Joint Special Operations University
357 Tully Street
Alison Building
Hurlburt Field, FL 32544

https://jsou.socom.mil
https://jsou.socom.mil/gateway/

JOINT SPECIAL OPERATIONS
JSOU
UNIVERSITY

Theoretical Perspectives of Terrorist Enemies as Networks

Robert G. Spulak, Jr.

Jessica Glicken Turnley

JSOU Report 05-3
October 2005

Joint Special Operations University and the Strategic Studies Department

The Joint Special Operations University (JSOU) provides its publications to contribute toward expanding the body of knowledge about Joint Special Operations. JSOU publications advance the insights and recommendations of national security professionals and Special Operations Forces' students and leaders for consideration by the SOF community and defense leadership.

JSOU is a subordinate organization of the US Special Operations Command (USSOCOM), MacDill Air Force Base, Florida. The mission of the Joint Special Operations University is to educate SOF executive, senior and intermediate leaders and selected other national and international security decision makers, both military and civilian, through teaching, outreach, and research in the science and art of joint special operations. JSOU provides education to the men and women of Special Operations Forces and to those who enable the SOF mission in a joint environment.

JSOU conducts research through its Strategic Studies Department where effort centers upon the USSOCOM mission and these operational priorities:

- Preempting global terrorist and CBRNE threats
- Enhancing homeland security
- Performing unconventional warfare and serving as a conventional force multiplier in conflict against state adversaries
- Conducting proactive stability operations
- Executing small-scale contingencies

The Strategic Studies Department also provides teaching and curriculum support to Professional Military Education institutions—the staff colleges and war colleges. It advances SOF strategic influence by its interaction in academic, interagency and US military communities.

The JSOU portal to the World Wide Web is https://jsou.socom.mil.

Joint Special Operations University

Brigadier General Steven J. Hashem
President

Dr. Brian A. Maher
Vice President

Strategic Studies Department

Lieutenant Colonel Michael C. McMahon
Director

James D. Anderson
Director of Research

Theoretical Perspectives of Terrorist Enemies as Networks

Robert G. Spulak, Jr.
Jessica Glicken Turnley

JSOU Report 05-3
The JSOU Press
Hurlburt Field, Florida
2005

****

Comments about this publication are invited and should be forwarded to Director, Strategic Studies Division, Joint Special Operations University, 357 Tully Street, Alison Building, Hurlburt Field, Florida 32544. Copies of this publication may be obtained by calling JSOU at 850-884-2763; FAX 850-884-4732.

****

This pamphlet and other JSOU publications can be found on the SOF Education Gateway at https://jsou.socom.mil/gateway/. Click on "Highlighted Research" to view. The Strategic Studies Department, JSOU is currently accepting written works relevant to special operations for potential publication. For more information please contact Mr. Jim Anderson, JSOU Director of Research, at 850-884-1569, DSN 579-1569, james.d.anderson@hurlburt.af.mil. Thank you for your interest in the JSOU Press.

ISBN 0-9767393-4-8

Foreword

This perspective of terrorist enemies as networks by two distinguished associate fellows of Joint Special Operations University follows as a result of its recent initiative to support USSOCOM strategic planning for the Global War on Terrorism. The paper is a manifestation of JSOU's goals for contributing products that will advance SOF strategic art and generating strategic outreach to the military, civilian, and academic communities in order to enrich those products.

Dr. Robert Spulak and Dr. Jessica Glicken Turnley presented the findings of this paper to assembled strategic planners from USSOCOM, other combatant commands, and interagency players at the Center for Special Operations plan development conference, September 2005, in Tampa, Florida. At that meeting the authors put forward a number of helpful planning concepts based on their professional studies in science and the humanities and their experiences in government and business.

The JSOU Strategic Studies Department is pleased to facilitate the association of USSOCOM strategic planners with civilian expertise and insights that can broaden military thought and encourage planning decisions directly relevant to the changing global environment. Through JSOU's strategic outreach initiative, experts in many professional disciplines have signaled their willingness to support the Nation's counterterrorism efforts. In that spirit, JSOU is proud to commend this paper to SOF readers and appreciates the support of Dr. Spulak and Dr. Turnley.

Lt Col Michael C. McMahon
Director, JSOU Strategic Studies Department

Jessica Glicken Turnley, Ph.D.

Dr. Turnley serves as President of Galisteo Consulting Group, Inc., a consulting firm in Albuquerque, NM. She also holds an appointment on the Defense Intelligence Agency Advisory Board.

Dr. Turnley provides services in the national security arena, strategic business planning, organizational development, corporate culture change, policy analysis, and economic development to clients in the public and private sector. She worked with Sandia National Laboratories on a range of projects, including the development of computational models of social organization and their possible relevance to the national war on terrorism. In other areas, she has helped the EPA develop approaches to assess social, cultural, and economic impacts at Superfund sites, participated in regional economic development efforts, and engaged in organizational audits and development projects for local organizations.

Dr. Turnley has a B.A. in Anthropology and English Literature from University of California Santa Cruz, an M.A. in Social Anthropology from University of Michigan, Ann Arbor, and a Ph.D. in Cultural Anthropology/Southeast Asian Studies from Cornell University. She was a Fulbright Scholar in Indonesia. A full resume can be found at the Galisteo website at www.galisteoconsulting.com

Robert G. Spulak, Jr., Ph.D.

Dr. Spulak is Manager of the Strategic Studies Department at Sandia National Laboratories. He is also an associate Fellow of Joint Special Operations University.

As a senior and principal analyst in the Sandia Systems Analysis Center, an independent and objective studies group, participated in studies on topics including technologies, weapon systems, defense policy, terrorism, and international relations. He has published policy papers in Strategic Review and Parameters.

Dr. Spulak has invested significant time with operational components, observing training, operational planning, and field and fleet exercises. He was one of the first members of the USSOCOM Future Concepts Working Group (FCWG) and is a member of the Naval Special Warfare (NSW) FCWG. He has contributed to SOF doctrine such as the SOF Vision, Desired Operational Capabilities, and SOF Attributes.

Robert Spulak received a B.A. in Physics with Highest Honors from the University of Northern Iowa in 1977 (with the "Purple and Old Gold" award for the outstanding physics graduate), an M.S. in Astronomy in 1978 and an M.S. in Nuclear Engineering in 1980 from the University

Executive Summary

Theoretical Perspectives of Terrorist Enemies as Networks

The term *network* is used to describe a wide variety of phenomena including terrorist groups. Networks are structures that are used to manage dispersion and are described by nodes (things dispersed) and relationships (or links) between nodes. There are many reasons for dispersion, including vulnerability, limits on operational capabilities, and service to geographical areas. Military forces throughout history have become more dispersed due to increased lethality of weapons and improved communications.

Theory is used to describe and explain the world and guide our thinