavior, something ecologists are only now coming to terms with. Similarly, differences in individual ability, competitiveness, experience, social interactions, and similar factors may have influences on overall group success.

An alternative approach to the Lotka-Volterra population models is based in the field of mathematics called game theory [26]. The key difference between ecological population models and game theory models for effectively modeling the same behaviors is that population models expend with biological detail for simplicity while game theory ignores underlying "genetic detail" (the "how" of behavior) but utilizes ecological realism to describe the system.

There are two new key incorporations beyond the competition model. First, individuals can be in different behavioral states at different times (e.g., searching, handling, fighting), incorporating a mechanistic reality into the model. These states and actions occur at certain frequencies, and the frequency at which one actor (say, Authority) is doing something ("searching for Population members to influence") may depend on the frequency with which the other actor (say, Rebel) is doing something else ("hunting for Authority troops"). Second, individuals weigh the gains and losses from each action (as much as that's possible) and then attempt to perform the optimum behavior based on their state and the state of an interacting individual.

"Adaptive Dynamics" is effectively a combination of game theory and population biology and is a relatively new area of study (~10 years old). It is now being used in ecology and other fields to study complex adaptive systems, involving a few moving parts and a discrete number of variables that when combined together have emergent properties . The advantage of this kind of modeling is that it incorporates specific variables along with stochasticity to model evolution in a complex, nonlinear ecological system. Such systems are those encountered both in nature and on a battlefield.

A "decision tree" is associated with this type of model. The tree keeps track of all possible events and actions that could occur to a member of the Authority . (The opposite can be done for events and actions of a Rebellion member.) In ecological competition, such trees are used to keep track of foraging behavior [27]. In our example the Authority member is assumed to be in one of three distinct states: *searching* for a member of the Population to "consume" (*i.e.* win over to the Authority's side), *handling* a member of the Population (*i.e.* talking to them, making deals, etc.), or *fighting over* a Population member with someone from the Rebellion (*i.e.* interference competition). This is an oversimplification but a useful one as it captures the general goals and strategy behind COIN.

The states change according to events and choices that the Authority member faces. Sometimes the response to an event is predetermined, and sometimes an action requires a choice. Tradeoffs to decision choices include "energy" and "time", and so each decision has some consequence associated with it.

These decision trees intersect with game theory: For each decision, we know the costs and benefits associated with each choice/decision and the probability associated with each choice. From consequences and probabilities, a modeler can arrive at a "payoff function" that is associated with a given strategy. Generally, one follows a strategy which maximizes this payoff function.

For the purposes of mathematical analysis, these probabilities are variables. For example, the probability of being "discovered" by a Rebel while handling a Population member might be called κ ; therefore the probability of not being discovered is $(1-\kappa)$, etc. In simulation studies, different reasonable values, hopefully based on actual field data, are

tried for different variables, and in this way, a spectrum of outcomes can be determined from a number of variables.

In addition, within the "conflict boxes" shown in Figure 4, are "conflict decision trees" (not shown). Hence, the conflict box does not necessarily mean that a conflict occurs, only that it is possible for one to occur. Similar to the main decision tree, the Authority member can either "be careful" (*i.e.* avoid) or "dare" (*i.e.* threaten) the Rebel, and if a conflict ensues, it can either be won or lost. If won, the Authority can in theory continue to "handle" the Population member; if lost, the Authority is relegated back to searching (at best).

Because this type of model is essentially "designed around" the problem at hand, there are less assumptions to be violated by reality because there are more details incorporated into the model. However, these Adaptive Dynamics models also have their peccadilloes. One, for example, has to do with the notion of a payoff. Every model of this type, even in ecology, must have some kind of short-term currency to approximate long-term cost or benefit of actions [28] . In ecology and evolution, the payoff approximates "fitness", which is the ultimate survival and reproductive power of a type of individual with a certain combination of genes, etc. In COIN, it is even harder to estimate the payoff associated with killing one Rebel or winning over one member of the Population to be pro-Authority. With regard to warfare, this is an area that must be given much careful thought.

Adaptive dynamics models, in the end, can offer predictions about the best strategies for providing the "highest payoff" when facing an opponent in a game who is expected to play a number of strategies with certain probabilities. It can predict consequences of various choices/actions and recommend strategies. This is conditional, of course, on the correct variables, states, and probabilities being included in the model.

Modeling war: what is it good for?

Models are, by definition, not reality [29]. They are deliberate oversimplifications of reality constructed systematically to gain insight into how a complex system of interacting factors operates in principle. As in the theoretical study of complex systems and networks in, say, biology or economics, here we propose that models can serve as a (perhaps crude) framework for understanding fundamental components of COIN warfare.

Specifically, in this initial effort, we have borrowed a class of model from ecology called "interference competition" models, in which two species compete for a common resource while simultaneously one preys on the other, creating interference. On the surface, this closely resembles what we see in a COIN system – A conventionally powerful Authority (the "top predator") competes with a Rebellion for access to political space comprised of control over the general Population, and at the same time, the Authority is directly preying on the Rebellion.

One general weakness with this kind of model is that biological realism of the behaviors involved is ignored for the sake of simplicity. For example, there is an assumption of interference without considering its mechanism or "adaptive value." In nature, a given animal in one state might attack and in another state might flee. In this sense, individuals within species are treated like "aimless billiard balls" that randomly encounter each other and subsequently act aggressively [30] . For many ecological purposes, this is okay; general insight about population dynamics can be gained while ignoring the realism of very complicated ecosystems. It is currently unclear how directly applicable this possibly useful model will be towards understanding the underpinnings of COIN.

As an alternative, we also considered a class of models based on game theory combined with population biology called "Adaptive Dynamics" models. This class of models is far more complicated but, as a worthy trade-off, also are more descriptive of the behaviors of individuals alone and during interactions than are the "Lotka-Volterra" models of competition (contrast Figures 3 and 4). While more difficult to work with, these models may in fact ultimately be better at describing the intricacies of COIN warfare. Ultimately, these Adaptive Dynamics models are most likely more useful. One caveat is that, unlike the century-old Lotka-Volterra competition models, Adaptive Dynamics models are a tenth the age and less developed and evaluated.

Neither of the proposed model frameworks is perfect. Assumptions are sometimes violated. Details are glossed over. Ties are drawn across vastly different areas of study. Metaphors are occasionally taken just a step too far. However, we think there is a good deal of value in this discussion. Our hope in introducing the topic of using ecological models to understand COIN is twofold.

One, we reason that "thinking like a biologist" can in itself provide food for thought with regard to studying and planning for COIN and other forms of warfare. Although comparing war fighters to foraging birds (for instance) may seem silly or juvenile on the surface, the problems that foraging animals face are literally life-and-death – they forage and

find prey, or they die. Similarities between some forms of animal behavior and that of soldiers on patrol, for example, are striking, and therefore, there may be some genuine value in this line of thought.

Two, we believe that these models, or variations or derivations thereof, may be useful for sketching out the broad strokes of the behaviors that occur during unconventional warfare and can thereby capture some major elements of it, allowing for some general insights to be obtained. It is not immediately clear if a simple or complex model is best, nor is it clear whether descriptive and vague models or very specific models are the answer. It is furthermore not clear that there is "an answer."

Further work in this area will allow us to make these determinations. In the near future, our group hopes to expand on the interference competition model concept and develop more detailed, deterministic, and stochastic models and simulations in order to explore the possible relationship between ecology and COIN.

There are additional, complicating issues with regard to utilizing ecology models in the study of unconventional warfare. These are not necessarily "problems" but things that should be taken into careful consideration before or during application of these models. One issue is "scale-dependence". The dynamics of interaction between A, R, and P depend on the scale one looks at. To some extent, there is also an issue of "density dependence", a complicating and common issue in population ecology. Some models may apply at one scale (town) but not at another (nation). Larger scales may also hold more heterogeneity, etc.

Another issue is "asymmetry of support". By this we mean that, in order to be judged as "successful", A and R require different levels of popular support. In ecological terms, R needs to consume less of P than A does to maintain equality. At present, it is not clear to us if or how a model needs to be modified to take this into account.

A final issue of note is "means versus will". The model only addresses the means to fight but ignores the reality of political will to keep fighting. This again may be asymmetrical with A finding it more difficult to maintain political will, particularly as an occupying force. Like asymmetry of support, it is not clear if this is a factor that can be ignored with regard to the models.

The general discussion of utilizing ecological models to model warfare leads to some other matters for discussion. One of these matters, with regard to COIN, is a debate about the proper or necessary ratio of Authority troops to those of the Rebels or, alternatively, those of the Authority to members of the Population in the AO. Both traditional and modern books and manuals recommend a ratio of 10-20:1 for A:R and 20-25:1000 for A:P [31]. This is largely based on experiences from previous COIN campaigns, which are generally dated. Additionally, historical data indicate that there is not necessarily a direct relationship between the ratios and relative success [32]. It is possible that further quantitative analysis using models like the ones presented in this paper could shed light on this issue. We have no conclusions as of yet. However, the "validity" of using predator-prey vs. competition models, as explained above, seems to suggest that "hunting insurgents", "policing criminals" and "political control" are not easily separable.

Through all of this, a key general issue is, how does one measure success in COIN? We ascertain that "access to the population" is a means to the end goal of "support of the population" via the cliché of winning their hearts, minds, and acquiescence. Within our ecological model of competition, this is represented as members of the Population effectively "joining" the Authority or Rebellion, thus increasing their population size.

In this paper, we have been asking how the study of warfare could benefit from ecology. But what about the reverse – Could the field of ecology benefit from the study of war? Hard science research often progresses in fits and starts by the whims of investigators' groupthink about what is "fashionable" (or fundable) at any given time. Often, the status quo remains until a tipping point occurs at which a majority of powerful scientists decide that a shift is in order. With regard to the present topic, some areas of ecological theory, such as IGP theory, are underdeveloped for no particular reason having to do with the models. More specifically, complicating factors such as adaptive behaviors, spatial heterogeneity, and prey refuges have generally not been incorporated into the theory and their effects on the system have not been well investigated. If these factors are critical to the understanding of COIN via ecology – and they well may be – initial work within the military community could stimulate ecologists to work on variants of these models, thus creating a circle of benefit for all involved.

There may be additional fields of study within the social sciences that can benefit from such work and may also contribute to it. One example is the recent thesis by Evans and Spies entitled, "Insurgency in the Hood: Understanding Insurgencies Through Urban Gangs" [33]. The authors suggest that it is very difficult to obtain unbiased, accurate data about insurgencies; it is easier to study organiza-

tions like gangs as a surrogate in order to gain insight to generalities of use to the war fighter. We further suggest that preliminary results from ecological models of COIN could be compared to data such as that from urban gangs which, at a fundamental level, operate somewhat like insurgencies.

Finally, we can consider these questions: What does modeling COIN using ecology mean for war fighters? Or war planners? Are the models useful for determining how to win, how not to lose, or how to avoid Pyrrhic victories? How should/could lessons from biology be incorporated into war fighter education, training, and doctrine? This paper, as a thought experiment, has raised more questions than it has answered. Some of them are: Are the variables in the ecological models measurable in COIN? Is there accurate data, and is it specific to a single insurgency? What are the relevant outputs of these models? Will the outputs be descriptive, or prescriptive

In the end, we return to the idea stated at the beginning of this paper – Biology is more than laboratory science; it is a way of thinking about the natural world. An increased emphasis on adaptation, evolution, behavior, metaphors, and models in these areas would have great benefits in the new climate of conflict in the early 21st century .

NOTES

[1] See, for example, David Killcullen, "Counterinsurgency Redux," *Survival* (Winter 2006-07),Vol 48, No. 4, pp. 111-130, and "Twenty-eight Articles: Fundamentals of Company-Level Counterinsurgency," Joint Information Operations Center, Australian Army, Summer 2006, pp. 29-35.

[2] See for example, Raphael Sagarin, "Adapt or Die: What Charles Darwin can teach Tom Ridge about homeland security," *Foreign Policy* Sep/Oct 2003, pp. 68-69; Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider* (2006), Penguin Group, New York; Mark D. Drapeau, "Fishing for Terrorist Starfish," *The Washington Times* Commentary 31 July 2007, p. A16; Richard Dawkins, *The Selfish Gene* (1976). Dawkins' biological metaphors include the transmission of ideas (usually from human to human) in units called "memes," which are akin to the better known genes – which transmit hereditary information from parent to offspring. See also the very recent book, *The Black Swan: The Impact of the Highly Improbable*, by Nassim Nicholas Taleb (2007), Random House, New York.

[3] See "Counterinsurgency Redux," note 2. Some additional biological metaphors used it the paper are "self-synchronizing swarm[s] of cells," "the war of the flea," the notion of a "complex conflict ecosystem," and "competing entities [maximizing] survivability." Also, from the same author Killcullen (2006) Three Pillars of Counterinsurgency, remarks delivered at the U.S. Government COIN Conference, Washington DC, 28 Sept 2006, there are terms such as "model," "environment," "survivability," "evolving," "adapting," and "predator."

[4] See the very interesting commentary on this by John A. Nagl, 2002 (2005: 2nd ed.), *Learning to Eat Soup With a Knife: Counterinsurgency Lessons from Malaya and Vietnam*, The University of Chicago Press, Chicago, IL. The title is partly a quotation from *Seven Pillars of Wisdom* by T. E. Lawrence ("Lawrence of Arabia") – "To make war upon rebellion is messy and slow, like eating soup with a knife."

[5] Nathan Leites and Charles World, *Rebellion and Authority*.

[6] The first quotation is from the Australian *Joint Services Glossary*; the second from Gordon McCormick of the Naval Postgraduate School (2007), Things Fall Apart: The 'Endgame' Dynamics of Internal Wars, RAND paper; and the final quotation is from David Killcullen (2006) Three Pillars of Counterinsurgency, remarks delivered at the U.S. Government COIN Conference, Washington DC, 28 Sept 2006.

[7] The U.S. Defense Department's 2006 Quadrennial Defense Review (QDR 2006) notes that transforming the DoD to a state in which it is prepared for unconventional warfare is a major priority.

[8] See "Counterinsurgency Redux," note 2.

[9] Alfred J. Lotka (1925), *Elements of physical biology*, Williams & Wilkins Co., Baltimore, MD. Vito Volterra (1926), Variazioni e fluttuazioni del numero d'individui in specie animali conviventi. Mem. R. Accad. Naz. dei Lincei. Ser. VI, vol. 2.

[10] See for example, Toshinori Okuyama and Robert L. Ruyle (2003) Analysis of adaptive foraging in an intra-guild predation system, *Web Ecology* 4: 1-6, and note 24.

[11] See for example, Nicholas J. Gotelli, *A Primer of Ecology* (1995), Sinauer Associates Inc., Sunderland, MA, Chapter 6.

[12] See note 6.

[13] The Lotka-Volterra predation equations take the form:

$$\frac{dA}{dt} = \alpha AR - \beta A$$

$$\frac{dR}{dt} = \gamma R - \delta AR$$

Here, the change in the Authority over time (*dA/dt*) is the

growth of the Authority due to positive interactions with the Rebellion (αAR) minus deaths due to natural causes (βA). Change in the Rebellion (dR/dt) is the natural growth rate (γR) minus the predation rate by the Authority (δAR).

[14] See note 10.

[15] James T. Quinlivan, 1995, Force Requirements in Stability Operations, *Parameters* Winter 1995, pp. 59-69. Accessed August 2007 at: http://carlisle.army.mil/usawc/Parameters/1995/quinliv.htm.

[16] See note 10, p. 112.

[17] The interference competition model takes the basic form:

$$\frac{dA}{dt} = r_A A\left(\frac{K_A - A - f(R)}{K_A}\right) + \alpha AR$$

$$\frac{dR}{dt} = r_R R\left(\frac{K_R - R - f(A)}{K_R}\right) - \beta AR$$

Here, r_A and r_R are the logistic growth rates of the Authority and Rebellion, respectively. The term r, the logistic growth rate (effectively a combined rate for "birth" and "death"), is commonly used in ecology and other fields like demography, and is typically a positive value between 0 and 4 (see http://en.wikipedia.org/wiki/Logistic_equation, accessed 1 Aug 2007). K_A and K_R are the respective "carrying capacities" for A and R. Carrying capacity is the maximum sustainable level of population size at equilibrium. The middle term in parentheses, in words, shows that the growth in the first term is decreased by intraspecific competition (e.g., $K_A - A$) and also by competition due to the other species (e.g., the $-f(R)$ term). Finally, the levels of Authority are increased by the interaction between A and R (the $+\alpha AR$ term), and levels of Rebellion are decreased (the $-\beta AR$ term). see Toshinori Okuyama and Robert L. Ruyle (2003) Analysis of adaptive foraging in an intraguild predation system, *Web Ecology* 4: 1-6.

Also see, for example, Thomas W. Schoener, 1976, Alternatives to Lotka-Volterra Competition: Models of Intermediate Complexity, *Theoretical Population Biology*, 10: 309-333.

[18] See Figure 1 of Toshinori Okuyama and Robert L. Ruyle (2003), note 23.

[19] G. A. Polis, C. A. Meyers, and R. D. Holt. 1989. The ecology and evolution of intraguild predation: potential competitors that eat each other. *Annual Review of Ecology and Systematics* 20: 297-330; M. Arim and P. A. Marquet. 2004. Intraguild predation: a widespread interaction related to species biology. *Ecology Letters* 7: 557-564.

[20] See note 12, Chapter 5.

[21] See note 25.

[22] See Nagl (2002), note 5, p. xvi.

[23] See http://en.wikipedia.org/wiki/Lotka-Volterra_inter-specific_competition_equations/, accessed July 30, 2007.

[24] See also Toshinori Okuyama and Robert L. Ruyle (2003), note 23, for incorporating the "antipredator behavior" of prey into interference competition models.

[25] Wouter K. Vahl, G. Sander van Doorn, and Franz J. Weissing, "unpublished manuscript", Ch. 6 in Wouter K. Vahl, Ph.D. dissertation, University of Groningen. See also, F. Huntingford and A. Turner, 1987, *Animal Conflict*, London: Chapman and Hall.

[26] See John Maynard Smith (1982) *Evolution and the Theory of Games* for relevance to biology.

[27] See also P. H. Crowley (2000), Hawks, doves, and mixed-symmetry games. *Journal of Theoretical Biology* 204: 543-563.

[28] See Vahl et al., note 33, page 167.

[29] Definition of "model" – "A schematic description of a system, theory, or phenomenon that accounts for its known or inferred properties and may be used for further study of its characteristics." *The American Heritage® Dictionary of the English Language, Fourth Edition*. Houghton Mifflin Company, 2004. 02 Aug. 2007. <Dictionary.com http://dictionary.reference.com/browse/model>.

[30] Jaap van der Meer and Bruno J. Ens, 1997, Models of interference and their consequences for the spatial distribution of ideal and free predators. *Journal of Animal Ecology* 66: 846-858.

[31] See David Galula (1964, 2006 ed.), *Counterinsurgency Warfare: Theory and Practice*, Praeger Security International, p. 61. Also see General Petreus (USA) and Lt. Gen. Mattis (USMC), in their much-discussed *Counterinsurgency Field Manual FM 3-24* (2006), recommend "a range of 20-25 counterinsurgents for every 1000 residents in an AO." See John C. McGrath, 2006, *Boots on the Ground: Troops Density in Contingency Operations*

[32] James T. Quinlivan, 1995, Force Requirements in Stability Operations, *Parameters* Winter 1995, pp. 59-69, Figure 1

[33] Edward Evans and James Spies (June 2006). Insurgency in the Hood: Understanding Insurgencies Through Urban Gangs. M.S. thesis, Naval Postgraduate School, Monterrey, CA.

AUTHORS

Mark D. Drapeau, Ph.D. is a 2006-2008 AAAS Science & Technology Policy Fellow in National Defense and Global Security at the Center for Technology and National Security Policy (CTNSP) of the National Defense University (NDU) in Washington, DC. Dr. Drapeau may be contacted via email at DrapeauM@ndu.edu or by phone at (202) 685-2406.

CDT Peyton Hurley (USMA, 2008) conducted research for this paper while a summer intern at the RAND Corporation in Arlington, VA.

Robert E. Armstrong, Ph.D. (COL, Ret., USAR) is a Senior Research Fellow at NDU-CTNSP.

QUOTES WORTH PONDERING

Entities of an essentially new sort are entering the sphere of scientific thought.

Classical science in its diverse disciplines, be it chemistry, biology, psychology or the social sciences, tried to isolate the elements of the observed universe

— chemical compounds and enzymes, cells, elementary sensations, freely competing individuals, what not —

expecting that, by putting them together again, conceptually or experimentally, the whole or system - cell, mind, society - would result and be intelligible.

Now we have learned that for an understanding not only the elements ***but their interrelations as well*** *are required..."*

— Ludwig Bertalanffy
General Systems Theory

Tools for Automated Analysis of Networked Verbal Communication

Peter W. Foltz, Noelle Lavoie, Robert J. Oberbreckling and Mark B. Rosenstein

ABSTRACT

One of the richest sources of information about performance in networked teams is their communication data. Nevertheless, analysis of communication requires tools that can assess both the content and patterns of information flowing in the network. This paper describes research and development of a set of tools for the automatic analysis of verbal communication. The tools use language technologies to analyze the content of communication, thereby permitting characterization of the topics and quality of information being transmitted. The tool can be used for automatically deriving accurate team performance metrics from communication in networked teams as well as providing visualization tools to provide teams and commanders better situational awareness. The toolset has the potential for providing near-real-time assessment of team performance including measures of situation awareness, knowledge gaps, workload, and detection of critical incidents. It can be used for tracking teams' behavior and cognitive states, determining appropriate feedback, and for automating After Action Reviews.

INTRODUCTION

As the military incorporates greater network-centric operations and technology, it becomes increasingly important to be able to monitor and assess performance of teams. However there are numerous challenges regarding how to effectively identify, track, analyze, and report on team performance in real-time in such complex operational environments. For example, current methods of assessing team and group performance rely largely on global outcome metrics, which often lack information rich enough to diagnose failures, detect critical incidents, or suggest improvements for the teams or for their collaborative aids. Thus, while there has been an increase in the availability of networked information, there needs to be a concomitant increase in the availability of tools that can leverage off of the networked data to monitor, support and enhance team performance.

Networked teams provide a rich source of information about their performance through their verbal communication. The communication data includes information both about the structure of the network and the content of information flowing on the network. The structure of the network can indicate such things as team member roles, paths of information flow and levels of connectedness within and across teams. The content of the information communicated provides a rich indication of what information team members know, what they tell others, and what their current situation is. in order to be able to assess that team's performance. Thus, communication data can provide information about team cognitive states, knowledge, errors, information sharing, coordination, leadership, stress, workload, intent, and situational status. Indeed, within distributed training, trainers and subject matter experts typically must rely on listening to a team's communication. Nevertheless, in order to exploit the communication data, technologies need to be available that can assess both the content and patterns of the verbal information flowing in the network and convert the analyses into results that would be usable by teams and commanders.

This paper provides an overview of ongoing research and development of a set of tools for the automatic analysis of verbal communication. The tools use language technologies to analyze the content of communication, thereby permitting characterization of the topics and quality of information being transmitted. These tools can both provide metrics of team performance as well as be integrated into applications to provide automated aids for training and operational feedback and monitoring. Finally the paper describe how these tools can be incorporated into to visualization tools designed to analyze the content and patterns of communication streams in order to provide teams and commanders with improved situational awareness and tests in a recent multi-national exercise.

VERBAL COMMUNICATION ANALYSIS

The overall goal of automated verbal communication analysis is apply a set of computational modeling approaches to verbal communication in order to convert the networked communication into useful characterizations of performance. These charac-

terizations could include metrics of team performance, feedback to commanders, or alerts about critical incidents related to performance. In order to do this analysis, there are several components needed. The first component is that there has to be available sources of verbal communication. Second, there must be some pre-existing measures of performance with which to associate the communication to performance. Finally, there must be a set of computational approaches to apply to the communication in order to perform the analysis. These computational approaches include computational linguistic methods to analyze communication, machine-learning techniques to associate communication to performance measures, and finally cognitive and task modeling techniques.

By applying the computational approaches to the communication, we have a complete communication analysis pipeline. Figure 1 shows a representation of the communication analysis pipeline. By combining the tools in the pipeline, we are able to convert spoken and written communication directly into performance metrics which can then be incorporated into visualization tools to provide commanders and soldiers with applications such as, automated AARs and debriefing, near-realtime alerts of critical incidents, feedback to commanders of teams performing poorly, graphic representations of type and quality of information flowing among a team. We outline the approach to this communication analysis below.

A. *Communication data*

For analysis purposes, communication data can include most kinds of verbal communication among team members. Typed communication (e.g., chat, email or instant messages) can be automatically formatted for input into the analysis tools. Audio communication can include the capture of any kind of spoken data, including use of Voice over IP systems, radios, and phones.

Because a majority of military communication is typically spoken, automatic speech recognition systems (ASR) can be applied for converting speech to text for input into the communication analysis system. The communication analysis technologies have been tested for the analysis of ASR input for a number of datasets of verbal communication (see [1]). The results indicated that even with typical ASR systems degrading word recognition by 40%, the model prediction performance degraded less than 10%. Thus, the approach appears to be quite robust to typical ASR errors. Nevertheless, specialized speech models must be developed for each new domain to optimize ASR performance.

B. Performance metrics

In order to provide feedback on team performance, the toolset learns to associate team perform-

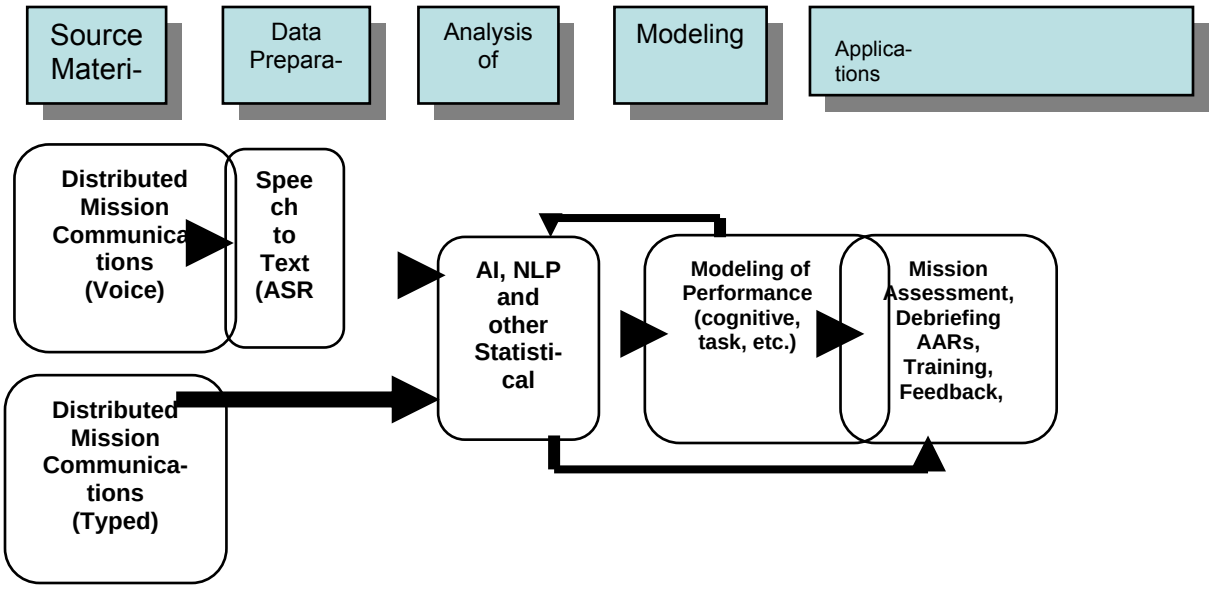


Figure 1. The Communication Analysis pipeline

ance metrics with the communication streams from those teams. Thus, the system typically requires one or more metrics of team performance. There are a wide range of issues in determining appropriate metrics for measuring team performance [2]. For example, metrics need to be associated with key outcomes or processes related to the team's tasks, they should able to be used in a manner to be able to provide feedback on deficiencies for individuals and/or teams, and they need to have a degree of reliability so that experts can agree on both the value of the metric and on how it should be scored for different teams [3].

Objective measures of performance can be used as metrics, indicating specific aspects performed by the teams. These measures can include such aspects as kills, deviations from optimal solution paths, objectives completed, and ACE reports. Alternatively, subjective measures of performance can be used as metrics. These can include, Subject Matter Experts (SME) ratings of such aspects as leadership, management of engagement, following doctrine, communication quality, situation awareness. Additionally SME provided information from AARs or identification of specific critical incidents, failures or errors can be used to measure performance. Nevertheless, all metrics will have varying levels of reliability as well as validity. For new metrics, it is often advisable to use ratings from more than one SME in order to determine reliability.

C. Computational modeling tools

The verbal communication data is converted to a computational representation which include measures of the content (what team members are talking about), quality (how well team members seem to know what they are talking about) and fluency (how well team members are talking about it). This process uses a combination of computational linguistic and machine learning techniques that analyze semantic, syntactic and statistical features of the communication stream.

The primary underlying technology used in this analysis is a method for mimicking human understanding of the meaning of natural language called. Latent Semantic Analysis (LSA) (see [4] for an overview of the technology). LSA is first automatically trained on a body of text containing knowledge of a domain, for example a set of training manuals, and/or domain relevant verbal communication. After such training, LSA is able to measure the degree of similarity of meaning of two communication utterances in a way that closely mimics human judgments. This capability can be used to understand the spoken interactions much in the same way a subject matter expert can compare the performance of one team or individual to others. The techniques has been widely used in other machine understanding technologies including commercial search engines, automated scoring of essay exams, and methods for modeling human language acquisition.

The results from the LSA analysis is combined with other computational language technologies which include techniques to measure syntactic complexity, patterns of interaction and coherence among team members, and statistical features of individual and team language (see [5] for examples of typical language analyses). The computational representation of the team language features are then used with machine-learning technology to predict the team performance metrics. In a sense, the overall method learns which features of team communication are associated with different metrics of team performance and then can predict scores for those metrics for any new set of communication data.

D. Performance metric prediction with the communication analysis toolkit

Tests of the toolkit's use for communication analysis have shown great promise. Tests are performed by training the system on one set of communication data and then testing its prediction performance on a new data set. This ensures that the models built will generalize to new communication. Using range of different types of military communication data, the toolkit is able to provide accurate predictions of the overall team performance and individual team metrics, it makes reliable judgments of the type of statements each team member is making, and it can predict team performance problems based on the patterns of communication among team members [6, 7].

Using human and ASR transcriptions of team missions in a UAV environment, in Air Force simulators of F-16 missions, and in Navy Tactical Decision-Making Under Stress (TADMUS) exercises, the tools predicted both objective team performance scores and SME ratings of performance at very high levels of reliability (correlations typically range from r=0.5 to r=0.9 over 20 tasks). It should be noted that the agreement between the toolkit's predictions and SMEs is typically within the range of one SME to another. In addition, the tools are able characterize the type of communication for individual utterances, (e.g., planning, stating facts, acknowledging) [8].

APPLICATIONS OF THE COMMUNICATION ANALYSIS TOOLKIT

A number of applications have been developed to further test the performance and validate the use of the toolkit in live situations. Below we describe three applications using the method to monitor and assess learning in online discussion environments, providing realtime analyses and visualizations of multi-national Stability and Support Operation exercises, and providing automated team performance metrics and detection of critical incidents in convoy operations.

A. Knowledge Post

In large networked organizations, it is difficult track performance in distributed exercises. Knowledge Post was designed for monitoring, moderating and assessing asynchronous collaborative learning and planning, The tools within Knowledge Post have been tested in a series of studies at the U.S. Army War College and the U.S. Air Force Academy [9,10, 11]. The application consists of an off-the-shelf threaded discussion group that has been substantially augmented with Latent Semantic Analysis based functionality to evaluate and support individual and team contributions.

Currently Knowledge Post supports the ability:

- To automatically notify the instructor when the discussion goes off track.
- To enhance the overall quality of the discussion and consequent learning level of the participants
- To have expert comments or library articles interjected into the discussion in appropriate places by automatically monitoring the discussion board activity.
- To find material in the discussion or electronic library that is similar in meaning to a given posting.
- To have contributions automatically summarized.

The utility of each of the aforementioned functions has been empirically evaluated with Army officers participating in planner exercises at the U. S. Army War College, and with cadets at the U. S. Air Force Academy

Among the findings of the studies were: the superiority of learning in a Knowledge Post environment over a face-to-face discussion with significant improved quality of discussion $F(2, 113) = 9.5$, $p < .001$; the usefulness of having a software agent automatically alert moderators when groups and individuals are floundering or drifting; increasing the solution quality of the group by interjecting expert comments automatically; and the usefulness to the participants of the Knowledge Post searching and summarizing features (see [9,10]).

TeamViz

TeamViz is a set of visualization tools and enhancements built on the Knowledge Post. toolset TeamViz was developed and run live during a U.S.-Singapore exercise designed to evaluate collaboration among joint, interagency, and multinational forces conducting combat and stability operations [12]. The system automatically analyzed the content and patterns of information flow of the networked communication and provided automated summarizations of the ongoing communications as well as network visualization tools to help improve situation awareness of team members. Analyses showed that the technology could track the flow of commander's intent among the team members as well as detect the effects of information injects on performance within the coalition task force and brigades who participated in the exercise. Singapore Officers used TeamViz in realtime to monitor the communication streams and inform commanders of important information flowing in the network as well as perceived information bottlenecks. Overall, the TeamViz technologies permit knowledge management of large amounts of communication as well as improve cognitive interoperability in distributed operations.

B. Competence Assessment and Alarms for Teams

Convoy operations require effective coordination among a number of vehicles and other elements, while maintaining security and accomplishing specific goals. Nevertheless, in training for convoy operations, it is difficult to monitor and provide feedback to team members in this complex environment. The DARPA Automated Competence Assessment and Alarms for Teams (DARCAAT) program was designed to do automated performance assessment and provide alarms for live and virtual convoy operations training. In currently ongoing research and development, we have collected communication data and SME-based performance measurements and developed specialized tools to assess performance in convoy operations.

Two sources of data were used to develop and validate the toolset, one from teams in a virtual environment and one from teams in live training environments. For the virtual environment, communication data was collected from the Fort Lewis MSTF,

PKT which uses the DARWARS Ambush! virtual environment convoy training. In the environment, up to 50 soldiers are able to jointly practice, battle drill training and leader/team development during convoy operations. Live training data was collected at the National Training Center, Fort Irwin from convoy lane STX training. Then, in collaboration with NTC observer controllers, SMEs rated team performance on a number of scales (Battle Drills, Following SOP, Situation Awareness, Command and Control, and overall team performance). The system is currently undergoing development and testing, however preliminary results indicate that the DARCAAT system is able to accurately match SME ratings of team performance as well as detect critical events (e.g., "training moments" or performance alarms) in teams. The developed toolset can then be used to provide automated performance assessment for the Observer-Controllers, permitting efficient automation of After Action Reviews.

CONCLUSIONS

Communication is the glue that holds networked teams together. The verbal content of a team's communication provides a window into its performance and cognitive states of the individuals and the team as a whole. The approach described in this paper can convert the communication into specific metrics of performance thereby permitting a better picture of the state of networked teams at any point.

The toolkit allows the analysis and modeling of both objective and subjective metrics of performance and is able to work with large amounts of communication data. Indeed, because of its machine-learning foundation, it works best with more data. The toolkit can automatically extract measures of performance by modeling how SMEs have rated such communication in related situations as well as modeling objective performance measures. Further, because the methods used are automatic and do not rely on any hand-coded of models, they allows performance models to be developed without the large amount of efforts typically involved in standard task-analysis or cognitive modeling approaches. Nevertheless, the approach can still be integrated with traditional assessment methods to develop objective and descriptive models of distributed team performance.

CHALLENGES/NEW DIRECTIONS

There remain a number of challenges to incorporating automated analysis of the content of communication into full-scale operational and training venues. While the results described in this paper use teams from 3 to about 70 soldiers, it is important to determine the challenges for scaling to large scale operations. In addition, there a number of additional technologies that can be included to improve and help generalization in performance. These include better modeling of network structures, incorporation of additional modalities of information (e.g., event and action information), improved computational modeling tools, and leveraging off of additional advances in how to measure performance in complex networked environments.

The automated analysis of communication can be used in a range of applications. These can include applications to monitor teams, give feedback, provide visualizations of information flow, alert commanders for poor performance, as well as be integrated into adaptable training systems which can adjust training based on performance of the team. Finally the overall approach helps understand the role of communication in complex networks. Results from analyses of teams in real-world situations can help understand both how communication affects team performance as well as how performance is reflected through communication. These are critical goals to achieve if we are to better understand performance in modern networked environments (e.g., [12]).

ACKNOWLEDGEMENT

This work was supported in part by grants and contracts from DARPA, ARI, ARL, ONR, and AFRL. The authors acknowledge the contributions of David Wroblewski, Brent Halsey, Tim McCandless, Kyle Habermehl, and Manju Putcha in development and data analyses for the projects described.

REFERENCES

Foltz, P. W., Laham, R. D. & Derr, M. (2003). Automated Speech Recognition for Modeling Team Performance. In *Proceedings of the 47th Annual Human Factors and Ergonomic Society Meeting*.

Brannick, M.T. Salas, E. & Prince, C. (1997) *Team performance assessment and measurement: Theory, methods, and applications*. Mahwah, NJ: LEA.

C.R. Paris; E. Salas; J.A. Cannon- Bowers (2001). Teamwork in multi-person systems: a review and analysis. *Ergonomics* (43:8) 1052-1075.

Landauer, T. K, Foltz, P. W. & Laham, D. (1998). An introduction to Latent Semantic Analysis. *Discourse Processes*, *25*(2&3), 259-284.

Jurafsky, J. & Martin, J. (200) Speech and Language Processing: An Introduction to Natural Language

Processing, Computational Linguistics, and Speech Recognition, New York, Prentice Hall.

Foltz, P. W. (2005). Tools for Enhancing Team Performance through Automated Modeling of the Content of Team Discourse. In *Proceedings of HCI International,* 2005.

Gorman, J. C., Foltz, P. W. Kiekel, P. A., Martin, M. A. & Cooke, N. J. (2003) Evaluation of Latent Semantic Analysis-based measures of communications content. *In Proceedings of the 47th Annual Human Factors and Ergonomic Society Meeting.*

Foltz, P. W., Martin, M. A., Abdelali, A., Rosenstein, M. B. & Oberbreckling, R. J. (2006). Automated Team Discourse Modeling: Test of Performance and Generalization. In *Proceedings of the 28th Annual Cognitive Science Conference.*

LaVoie, N., Psotka, J., Lochbaum, K. E., & Krupnick, C. (2004). Automated Tools for Distance Learning. Paper presented at the New Learning Technologies Conference. February 18-20, 2004. Orlando, FL

LaVoie, N, Streeter, L., Lochbaum, K. Boyce, L., Krupnick, C., and Psotka, J. Automating Expertise in Collaborative Learning Environments. International Journal of Computer-supported Collaborative Learning. Submitted.

Lochbaum, K., Streeter, L., & Psotka, J. (2002). Exploiting technology to harness the power of peers. Interservice/Industry Training, Simulation and Education Conference, Orlando, FL, December 2-5, 2002.

Pierce, L., Sutton, J., Foltz, P. W., Lavoie, N., Scott-Nash, S., Lauper, U. (2006). Technologies for Augmented Collaboration. *Proceedings of CCRTS,* San Diego, CA, July.

Committee on Network Science for Future Army Applications, (2006). National Research Council. ISBN: 0-309-65388-6

AUTHORS

All authors are with Pearson Knowledge Technologies. 4940 Pearl East Circle, Suite 200, Boulder, CO, 80305. Peter W Foltz is the corresponding author:, phone: 303-545-9092, email: pfoltz@pearsonkt.com

QUOTES WORTH PONDERING

Language is not merely a set of
unrelated sounds, clauses, rules
and meanings;
it is a total coherent system of these
integrating with each other,
and with behavior, context,
universe of discourse
and observer perspective.

— Kenneth L. Pike

The properties of a complex
information system are rarely
independent of the processes by which
it has been produced.

The methods used in such system
development processes always
embed social perspectives on values;
on the power structure of the
organization carrying out the process;
on how to treat conflicts; and so on.

— Kristen Nygaard,
Preface to Claudio Ciborra's
The Labyrinths of Information

Social Network Monitoring of Al-Qaeda

Ian McCulloh, Kathleen M. Carley and Matthew Webb

ABSTRACT

Social network monitoring is the application of statistical process control charts to changing social network measures over time. Quality engineers use control charts to detect slight changes in industrial manufacturing processes. Once detected, the quality engineer will identify a maximum likely change point, when the process began to change, and search for the specific cause of the change. These tools allow quality engineers to quickly identify changes before they cause significant financial loss to the manufacturing company. In the same manner, analysts can use control charts to detect slight changes in dynamic social network measures.

A cumulative sum (CUSUM) control chart is applied to a dynamic social network data set of the Al-Qaeda terrorist organization. The data set ranges from 1988 to 2004. The CUSUM identifies a shift in several network measures in the Al-Qaeda network between 2000 and 2001. The CUSUM most likely change point for all measures is 1997. This example suggests that if analysts were to use social network monitoring to monitor terrorist networks, dangerous shifts in the network might be detected before they become a problem. Furthermore, the specific cause of change could be identified, allowing analysts to exploit positive changes in a terrorist organization and mitigate negative changes.

INTRODUCTION

Social network analysis (SNA) is the mathematical methodology of quantifying relationships between individual people or organizations. SNA considers individuals or groups as nodes in a graph, while relationships between nodes are graph edges. There can exist many different types of relationships, such as communication, finance, religion, or nationality. This methodology offers a wealth of potential tools for military intelligence and the war on terror.

The Center for Computational Analysis of Social and Organizational Systems (CASOS) maintains social network data on the Al-Qaeda terrorist network, developed under a research grant from the Office of Naval Research (ONR). This data includes many different relationships to include communication, financial, physical, etc. The data set begins with intelligence collected in 1988 and includes consecutive years through 2004. Using this data and SNA methods, analysts are able to calculate and quantify the most influential terrorists in the network, the most knowledgeable, individuals that connect separate subsections within the group, and much more. While it is important to understand terrorist organizations from an SNA perspective, it does not necessarily identify critical changes in social network structure over time.

Statistical process control charts may be useful in monitoring social networks for important changes over time. Control charts are used by quality engineers in industry to monitor manufacturing processes for changes to important quality characteristics. The quality engineer records observations of a specified quality measure and calculates an appropriate statistic. He then compares the statistic to a control limit. If the statistic exceeds the control limit, the chart is said to "signal" that there may have been a change to the quality characteristic that is being monitored. The quality engineer will then inspect the process to see if it is out of calibration, before the process continues to produce product that is outside quality specifications. He then corrects the process if necessary; and begins to search for the specific cause of the signal. Some control chart algorithms offer an estimate of when the process fell "out-of-control". This saves time in identifying the specific cause of the signal. These same control chart algorithms can be applied to SNA measures observed on networks collected over time. Instead of observing quality characteristics, however, normally distributed network measures are used.

A cumulative sum (CUSUM) control chart is a commonly used statistic in quality engineering that offers an estimate of when the observed process changes. The CUSUM statistic is therefore applied to several normally distributed measures from the ONR Al-Qaeda SNA data from 1988-2004. Using an arbitrary control limit, the control chart is able to successfully predict changes to the Al-Qaeda network prior to their terrorist attacks of September 11th.

CUSUM STATISTIC

The CUSUM control chart is a widely used control chart derived from the sequential probability ratio test (SPRT) (Page, 1961). The SPRT was derived from the Neyman and Pearson (1933) most powerful test for a simple hypothesis. Neyman and Pearson's test statistic is

$$\Lambda_t = \frac{\prod_{i=1}^{t} f(x_i;\mu_1)}{\prod_{i=1}^{t} f(x_i;\mu_0)} \quad . \qquad (2.1)$$

Neyman and Pearson showed that the most powerful test of H_o against H_1 is obtained by rejecting H_o if $\Lambda_t \geq K$ and concluding in favor of H_o if $\Lambda_t < K$, where K is determined by the level of significance, α. The level of significance is the probability that H_o is rejected when it is true.

Wald (1947) demonstrated that the Neyman and Pearson hypothesis testing method could be applied sequentially and could significantly reduce the number of samples required to reach a conclusion. Wald's sequential probability ratio test (SPRT) compares Λ_t to two constants A and B where $0 < B < A < \infty$. Observations are collected and examined one-at-a-time. After the tth observation there are three possible outcomes. If $\Lambda_t < B$, then the test concludes in favor of H_o. If $\Lambda_t > A$, then H_o is rejected in favor of H_1. If $B \leq \Lambda_t \leq A$ then sampling will continue with observation $t + 1$.

The SPRT can be used to test H_o: $\mu = \mu_o$ against H_1: $\mu = \mu_1$ for normal means. Without loss of generality we will assume that $\mu_1 > \mu_o$. Having observed t observations, the SPR is

$$\Lambda_t = \frac{\prod_{i=1}^{t}\left(\frac{1}{\sigma\sqrt{2\pi}}\exp\left(-\frac{1}{2}\left(\frac{x_i-\mu_1}{\sigma}\right)^2\right)\right)}{\prod_{i=1}^{t}\left(\frac{1}{\sigma\sqrt{2\pi}}\exp\left(-\frac{1}{2}\left(\frac{x_i-\mu_0}{\sigma}\right)^2\right)\right)} \quad .$$

This can be reduced algebraically to

$$\Lambda_t = \exp\left(\left(\frac{\mu_1-\mu_0}{\sigma^2}\right)\sum_{i=1}^{t} x_i + t\left(\frac{\mu_0^2-\mu_1^2}{2\sigma^2}\right)\right) \quad . \qquad (2.2)$$

The sequential probability ratio, Λ_t, is compared to appropriate constants A and B as each new observation t is formed. Following observation t, the test concludes in favor of H_o if $\Lambda_t < B$. If $\Lambda_t > A$, then the test concludes in favor of H_1. If $B \leq \Lambda_t \leq A$, then sample $t + 1$ is obtained and a revised Λ_{t+1} is computed. This procedure continues until either $\Lambda_t < B$ or $\Lambda_t > A$.

In a Social Network Monitoring (SNM) application of the SPRT, μ_o is the mean of a social network measure and μ_1 is the mean after a change in the network. Since one would never conclude in favor of H_o that the network is unchanged and stop all sampling, the procedure continues until it signals that there is a change in the network. This implementation of the SPRT procedure leads to the CUSUM control chart.

The CUSUM control chart is based on cumulative sums of a network measure over time and is derived from the sequential probability ratio test (SPRT). In a control chart application of the SPRT, one would continue to monitor the network until $\Lambda_t > A$ when the procedure signals that there is a change in the network. The SPRT leads to the following expression for detecting an increase in the mean of a normally distributed network measure. The procedure would signal when

$$\Lambda_t = \exp\left(\left(\frac{\mu_1-\mu_0}{\sigma^2}\right)\sum_{i=1}^{t} x_i + t\left(\frac{\mu_0^2-\mu_1^2}{2\sigma^2}\right)\right) > A \quad . \qquad (2.3)$$

This expression can be simplified by taking the natural logarithm of both sides of the inequality,

$$\left(\frac{\mu_1-\mu_0}{\sigma^2}\right)\sum_{i=1}^{t} x_i + t\left(\frac{\mu_0^2-\mu_1^2}{2\sigma^2}\right) > \log A$$

This decision rule can be algebraically reduced to

$$\sum_{i=1}^{t} x_i - t\left(\frac{\mu_0+\mu_1}{2}\right) > A'$$

, where

$$A' = \left(\frac{\sigma^2}{\mu_1-\mu_0}\right)\log A \quad .$$

By allowing $\mu_1 = \mu_o + \delta\sigma_x$, the procedure signals when

$$\sum_{i=1}^{t} x_i - t\left(\frac{\mu_0+(\mu_0+\delta)}{2}\right) = \sum_{i=1}^{t}\left(x_i - \mu_0 - \frac{\delta}{2}\right) > A'$$

where δ is the standardized difference in the network measure under H_o and H_1. This decision rule can then be further simplified by using the cumulative statistic

$$C_t = \sum_{i=1}^{t}(Z_i - k) \quad ,$$

where $Z_i = (x_i - \mu_o)/\sigma_x$, and $k = \delta / 2$. The common choice of k in quality applications is 0.5, which corresponds to a standardized magnitude of change in

mean of $\delta = 1$. Thus, observations are examined sequentially until $C_t > A'$.

The CUSUM sequentially compares the statistic C_t against a control limit A' until $C_t > A'$. Since one is not interested in concluding that the network is unchanged, the cumulative statistic is

$$C_t^+ = \max\{0, \quad Z_t - k + C_{t-1}^+\} \quad . \qquad (2.4)$$

If this rule was not implemented the control chart would require more subgroups to signal if $C_t < 0$. The statistic C_t^+ is compared to a constant, h^+. If $C_t^+ > h^+$, then the control chart signals that an increase in a network measure has occurred.

A required assumption for the derivation of the CUSUM statistic is that the network measure under observation is normally distributed. There is still much work to be done in the area of classifying the probability space of a social network. However, the central limit theorem does allow us to understand the distribution of a sample average of 30 or more observations. Therefore, network measures that are averaged over 30 or more nodes will have a normally distributed measure. Some of the measures that have been investigated include the Average Betweenness, Average Closeness, Average Degree, and Average Eigenvector Centrality.

For $\delta < 0$, the SPRT similarly leads to the CUSUM procedure for detecting a decrease in a network measure. In this case,

$$C_t^- = \max\{0, \quad -Z_t - k + C_{t-1}^+\}$$

is compared to a constant, h^-. If $C_t^- > h^-$, then the control chart signals that a decrease in a network measure has occurred.

To monitor for both increases and decreases in the mean, two one-sided control charts are employed. One chart is used for monitoring for increases in the mean of a network measure and the other is used for detecting decreases in mean. If the process remains in-control, $C_t^{\pm}$ will fluctuate around zero. If there is an increase in the mean of a network measure, C_t^+ will tend to increase. Conversely, if there is a decrease, then C_t^- will tend to increase. When $C_t^+ > h^+$ or $C_t^- > h^-$, the two one-sided CUSUM control chart scheme signals that the process is out-of-control.

The CUSUM control chart's ability to detect changes has been extensively investigated in the literature. Lorden (1971) introduced a minimax criteria that minimizes the average number of observations to detect a change, subject to a given probability of false alarms. He also proposed the use of a maximum likelihood approach to rapidly detect changes in a process. Lorden's approach does better than the CUSUM at detecting a wide range of changes in the mean of a process, but does not completely outperform the CUSUM for all potential changes in the process mean.

Moustakides (1986) proved that Page's CUSUM control chart will detect a specific standardized step change in the mean of a measure with fewer subgroups than any other statistical test. The specific step change in mean is a standardized change of $\delta = 2k$, where k is the control chart parameter in Equation 2.4. Therefore, the CUSUM control chart is the best chart to use for detecting a standardized change in mean of $\delta = 2k$. However, other control charts may detect other changes in the mean with fewer subgroups. Several attempts to improve upon the CUSUM control chart have been investigated in the literature. However, the CUSUM is used to demonstrate the general applicability of control charts in dynamic social network analysis, due to its simplicity and versatility.

RESULTS

Social network measures were plotted for number of agents, average degree, average betweenness, average closeness, average eigenvector centrality, and density. Each of these network measures were increasing from 1988 until 1994. The measures then leveled off. There are many possible reasons for this burn-in period, the least of which is the quality of intelligence gathering on Al-Qaeda. For this reason, the average measure and standard deviation were calculated over five years beginning in 1994. The CUSUM control chart was used to monitor the five measures above from 1994 to 2004. Figure 1 displays the plot of the social network measure for the average closeness of members in the Al-Qaeda network. The reference value, k, and the control limit, h, were arbitrarily set at 0.5 and 4 respectively for all of the social network control charts. Figure 2 shows the CUSUM statistic for the average closeness that is plotted in Figure 1. It can be seen that the CUSUM statistic in Figure 2 is a more dramatic indication of network change than simply monitoring the network measure in Figure 1. This is a result of the CUSUM statistic taking into account previous observations of the network. A single observation of a network measure that is slightly higher than normal may not indicate a change in the network. Multiple observations that are slightly higher than normal, however, may indicate a shift in the mean of the measure.

Recall that the CUSUM will either detect increases or decreases in a measure, but not both. Therefore, two control charts must be run for each social network measure being monitored. One chart

Figure 1. Control Chart for the Average Closeness of Al-Qaeda Members

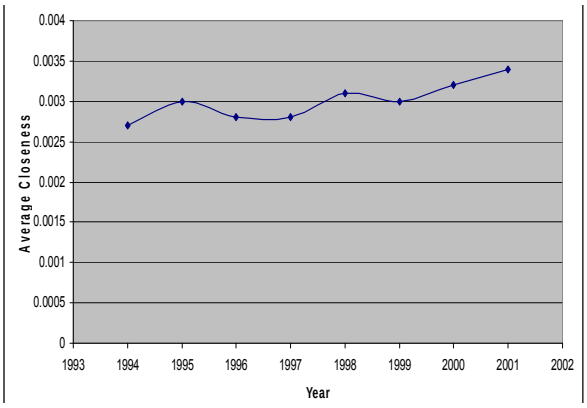
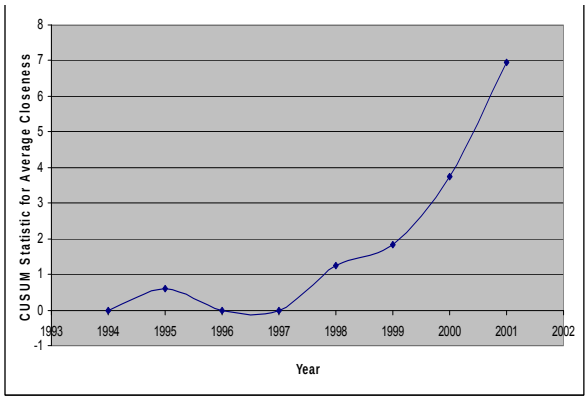


Figure 2. CUSUM Control Chart for Average Closeness of Al-Qaeda



is used for increases and the other chart for decreases. Table 1 displays the CUSUM statistic values for detecting increases in a measure, while table 2 shows the values for decreases in a measure.

The control chart will signal a false alarm after 168 observations on average when the control limit is arbitrarily set to $h = 4$ (McCulloh, 2004). This corresponds to a probability of false alarm of

Table 1. CUSUM Statistic for Detecting Increases in a Network Measure

	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004
Number Agents	0.00	0.00	0.00	0.00	1.19	2.12	3.43	4.99	2.18	0.00	0.00
Average Centrality	0.00	0.60	0.00	0.00	1.19	3.74	6.10	9.24	4.39	0.00	0.00
Average Between-ness	0.00	0.43	0.00	0.00	2.02	3.24	5.26	8.46	5.31	0.00	0.00
Average Closeness	0.00	0.59	0.00	0.00	1.25	1.84	3.74	6.95	3.61	0.00	0.00
Average Density	0.00	0.60	0.00	0.00	1.19	3.74	6.10	9.24	4.39	0.00	0.00

Table 2. CUSUM Statistic for Detecting Decreases in a Network Measure

	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004
Number Agents	0.00	0.00	0.37	0.37	0.00	0.00	0.00	0.00	1.81	6.68	16.48
Average Centrality	0.34	0.00	0.00	0.15	0.00	0.00	0.00	0.00	3.85	12.58	27.15
Average Between-ness	0.00	0.00	0.56	0.72	0.00	0.00	0.00	0.00	2.15	9.07	19.16
Average Closeness	0.37	0.00	0.00	0.00	0.00	0.00	0.00	0.00	2.34	10.57	26.00
Average Density	0.34	0.00	0.00	0.15	0.00	0.00	0.00	0.00	3.85	12.58	27.15

less than 1%. It can be seen in Table 1 that the CUSUM statistic exceeds the control limit of 4 and signals that there might be a significant change in the Al-Qaeda network in either 2000 or 2001 for all five measures. Therefore, an analyst monitoring Al-Qaeda would be alerted to a critical, yet subtle change in the network prior to the September 11 terrorist attacks.

The CUSUM control chart also has a built in feature for determining the most likely time that the change occurred. This time is identified as the last point in time when the CUSUM statistic is equal to 0. For all measures, this point in time is 1997. To understand the cause of the change in the Al-Qaeda network, an analyst should look at events occurring in 1997.

Several very interesting events related to Al-Qaeda and Islamic extremism occurred in 1997. Six Islamic militants massacred 58 foreign tourists and at least four Egyptians in Luxor, Egypt. Coalition forces deployed to Egypt in 1997 for a bi-annual training exercise were repeatedly attacked by Islamic militants. The coalition suffered numerous casualties and shortened their deployment. In early 1998, Zawahiri and Bin Laden were publicly reunited, although based on press release timings; they must have been working throughout 1997 planning future terrorist operations. In February of 1998, an Arab newspaper introduced the "International Islamic Front for Combating Crusaders and Jews." This organization, established in 1997, was founded by Bin Laden, Zawahiri, leaders of the Egyptian Islamic Group, the Jamiat-ul-Ulema-e-Pakistan, and the Jihad Movement in Bangladesh, among others. The Front condemned the sins of American foreign policy and called on every Muslim to comply with God's order to kill the Americans and plunder their money. Six months later the US embassies in Tanzania and Kenya were bombed by Al-Qaeda. Essentially, 1997 was possibly the most critical year in uniting Islamic militants and organizing Al-Qaeda for offensive terrorist attacks against the United States.

Table 2 shows similar results for detecting decreases in network measures. The control chart for all measures signals a possible network change in 2003. The most likely time that this change occurred was 2001, which corresponds to the U.S. invasion of Afghanistan.

CONCLUSIONS

Control charts are a critical quality engineering tool that assists manufacturing firms maintain profitability. This Al-Qaeda example demonstrates that social network monitoring could enable analysts to detect important changes in terrorist networks. Furthermore, the most likely time that the change occurred can also be detected. This paper does not mean to imply that the CUSUM statistic is the answer to social network monitoring. The CUSUM is simply used to illustrate the usefulness of a statistical process control chart for monitoring social networks. There are many other control chart statistics that could be used to monitor a dynamic social network. More research in this area is needed to characterize the nature of dynamic social networks, and to identify what statistics are best to minimize the probability of false alarms and increase the speed of detecting changes.

Future research in social network monitoring should also focus on friendly organizations as opposed to terrorist networks. Although understanding terrorism is an important application of social network monitoring, there is always a great amount of unknown information in terrorist organizations. The terrorist are just not good at filling out the surveys required to understand the true social network. Friendly organizations, on the other hand, provide researchers the opportunity to monitor all social connections, and through surveys and interviews, understand why those connections exist and when they change.

With a better understanding of social network monitoring, there is a wide range of potential applications. Intelligence analysts can better monitor terrorist organizations. Military commanders can have improved situational awareness of their units by monitoring communications among subordinates and linking the communication network to morale and motivation. Civilian business leaders can monitor the success and progress of strategic combinations, such as mergers and acquisitions. Most application areas of dynamic network analysis can make use of social network monitoring to detect and identify changes in a dynamic social network.

ACKNOWLEDGEMENT

This work was supported in part by the Office of Naval Research (ONR), United States Navy Grant No. N00014-02-10973 on Dynamic Network Analysis, the Army Research Labs Grant No. DAAD19-01-2-0009 , the Air Force Office of Sponsored Research (MURI: Cultural Modeling of the Adversary Organization, 600322), and the NSF IGERT program in CASOS (DGE-9972762). Additional support was provided by CASOS and ISR at Carnegie Mellon University. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official

policies, either expressed or implied, of the Office of Naval Research, the Army Research Labs, the Air Force Office of Sponsored Research, the Department of Defense, the National Science Foundation, or the U.S. government.

REFERENCES

Carley, K. M. (2003). Dynamic network analysis. *Dynamic social network analysis: Workshop summary and papers*: 133-145. P. Pattison (Ed.), Washington D.C.: The National Academies Press.

Carley, Kathleen & Reminga, Jeffrey & Borgatti, Steve. (2003). Destabilizing Dynamic Networks Under Conditions of Uncertainty. *International Conference on Integration of Knowledge Intensive Multi-Agent Systems, 2003. IEEE KIMAS, Boston MA*, Boston MA: IEEE KIMAS.

Carley, Kathleen. (2003). Destabilizing Terrorist Networks. *Proceedings of the 8th International Command and Control Research and Technology Symposium. Conference held at the National Defense War College, Washington DC. Evidence Based Research, Track 3, Electronic Publication*, WebSite:http://www.dodccrp.org/events/2003/8th_ICCRTS/pdf/021.pdf

Carley, Kathleen & Lee, Ju-Sung & Krackhardt, David. (2001). Destabilizing Networks. *Connections*, 24(3), 31-34.

Frantz, Terrill & Carley, Kathleen. (2005). A Formal Characterization of Cellular Networks. *Carnegie Mellon University, School of Computer Science, Institute for Software Research International, Technical Report CMU-ISRI-05-109*

Ghosh, B.K. (1970). *Sequential Tests of Statistical Hypotheses*, Addison-Wesley Publishing Company, Inc., Reading, Massachusetts.

Govindarajulu, Z. (1981). *The Sequential Statistical Analysis*, American Sciences Press, Inc., Columbus Ohio.

Lorden, G. (1971). Procedures for Reacting to a Change in Distribution. *Annals of Mathematical Statistics* **42**, pp. 1897-1908.

Lucas, J.M. (1982). Combined Shewhart-CUSUM Quality Control Schemes. *Journal of Quality Technology* **14**, pp. 51-59.

Marquand, Robert (2001). The tenets of terror. *Christian Science Monitor*,18 Oct 2001.

McCulloh, I. (2004). *Generalized Cumulative Sum Control Charts.* Masters Thesis, Florida State University, Tallahassee, FL.

Montgomery, D.C. (1991). *Introduction to Statistical Quality Control*, 2nd Edition, John Wiley and Sons, New York.

Moustakides, G.V. (1986). Optimal Stopping Rules for Detecting Changes in Distributions. *Annals of Mathematical Statistics* **14**, 1379-1387.Moustakides, G.V. (1998). Quickest Detection of Abrupt Changes for a Class of Random Processes. *IEEE Transactions* **44**, pp. 1965-1968.

Moustakides, G.V. (2004). Optimality of the CUSUM Procedure in Continuous Time. *Annals of Statistics.* **32**, (to appear).

Neyman, J. and Pearson, E.S. (1933). On the Problem of the Most Efficient Tests of Statistical Hypotheses. *Philosophical Transactions Royal Society Series A.* **231**, pp. 289-337.

Page, E.S. (1954). Continuous Inspection Schemes. *Biometrika* **41**, pp. 100-115.

Page, E.S. (1961). Cumulative Sum Control Charts. *Technometrics* **3**, pp. 1-9.

Pignatiello, J.J., Jr. and Samuel, T.R. (2001). Estimation of the Change Point of a Normal Process Mean in SPC Applications. *Journal of Quality and Technology*. **33**, pp. 82-95.

Shiryayev, A.N. (1996). Minimax Optimality of the Method of Cumulative Sums (CUSUM) in the Case of Continuous Time. *Russian Mathematics Survey* **51**, pp. 750-751.

Siegmund, D. (1986). Boundary Crossing Probabilities and Statistical Applications. *Annals of Mathematical Statistics* **14**, pp. 361-404.

Topper, Curtis & Carley, Kathleen. (1999). A Structural Perspective on the Emergence of network Organizations. *Journal of Mathematical Sociology*, 24(1), 67-96.

Wald A. (1945). Sequential Tests of Statistical Hypotheses. *Annals of Mathematical Statistics* **16**, pp. 117-186.

Wald A. (1947). *Sequential Analysis,* Wiley, New York.

Wald, A. and Wolfowitz, J. (1948). Optimum Character of the Sequential Probability Ratio Test. *Annals of Mathematical Statistics* **19**, pp. 326-339.

Weiss, L. (1953). Testing One Simple Hypothesis Against Another. *Annals of Mathematical Statistics* **24**, pp. 273-281.

Weiss, L. (1962). On Sequential Tests Which Minimize the Maximum Expected Sample Size. *Journal of the American Statistical Association* **57**, pp. 551-557.

Vance, L.C. (1986). Average Run Lengths of Cumulative Sum Control Charts for Controlling Normal Means. *Journal of Quality Technology* **18**, pp. 189-193.

AUTHORS

Ian McCulloh is a Major in the U.S. Army. He's currently completing a PhD at Carnegie Mellon University.

Kathleen M. Carley is a professor of Computer Science at the Institute for Software Research, Carnegie Mellon University, where she directs the Center for Computational Analysis of Social and Organizational Systems (CASOS).

Matthew Webb is a 2nd Lieutenant in the U.S. Army. He co-authored this paper while a cadet at the U.S. Military Academy, Class of 2007.

FROM THE USMA-ARI WORKSHOP

Information Sources for Improved Social Relationship Discovery

Janet F. O'May and Joan E. Forester

ABSTRACT

Traditional (signal, human, and measurement and signature intelligence) and nontraditional (financial and social context) information and data are equally important to the intelligence analysis process and are required to form actionable intelligence. Two sources of nontraditional data are Web-based news and foreign documents. The U.S. Army Research Laboratory (ARL) is currently conducting research in three areas. The first is to conduct an experiment to test the feasibility of using machine translated documents found during operations to feed Social Network Analysis (SNA) software packages. A second task is the Real-Time News Analysis (RTNA) project. RTNA is being developed to gather real-time streaming data from Web-based news sources and pre-process it by information extraction, categorization, message understanding, concept mining, and fusing. This data will then be fed to ARL's SNA for Army Actionable Intelligence (SNA3I) project. This third project is developing a test bed of currently available SNA software and working on enhanced algorithms and visualization techniques to improve relationship discovery.

INTRODUCTION

Command and control are the procedures used to organize and direct armed forces to successfully complete a mission [1]. When an order is issued, the tasks necessary to carry out the mission are devised by the Commander and staff. The S2, part of the Commander's staff, is responsible for preparing an intelligence estimate, and analyzing data to understand the social climate of the area of operation. Cultural and social information, such as economic, psychological, political, and religious factors of the population, are required. As the U.S. Army moves away from traditional methods of warfare and moves to operations other than war, the cultural make-up of an area becomes more critical. In addition to traditional sources of data such as human, sensor, and imagery information, real-time data could benefit the intelligence estimate process. The World Wide Web contains large amounts of non-traditional data and could augment traditional sources for intelligence analysis. Additionally, documents found in the field may be translated and reviewed for any pertinent data to the mission or operation.

The large amount of data accessible from the World Wide Web would overwhelm most Intelligence Officers. Generally, the operational tempo of current military missions does not allow enough time to process the amount of data typically available on the World Wide Web. The information must be filtered and consolidated. Also once an Intelligence Officer has the data, techniques and methodologies must be available to transform the data into meaningful knowledge.

BACKGROUND

The U.S. Army Research Laboratory (ARL) currently has three projects in the Intelligence arena. The first is the Real-Time News Analysis (RTNA) project. Current data from news sources and web logs (blogs) may enhance traditional intelligence data. RTNA is being developed to harvest real-time streaming data from world web-based news sources and pre-process it by filtering, classifying, tagging, and fusing. The data, now transformed to knowledge, is ready for interpretation using ARL's Social Network Analysis (SNA) for Army Actionable Intelligence (SNA3I) project. SNA3I is looking at methods to take this knowledge and apply it to varying SNA software packages based upon the type of data and the required information. Algorithms must be developed to provide heuristics for determining the correct SNA software package to provide the most comprehensive analysis. ARL is not trying to develop SNA software but to utilize software currently available to better suit the needs of the Intelligence Community. Additional work will be completed on improving the visualization of the data from the SNA packages.

A third related project will be conducting an experiment in the summer of 2007 to determine if foreign language documents found during military operations can be used to also increase actionable intelligence. This experiment will be conducted by student contractors working at ARL and explores the use of machine translation for SNA.

The goal of these projects is to increase the amount of current data available to an S2 or Intelligence Analyst and then provide the best overview of the data for further analysis. However, just increasing the amount of data could prove detrimental to the Intelligence Analyst. ARL is committed to providing more data and also ensuring that the data will be properly stored with appropriate tagging for easy retrieval. The data will be collated with similar information. This paper discusses the reasoning behind the three ARL projects, their interrelationship, and possible future work.

REAL-TIME NEWS ANALYSIS (RTNA)

A. Overview

The goal of these projects is to increase the amount of current data available to an S2 or Intelligence Analyst and then provide the best overview of the data for further analysis. However, just increasing the amount of data could prove detrimental to the Intelligence Analyst. ARL is committed to providing more data and also ensuring that the data will be properly stored with appropriate tagging for easy retrieval. The data will be collated with similar information. This paper discusses the reasoning behind the three ARL projects, their interrelationship, and possible future work.

The RTNA project is to be a networked service for multiple projects, one of which is the SNA3I project. RTNA will be a complete system that locates news stories, extracts text data, pre-processes the data, and creates a repository for easy retrieval. RTNA will support three target audiences – the Soldier in the field, the Intelligence Analyst or S2, and the laboratory researcher.

RTNA will address three types of data. The first type is actionable data, or knowledge. This is data that is timely and meaningful and has gone through extensive processing. The target audience for this data is a Soldier in the field. For example, a Soldier would request a piece of information through an application programming interface (API) similar to the familiar Google query. RTNA would then search for applicable news sources. However, this is not meant to be just another search engine. RTNA will provide a user-directed feature that will allow a Soldier to better describe data requirements. The graphical user interface's (GUI) capability will allow a user to enter parameters to tailor the search. Possible parameters include: geographic areas of interest; characteristics (such as social, economic, or political); dates to restrict the search to a specific time period; multiple key words; and selection of preferred news sources.

The second type of data is reference data, or information to include data that has been partially processed. This would be a large set of pre-processed pertinent news stories that have been filtered and tagged. RTNA has been collecting news stories since the summer of 2006 based upon key words. This collection will be text mined to serve as a baseline repository. The tagging process will incorporate a generic methodology, such as extensible markup language (XML), to allow ease of loading into disparate software packages. A future direction will increase usability by adding different methods of tagging or organizing the data to fulfill specialized software requirements. The reference data will provide a large repository to be readily available for researchers and Intelligence Analysts.

The third type of data is comprised of all pertinent unprocessed news stories. This is a future direction and the data for this repository will be collected in real-time using Web crawler software. "A Web crawler (also known as a Web spider or Web robot) is a program or automated script which browses the World Wide Web in a methodical, automated manner [2]." The web crawler will interrogate available news sources to obtain data that benefits the analyst or researcher. The web crawler would be trained to access U.S. news sites along with other English language sources.

B. Process

The RTNA process is comprised of several steps. The first step is to locate news stories, this is accomplished through 1) a Google API based upon a user-defined query, 2) alerts that forward articles as they are posted to news sites, or 3) the use of a web crawler that searches out and retrieves the stories.

The second step is the actual news extraction. This is first accomplished by retaining only the pertinent information from a web page. A news web site will contain more information than just the actual story, e.g., advertisements, links to other stories, site banners, graphics, pictures, or video clips. This extraneous information is removed to just leave the text of the story. The news extraction process also includes identifying duplicate or similar stories. As only one instance is needed, RTNA will incorporate heuristics to assure that the selected news story has all the information contained in the duplicates. After the "best" story is selected, it will be saved in text and XML formats. A future enhancement will store and cross-reference all the duplicate stories for further analysis.

The third and final phase is multi-level knowledge extraction from the saved stories and can in-

volve multiple processes. One process is text mining. "Text mining usually involves the process of structuring the input text (usually parsing, along with the addition of some derived linguistic features and the removal of others, and subsequent insertion into a database), deriving patterns within the structured data, and finally evaluation and interpretation of the output. 'High quality' in text mining usually refers to some combination of relevance, novelty, and interestingness. Typical text mining tasks include text categorization, text clustering, concept/entity extraction, sentiment analysis, document summarization, and entity relation modeling (*i.e.*, learning relations between named entities) [3]." Other processes for possible application include: parsing, tagging, filtering, and fusing the data. The processes employed will be dependent upon how the data will be used and what software packages will be receiving the data.

Individual steps in the RTNA project are currently being undertaken by other software packages and developers; however RTNA's goal is to combine all of these steps within a single data-creation process. The process is being designed as a fully automated service with no human interaction necessary. Gathered text data will be saved in a generic format to be accessible by disparate applications.

SOCIAL NETWORK ANALYSIS (SNA) FOR ARMY ACTIONABLE INTELLIGENCE (SNA3I)

A. SNA

The Army has changed the way that it operates. It no longer fights in large tank-on-tank conflicts, but can be involved in asynchronous warfare and rebuilding and humanitarian efforts. Military mission completion relies on the Commander's and the staff's ability to understand the cultural and social climate within their area of operation. The cultural climate of a region is just as important as traditional factors such as terrain and weather. The S2 must be able to access the most up-to-date information in order to provide information to the Commander in the operations planning stages.

RTNA will provide data, however data only has value if it fulfills the intelligence requirements so it will be used to provide data to SNA3I. Actionable intelligence is defined as "having the necessary information immediately available in order to deal with the situation at hand [4]." As the Army is placed in situations dependant upon knowing as much about the population in areas of operation as possible, information on social contacts must be quickly and reliably obtained.

SNA examines the relationships between people and how they communicate and interact. An offshoot of SNA is dynamic network analysis (DNA) which "varies from traditional social network analysis in that it can handle large dynamic multi-mode, multi-link networks with varying levels of uncertainty [5]." Knowing which groups of the population are connected and providing a basic understanding of who can be "trusted" will be invaluable to not only the Soldier on the ground but also to the Commander and staff in planning operations. ARL is working to incorporate DNA into improved mission planning.

B. SNA3I Status

ARL's SNA3I project started in fiscal year 2007 and is comprised of three tasks. The first task is investigating the employment of concept maps for improved tactical intelligence. "Concept maps offer a method to represent information visually… Concept maps harness the power of our vision to understand complex information 'at-a-glance [6].'" ARL is partnering with the Institute for Human and Machine Cognition (IHMC) at the University of West Florida. Using IHMC's software, Cmap, ARL is exploring the feasibility of creating concept maps that will enhance the military decision making process within scenarios.

A second task is exploring the use of machine translated documents to feed SNA software packages. This process will be tested in an upcoming experiment and will be addressed in Section V.

The third task is applying DNA for actionable intelligence. This uses existing SNA software to process data. The initial subtasks include setting up a SNA test bed, exploring methodologies for improved algorithms to uncover social relationships, building APIs to access disparate software, and investigating visualization techniques to improve software output. ARL will be enhancing existing software to adapt for military intelligence applications.

C. SNA3I Test Bed

ARL is creating a software test bed to evaluate SNA packages. The process began summer of 2006 with a preliminary examination of existing packages. Ms. Ashley Foots, a student under the George Washington University apprenticeship program, performed an initial review of free and low cost SNA packages. Based upon her recommendation, two packages have been incorporated into the test bed. More packages are to be added and evaluated in the future. Work is beginning on how to match SNA software packages to best fit the available data. Heuristics will be developed to fit data with

software and to provide the most effective visualization based upon the software output. This future work will involve close contact with Intelligence Analysts and S2s to ensure that the enhancements developed in the laboratory benefit the intelligence analysis process through SNA software selection and output display.

Work is also underway to develop three dimensional graphics for better understanding of relationships. Currently most SNA software provides a two dimensional network map of relationships. ARL is exploring methodologies and techniques to better display the relationships uncovered through the SNA process using three dimensional representations.

SNA AND MACHINE TRANSLATED DOCUMENTS

This project grew from the hypothesis that if a Soldier in the field obtains documents and sufficient translation capabilities exist, the text from these documents can be sent to SNA software packages. The SNA software will provide actionable intelligence if given valuable translated text.

ARL participates in the George Washington University Science and Engineering Apprentice Program (SEAP). SEAP provides an opportunity for students to work in a research environment. ARL will be using students to conduct an experiment this summer to test the above hypothesis. The students will first obtain foreign documents. The documents will be translated by two methods – human and machine. Each document ideally will be translated by four or five machine translators and two humans.

The documents will then be processed using the AutoMap and Organizational Risk Analyzer (ORA) software developed by Carnegie Mellon University. AutoMap is used to text mine the documents and ORA will display relationships uncovered in the documents. AutoMap and ORA results will compare the human to the machine translated documents. The experiment will also evaluate if any pertinent relationships were uncovered by employing the software packages.

The study will seek to determine two conclusions. The first is: will current machine translators be able to reliably translate found documents? And secondly, will the documents reliably serve as input to SNA packages to garner actionable intelligence? Results of the experiment will be published after completion.

CONCLUSION

A basic understanding of the cultural climate of an area of interest is critical to mission success. The practice of bringing in large formations of armored equipment and air support to win a conflict is no longer applicable in the current world environment. Careful attention must be paid to understand nuances previously overlooked such as the cultural and social features of an area. Analysts must be able to quickly gather and evaluate large amounts of data to provide the Commander necessary information to understand the area of operation. The RTNA and SNA3I projects are working jointly to obtain large amounts of current data from World Wide Web news sources, process the data, and then provide the appropriately formatted data to SNA software and visualization routines for a quick and concise overview. The machine translation project is determining if documents found in an area of operation can be translated successfully and then be used to provide additional intelligence data. If the Analyst has a clearer picture of the current social climate, it is then possible to provide better information to a Commander to improve mission effectiveness [7].

ACKNOWLEDGMENT

The authors wish to acknowledge members of the SNA and RTNA teams for their contribution to this effort: Mr. Andrew Neiderer, Dr. John Brand, Mr. Richard Kaste, Mr. Eric Heilman, Mr. John Richardson, Ms. Ashley Foots, and Ms. Michelle McVey.

REFERENCES

Command and Control definition, http://www.army-technology.com/glossary/command-and-control.html, accessed 19 December 2006

Definition from Wikipedia, http://en.wikipedia.org/wiki/Web_crawler, accessed 21 December 2006.

Definition from Wikipedia, http://en.wikipedia.org/wiki/Text_mining, accessed 21 December 2006.

PCMAG.com encyclopedia, http://www.pcmag.com/encyclopedia_term/0,2542,t=actionable+ intelligence &i=37443,00.asp, accessed 22 December 2006.

K. M. Carley, Dynamic Network Analysis, Institute for Software Research International, http://www.si.umich.edu/stiet/researchseminar/Winter%202003/DNA.pdf, accessed 22 December 2006.

Introduction to Concept Maps, http://classes.aces.uiuc.edu/ACES100/Mind/CMap.html, accessed 22 December 2006.

J. Forester and J. O'May, "Real Time News Analysis for Improved Social Relationship Discovery," proceedings of the 12th International Command and Control Research and Technology Symposium, June 2007.

AUTHORS

The authors are affiliated with the Army Research Laboratory's Computational and Information Sciences Directorate.

A Methodology for Simulating Net-Centric Technologies: An Operations Research Approach

Joshua Lospinosa

ABSTRACT

Captured enemy documents, also known as 'CED', are vitally important to today's Army. With the capability to fill vital intelligence requirements, CED help Army units accomplish their missions and corroborate enemy prisoner of war interrogations. The language instant screening tool (LIST) technology being produced at the United States Military Academy provides a net-centric solution to expedite Army doctrine as outlined in Field Manual 34-52. When modeling CED reporting procedures from FM 34-52, this study finds that LIST technologies could facilitate a net-centric enabled intelligence and information structure that is able to reduce dissemination times to a level that were previously unobtainable. The intent of this paper is to provide a methodology whereby further operations research may be conducted to support a net-centric tool suite that will ultimately benefit today's Army.

INTRODUCTION

The advent of the Micro PC into mainstream computing through such companies as Sony prompted cadets [1] at the United States Military Academy to create the LIST project. LIST, which stands for Language Instant System Translation, is an attempt at facilitating the collection, reporting, interpolation, and dissemination of information contained in a captured enemy document, or CED. Since the Micro PC's form factor is conducive to transport by personnel within a company, LIST offers a network centric tool which promises to revolutionize CED collection.

Through the use of a camera, GPS data, and a series of interoperated programs, LIST allows a soldier to take a picture of a machine printed document in any language (currently being developed in Arabic), index it for keywords through advanced latent semantic text analysis, append metadata (GPS, date-time, keywords, unit), and relay the information to higher in near real time. Latent semantic text analysis will allow automated screening of CED, effectively pushing exploitation capabilities down to lower echelons. While this capability has the capacity to revolutionize the Army's information structures, network centric principles indicate that organizational adaptation must accompany technological advancement.

PURPOSE OF RESEARCH

The principles of operations research entail comparison of performance measures and values against costs; but what performance measures matter? When deciding on purchasing the LIST technology, an Army unit must evaluate more than just the ease in which LIST makes reporting CED. For without a rigorous and thorough analysis of how far the implications of LIST technology reach, decision analysis falls short.

To mitigate this potential bias, research must be conducted to evaluate not only the specifications of LIST technology (report time, processing time, battery life, etc.), but also how well LIST fits into the organizational norms, standard operating procedures, and structural considerations. For example, LIST technology promises to increase information velocity and decrease the effect of CED's perishable nature; however, if CED begins to pile up without thorough analysis and exploitation, what has really changed?

Furthermore, rigorous analysis of organizational performance permits policy recommendations beyond simple acquisition decisions as exemplified in current command and control methodologies [2]. As a result, it becomes increasingly evident that fruitful research will illuminate how LIST technology interacts with these methodologies.

The scope of this research project is to provide methodology and guidelines for further study. Ten active Army divisions, with varied CED processing capabilities, provide a challenge in mathematical modeling. Operations research requires close collaboration with decision makers; with so many configurations and stakeholders involved, this research project provides no directly applicable solutions. The methodology, however, promises a strong platform for further adapted studies.

BACKGROUND

In support of the Office of the Secretary of Defense, Office of Force Transformation, a Network Centric Operations case study [3] used inference chains from the NCO Conceptual Framework to analyze an order of magnitude increase in a team

effort to demonstrate force effectiveness. In another team effort [4] the Department of Computer Science at Texas A&M University published the results of battlefield simulations under NCO concepts in Simulating Teamwork and Information-Flow in Tactical Operations Centers using Multi-Agent Systems. By extending smaller scale distributed battlefield simulations like ModSAF and JANUS, the team created the TaskableAgents architecture to model human-decision making at the battalion and above level.

Clearly, the Army is interested in utilizing simulations to make good decisions on incredibly complex implementations. Unfortunately, the intelligence community has not benefited from a rigorous analysis of the captured enemy documents cycle. Army doctrine provides an invaluable platform for conducting an analysis of LIST technology. The US Army Field Manual on Interrogation (FM 34-52), Chapter 4, will provide the guidelines of this study. Standard agreement (STANAG) 2084 defines a captured enemy document, or CED as "any piece of recorded information, regardless of form, obtained from the enemy, which subsequently comes into the hands of a friendly force." CED are typically captured from enemy locations or dead, and they are rarely produced from willing sources. When enemy prisoners of war are taken, CED collected from the area are invaluable in corroborating human intelligence in the intelligence cycle. When an EPW is taken, CED physically travel with him to the appropriate echelons.

When no enemy prisoner of war (EPW) is taken and CED is collected, it is forwarded to the nearest Document Exploitation (DOCEX) center. These DOCEX centers are geographically dispersed and few in number—"[DOCEX centers] are normally organic to major [NATO] commands." CED of this nature typically generate 525 to 5,300 sources per division per week. This astounding range and number makes thorough and timely evaluation of CED impossible.

CED are categorized into 4 compartments depending on their contents. Unless previously arranged, assets required for classification of CED are reserved at the corps level. Category A documents contain spot reportable information on enemy composition, disposition, and aid in accomplishing friendly missions. Category B documents contain secret information on cryptology and communication information. Category C documents help with general intelligence, and Category D documents are of no value.

PRESENT-DAY CED HANDLING

Captured CED undergo accountability at the time of capture. The frontline unit responsible for acquiring the CED append a captured document tag (CDT) to the document which includes date-time groups, location, capturing unit, identity, and circumstances. Since CED are time sensitive, the value must be exploited as quickly as possible. The CED is then physically transported as quickly as possible to higher echelons. The following timeline is then adhered to:

1. Battalion S2 shop ensures that all untagged CED are reconciled, and performs DOCEX if possible, but places priority on expediting to brigade.
2. Brigade assigns escorts to each battalion's CED and physically transports the documents to the Division level. An IPW team can be assembled to glean whatever DOCEX information available. This team focuses on information pertinent to EP interrogation.
3. MP escorts all CED from division to corps. A Division IPW section performs functions similar to the Brigade IPW.
4. The Corps CED team is the first to screen incoming CED for intelligence value. After batching CED into categories, the Corps CED team transports the CED to the combined-corps interrogation facility.
5. The CCIF provides a CIF DOCEX element. This element attempts to produce meaningful SALUTE reports and fill corps information requirements. Based upon the category of the CED, the CED is routed to the appropriate theatre asset.
6. Theatre Document Examiners perform final screening of CED before they are stored or disposed of.

A thorough description of all steps in the CED exploitation doctrine is available from FM 34-52. Accountability and logging of CED is a Accountability and logging of CED is a redundant and tedious process. Doctrine provides a flexible architecture for exploitation. If a battalion or brigade has the capacity to translate a screened CED, it does so and attaches a translation report. Three types of translations exist. A full translation is time-intensive and requires manpower sufficient to complete the task. It is unlikely that this kind of analysis can be performed below the corps level. Extract translations require a full translation of only a portion of a document. Summary translations still require a full

read through of a document, but only require the main points to be conveyed as output. To reduce redundancy, exploitations (translations) of CED are physically attached to the document.

Evacuation procedures for CED are conducted through the intelligence chain of command. Competence is of high importance here—a subordinate unit such as a Brigade must make an intelligent assessment of the CED based on limited exploitation capabilities and either exploit the CED at their level or decide to evacuate it to division level. Categorization is important for document triage.

Finally, when a CED is associated with an EPW, the process must be modified significantly. An EPW's cognitive capacity to retain valuable information diminish significantly with time—quickly forwarding him to the Corps level for interrogation takes priority over screening the CED associated with him.

Methodology for Analysis

Previous empirical research involving Network Centric Operational (NCO) concepts can be extended to CED processing to create an interoperable simulation package. However, the modeling of CED flow within an organization is required. With only doctrine to work with, extrapolating models for information structures within organizations as large as a theatre is impossible without empirical research. This research project, therefore, provides a methodology for interpolating this empirical research into a powerful decision making and simulation tool.

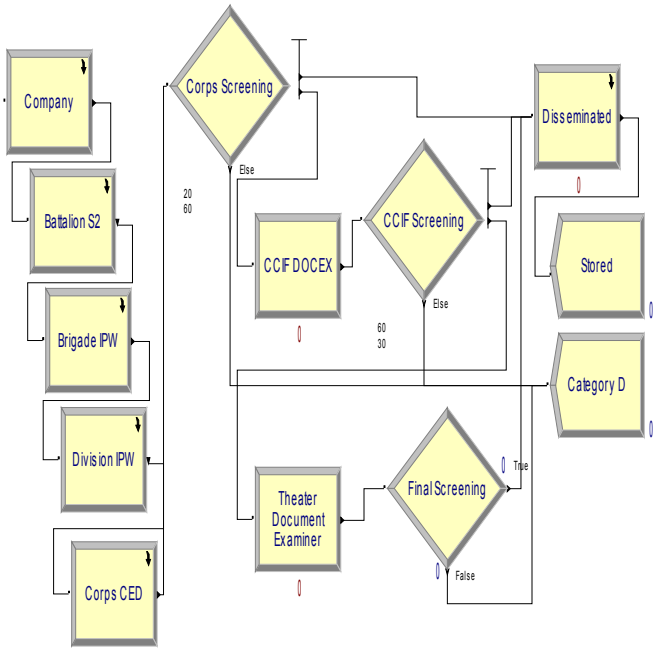
Using industry standard simulation software, mathematical statistics, and statistical regression, this research project will effectively allow decision makers to quantify aspects of information dissemination time, organizational work load, and information reliability. The first step is to define the organizational information structures. After establishing standard operating procedures (SOP's) for CED processing, the methodology requires statistical inputs. The rigorous nature of industry standard simulation software and mathematical statistics allows for virtually any random variable input. The second step is to model these random variables; such considerations include spatial separations between units, translation time, frequency of CED, categorical probabilities, time sensitivity, translation capabilities, translation requirements, and others. The third step involves data collection and statistical regression, which provides the capacity of natural experimentation required to produce an effective model.

With an effective model, the final step is to analytically solve for functions of these random variables within the defined organizational structure. If mathematical statistics fails to provide an analytical solution, simulation techniques can be used effectively to produce metrics which a decision maker can use to decide among alternatives.

Empirical Framework and Results

To illustrate the power of this architecture, this research project models three separate infostructure organizations: present day, present day with LIST functionality, and a proposed infostructure guided with a selective control C2 philosophy using LIST functionality.

Rockwell's Arena Simulation package provides a powerful architecture for modeling complex organizational processes. To model the flow of CED throughout a Theater info-structure, feasible mathematical values were postulated as random variable parameters. The following flowchart shows the complexity of the Theater CED info-structure:



After running years worth of simulations in a few hours, Arena was able to determine that, based on feasible random variable parameters, the current system performs moderately well; the average time to dissemination was 23.72 hours.

Having established a reasonable flow chart, we can estimate the simulations outcome using mathematical statistics. Since the Gamma function allows widely flexible curvature and a relatively simple composition, it is used extensively throughout the simulation. Note, however, that further empirical work could uncover the true underlying distributions of the random variables used in this simulation. The following table shows the random variables utilized in the simulation and their associated parameters:

Random Variable	α	β	Avg. Time	Var.
CED Frequency (at company	1	2.1	2.1	χ
Company Process Time	1	2.1	2.1	δ
Battalion Process Time	2	2.1	4.2	ε
Brigade Process Time	1	2.1	2.1	θ
Division Process Time	1	2.1	2.1	γ
Corps Process Time	2.5	2.1	5.25	η
CCIF Process Time	2	2.1	4.2	ι
Theatre Process Time	1	2.1	2.1	φ

If we assume independence among these random variables, the moment generating function technique allows us to compose summations of random variables through the product of moment generating functions. The moment generating function of a gamma-distributed random variable is the following:

$$m_g[t] = (\beta \cdot t)^{-\alpha}$$

Because we have chosen random variables with equal β parameters, composing the function for total time (κ) is trivial:

$$\kappa = \delta + \varepsilon + \phi + \gamma + \eta + \iota + \varphi$$

Using the MGF technique, the following function is the MGF of κ=

$$m_{g,k}[t] = (1 - \beta \cdot t)^{-\delta+\varepsilon+\phi+\gamma+\eta+\iota+\varphi}$$

Recognizing that this is simply another gamma function, κ is distributed Gamma with

$$\alpha = \delta+\varepsilon+\phi+\gamma+\eta+\iota+\varphi$$

and the same β of the other random variables. Using the parameters supplied, the PDF for total time is the following:

$$f[x] = \frac{1}{2.1^{11.5}\Gamma[11.5]} x^{10.5} e^{\frac{-x}{2.1}}$$

The expected value of κ is 24.15, validating our simulation. Since the mathematical statistics used here does not include the ability of corps and some division level assets to exploit documents, the expected value is upward biased (too large). Further empirical studies could prove to make these parameters fit present day organizations.

LIST Infusion

Since LIST technology promises to decrease the time it takes for companies and battalions to relay information to higher, it is clear that the expected values of company processing time and battalion processing time will decrease drastically. Since semantic text analysis promises to automate the process of summary translation, document triage will decrease the amount of time it takes for documents wait in queue—more Category D documents can be separated from the important CED. This indicates that the rest of the processing times will fall as well.

The following notional values are used in the simulation of List Infusion:

Random Variable	α	β	Avg. Time	Var.
CED Frequency (at company level)	1	2.1	2.1	χ
Company Process Time	.2	2.1	0.42	δ
Battalion Process Time	.5	2.1	1.05	ε
Brigade Process Time	.75	2.1	1.575	ϕ
Division Process Time	.75	2.1	1.575	γ
Corps Process Time	2	2.1	4.2	η
CCIF Process Time	1.5	2.1	3.15	ι
Theatre Process Time	.75	2.1	1.575	κ

Simulating the exact same flowchart over the same period of time verifies this fairly obvious hypothesis—LIST could decrease expected exploitation time of CED to 11.11 hours and decrease time sensitive CED loss to less than 1%. The analytical solution provides an expected time of 13.545 hours, verifying the simulation (again with an upward bias).

Consequently, LIST could half the CED transporting time. There are, however, limitations to this simulation. The first and most obvious limitation is that the parameters used in simulation are purely hypothetical. Empirical research and linear regression would be necessary to estimate these parameters accurately through a process called bootstrapping. Next, CED with an EPW attachment does not benefit from LIST nearly as much as CED collected from an enemy body or abandoned location. Since the CED is used only to corroborate interrogation of an EPW, it is not as useful to electronically send copies of the CED around the infostructure. It could, however, be useful for aiding interrogators at the Corps level and expedite the interrogation process.

Net-Centric Infusion

The final stage of analysis includes modifying the flowchart to reflect selective control C2 architecture. The concept here is the utilization of LIST as a small part of a greater net-centric force enabled with information age technology. In researching the Net-Centric phenomena, we see in Moxley's formula [5] that information in a network is a function of methodology and domains:

$$M[d,b] = N_k$$

The most important concept behind this fundamental relation is that, as we have seen, network analysis is focused on empirical analysis of the physical aspects. Network science relies on a principled approach to the primordial components of networks as they manifest themselves wherever they exist, whether they are physical, social, or biological.

Moxley's Network Science Taxonomy compares our current knowledge base on these network domains. To date, we have a higher level of physical networks such as wireless internet and telecommunications. Unfortunately, relatively little is known about the social and information domains. These latter domains entail precisely what must be fundamentally modified in the CED reporting process and the Army's infostructure in general.

The value creation process is of utmost concern in the operations research field. Through breaking down the value creation process into its individual parts, analytical methods can garner information about the contributions of each node to the overall effectiveness of an organization. With the addition of nodes into an effective organization, Metcalfe's law dictates that the value of the network increases exponentially. The following proportion illustrates this relation, where V is value in the network and n is the number of nodes connected to it:

$$V \text{ proportional to } n^2$$

Because CEDs represent knowledge within the network, this relation manifests direct applicability to future organizational changes to Army infostructure.

Virtual organizations have exploited this phenomenon with great results. Because the importance of physical location is diminished, virtual collaboration and virtual integration allows economies of scale to be achieved.

Army organizations can achieve full spectrum dominance through a superior information position. The challenge arises in command and control; how will an Army organization apply the relatively abstract concepts of value creation, virtual collaboration, and information superiority while conserving the redundancy, security, and interoperability that is integral in a robust Army organization?

The answer to this question is still the subject of hot debate within decision makers in the Army. Many competing philosophies exist on the subject. Dr. David S. Alberts and Richard E. Hayes have postulated on the subject extensively. Their publication, *Understanding Command and Control*, provides the basis for understanding this tradeoff. While traditional notions of Command and Control exist, they are correct in the doctrinal sense in that in order to fully understand C2, it is necessary to overstep the boundaries of conventional thinking.

This paper provides a methodology for analyzing decisions involving Net-Centric adaptations; the analytical and simulations-based techniques covered here cannot hope to solve the complex issues involving the C2 tradeoff quagmire. Nonetheless, a fully Net-Centric CED system would be seamlessly integrated with a larger intelligence network within the Department of Defense. To eliminate separate processes which exist within the current stove-piped architecture, a solution may include the following notional architecture for CED reporting:

1. A front line company acquires CED. Using LIST technology to append metadata such as time, location, unit, and keywords (through semantic text analysis), the company intelligence NCO relays the CEDs electronically to the Battalion S2.
2. Within moments, the Battalion S2 is able to

perform more processor-intensive analysis on the document in an attempt to provide DOCEX within an hour of CED acquisition. At the same time, the electronic CED is posted to a Theatre-wide server where combined-corps level assets are assigned to full or extract human translations.

3. These high echelon assets are optimally assigned to CED within hours based upon keywords gleaned by semantic text analysis.
4. Dedicated personnel from the battalion to the theatre continually monitor the Theatre-level server for potential Category A-C documents and exploit those documents, appending findings to the metadata.

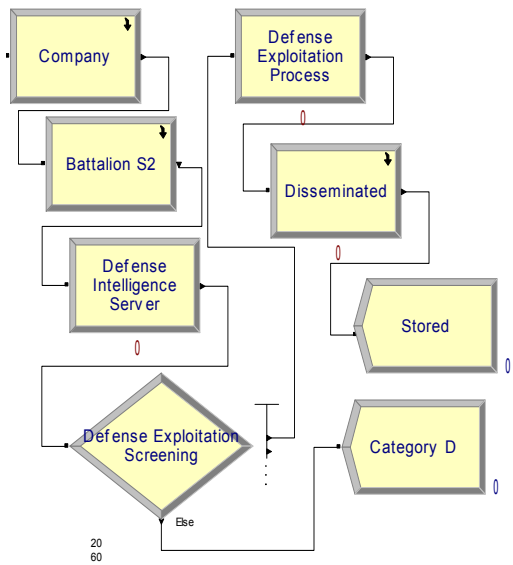
Because the top-down hierarchy paradigm is completely thrown out here, competence at all levels is of utmost importance. Skilled intelligence personnel will be relied upon to make accurate and intelligent assessments CED available on the server. Through centralizing the information available to subordinate units, the theatre commander permits collaborative effort without redundancy in order to maximize efficiency. Based upon keywords, leaders at all levels have access to pertinent PIR and CED by pulling information off of the server.

Posting CED onto a server is limited only to bandwidth considerations and the processing time required by LIST. Since the previous simulation measures expected time to dissemination, this new architecture could reduce a 20 hour process into a half-hour process. Analytically, this process is akin to eliminating the brigade through theatre processing times.

Arena still provides a good tool for analyzing this architecture. Through removing the stove piping under current doctrine, a highly interconnected network of intelligence analysts can access a cornucopia of information virtually without being fettered by geographical limitations. To simulate this, the following notional values will be used:

Random Variable	α	β	Avg. Time	Var.
CED Frequency (at company level)	1	2.1	2.1	χ
Company Process Time	.2	2.1	0.42	δ
Battalion Process Time	.5	2.1	1.05	ε
Exploitation Assets Available	100 (fixed)			
Exploitation Time	1	2.1	2.1	λ

Mapping this organization in Arena is also a simplified process:



Economists strive to achieve perfectly efficient systems. When scarce resources are not allocated in the best way, the system is inefficient. This Net-Centric network represents a perfectly efficient system. Because no translator will ever be idle when an important CED needs to be exploited, the optimal configuration has been achieved. The results are impressive: given these notional inputs, CEDs are processed within 3.852 hours of being captured.

Variance and Risk

The mean time to dissemination provides a good measure of the expected efficiency of an information structure. However, a rigorous operations research analysis requires a look at variability. Variability manifests itself in two main aspects of this paper's analysis. Firstly, the notional random variable distri-

scarce resources are not allocated in the best way, the system is inefficient. This Net-Centric network represents a perfectly efficient system. Because no translator will ever be idle when an important CED needs to be exploited, the optimal configuration has been achieved. The results are impressive: given these notional inputs, CEDs are processed within 3.852 hours of being captured.

Variance and Risk

The mean time to dissemination provides a good measure of the expected efficiency of an information structure. However, a rigorous operations research analysis requires a look at variability. Variability manifests itself in two main aspects of this paper's analysis. Firstly, the notional random variable distributions have assumed a constant beta term (β), which is often referred to as the shaping parameter. It is highly unlikely that the shaping parameters are equal among these distributions.

The beauty of the gamma distributed random variable is its flexibility; but how does having different shaping parameters affect analysis? For the simulations, nothing changes. The moment generating technique, however, is significantly more complicated. Instead of having a nice underlying distribution for the time to dissemination, the distribution is probably unknown. The moment generating function technique provides a solution:

$$m_g[t] = \left(\sum_{i=0}^{n} \beta_n \cdot t\right)^{-\sum_{i=0}^{n} \alpha_n}$$

By finding the first derivative with respect to t of the function above, the first moment of the function is found. Because the first moment of any function is the mean, we have found the expected value. If the random variables of interest are independent, this technique is applicable to any combination of random variable distributions with known moment generating functions. Simply multiplying these functions together will yield the moment generating function of the desired exploit time distribution.

Variation is important for the individual random variables comprising the time to dissemination, but knowing the variation of exploit time is equally important. Finding this variation is available through the simulations, or through finding the second moment of the underlying distribution (the second derivative with respect to t).

The variability of time to dissemination can tell a decision maker the risk involved with the organization under consideration. It may be desirable that it takes only 8 hours to exploit a CED, but if the standard deviation of this distribution is 10 hours, there will be some documents which could take more than 24 hours to exploit. Taking these factors into consideration will certainly be important to a decision maker, and measures of these factors are available through the methodology previously outlined.

Future Research

Because the net-centric system effectually pools the CEDs into a vast network of exploitation assets, the availability of those assets becomes more of a concern than it did in previous architectures. Because of this change, the moment generating function technique does not entail the analytical rigor required for this complex system.

Stochastic queue theory is a technique employed by businesses everywhere. A brief hypothetical situation relays the power of this technique: if the frequency of CEDs explodes into unforeseen levels, exploitation assets may be too busy to look at CEDs that have been classified via latent semantic text analysis triage as less likely to contain valid information requirements. When this occurs, time accrues for the documents in queue. When performing simulation based analysis of Net-Centric implementations, stochastic queue theory should be used to verify the model.

Conclusion

Further work is required to port the methodology contained in this paper into an applicable package for evaluating Net-Centric technologies. Empirical studies promise to calibrate the results of the simulation and analytical solution proposed, but the moment generating function technique shows us that, holding the shaping parameter β constant, reducing the mean time of any component of CED dissemination reduces total time by a factor of β. Since we can expect significant decreases in Company and Battalion relay times, even using the current doctrine outlined in FM 34-52, a unit can potentially half its total CED relay time.

The specifics of this methodology require a good deal of adaptation in order to prove useful. Nonetheless, the power of net-centric technologies has been illustrated, and a robust platform for evaluating those technologies has been presented. How organizations choose to implement net-centricity will be of paramount concern. Without organizational flexibility, the margin of power superiority that our armed forces enjoy now will certainly diminish in the future.

NOTES

[1]Assistance provided by MAJ Ian McCulloh, U.S. Army
[2] As indicated in *Power to the Edge*, 2002
[3] Gonzales et al, 2007
[4] Zhang et al, 2001
[5] Advisor, Course Director and Director of Research for Network Science, United States Military Academy, West Point, NY.

REFERENCES

Department Of The Army. Intelligence Interrogation. 1992. FM 34-52. 25 Mar. 2007 <http://www.fas.org/irp/doddir/army/fm34-52.pdf>.

Alberts, D. Power to the Edge. Washington, DC: CISSP, 2002.

Gonzales, D., Johnson, M., McEver, J., Leedom, D., Kingston, G., and Tseng, M. "Network Centric Operations Case Study." Pending Distribution (2007). 25 Mar., 2007. <http://www.act.nato.int/events/documents/nnec/stryker.pdf>.

Moxley, F. *The Art of Network Science.* (Forthcoming) Copyright 2007.

Y. Zhang, L. He, K. Biggers, J. Yen and T. Ioerger, Simulating teamwork and information flow in tactical operations centers using multi-agent systems, *Proceedings of the tenth conference on computer generated forces and behavioral representation*, Norfolk, VA (2001), pp. 529–539.

Wackerly, D., Mendenhall, W., and Scheaffer, R. Mathematical Statistics with Applications. 6th ed. Pacific Grove, CA: Duxbury Thomson Learning, 2001. UK.

AUTHOR

Cadet Joshua Lospinosa is a member of the United States Military Academy Class of 2009.

The views expressed herein are those of the author and do not purport to reflect the position of the United States Military Academy, the Department of the Army or Department of Defense.

Editor's Note:

Joshua wrote this paper during his second (sophomore) year as a cadet. It won the 'Best Track Paper–Networks & Networking' award at the 2007 International Command and Control Research and Technology Symposium (ICCRTS 07) .

QUOTES WORTH PONDERING

If you strip away the technological buzzwords and graphical user interfaces, cyberspace isn't all that different from its flesh-and-blood, bricks-and-mortar, atoms-not-bits, real-world counterpart.

Like the physical world, people populate it.

These people interact with others, form complex social and business relationships, live and die. Cyberspace has communities, large and small….

And the threats in the digital world mirror the threats in the physical world.

—Bruce Schneier
Secrets and Lies: Digital Security in a Networked World

LINKS AND UPCOMING EVENTS

October 22-24 2007 USMA—Army Research Office Workshop

The workshop is being sponsored by the US Army Research Office (ARO) and the National Science Foundation (NSF). The workshop is held at the historic United States Military Academy at West Point, located one hour north of New York City on the banks of the Hudson River. Please select a link to the left for more information about the workshop. The 2007 USMA-ARO Network Science Workshop will encourage participants to explore what is meant by Network Science. We will devote the opening Panel Session to discussing the definition of Network Science and the areas of interest from the point of view of several different disciplines. We will have plenary speakers discuss scientific results and user representatives state the needed capabilities. Four tracks will explore Network Science tools, theory, policy, and modeling. A final panel session will summarize results from the four tracks.

Is your organization sponsoring or conducting network science research?
Hosting a network science event? Let us know!

USMA Network Science Sponsors

Army Research Institute www.hqda.army.mil/ari/

Army Research Office www.arl.army.mil/www/default.cfm?Action=29&Page=29

Command and Control Research Program, Office of the Assistant Secretary of Defense, Networks and Information Integration www.dodccrp.org/

National Science Foundation www.nsf.gov/

Author Organizations For This Issue

Science of Networks in Communities Research Program sonic.ncsa.uiuc.edu

Pearson Knowledge Technologies www.pearsonkt.com

Center for Technology and National Security Policy, National Defense University www.ndu.edu/CTNSP/

Center for Computational Analysis of Social and Organizational Systems, Carnegie Mellon University www.casos.cs.cmu.edu

Army Research Laboratory, Computational and Information Sciences Directorate www.arl.army.mil/www/default.cfm?Action=30

RECOMMENDED READING

New to Network Science and Network Centric Warfare?

These books are good places to start.

Committee on Network Science for Future Army Applications, National Research Council. ***Network Science***. *(This book can be purchased or downloaded from: http://books.nap.edu/openbook.php?isbn=0309100267 .)*

David S. Alberts and Richard E. Hayes. ***Power to the Edge: Command and Control in the Information Age.***

David S. Alberts and Richard E. Hayes. ***Understanding Command and Control.***

David S. Alberts, John J. Gartstka and Frederick P. Stein. ***Network Centric Warfare.***

(These books can be downloaded from the Command and Control Research Program website: www.dodccrp.org/html4/books_main.html)

Albert-László Barabási. Linked: How everything is connected to everything else and what it means for business, science and everyday life.

Mark Buchanan. Small Worlds and the Groundbreaking Theory of Networks.

Mark Newman, Albert-László Barabási and Duncan J. Watts. The Structure and Dynamics of Networks.

DO YOU KNOW...

You can find out more about

- The staff of the Network Science Center
- The Center's research affiliates
- Network science research activities at USMA
- Network science-related courses at USMA
- Upcoming events

at our website: www.netscience.usma.edu

NSC Report STAFF

Ms Robin Burk
Editor
Dr. Frederick I. Moxley
Senior Advisor
Dr. John James
Director,
Center for Network Science

EDITORIAL BOARD

Behavior Science & Leadership	LTC John Graham, Ph.D.
Chemistry & Life Science	COL Robert, Ph.D.
Civil & Mechanical Engineering	LTC Kenneth McDonald, Ph.D.
Electrical Engineering & Computer Science	Dr. Frederick I. Moxley, Ph.D.
Geography and Environmental Eng	COL Jason Lynch
Mathematical Sciences	COL Steve Horton, Ph.D.
Physics	MAJ Jeffrey Spear
Social Sciences	Dr. James Forrest
Systems Engineering	LTC Robert Kewley, Ph.D.

Address correspondence to:
The Network Science Report
Network Science Center
607 Cullum Road
United States Military Academy
West Point, NY 10996

The Network Science Report is a publication of the United States Military Academy's Network Science Center and is made possible by the support of the Director of Research within the Office of the Assistant Secretary of Defense for Networks and Information Integration. Publication of the USMA-ARI Workshop papers is supported by the Army Research Institute. The views expressed in this report are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

ISBN 978-1-934808-00-9

October 2007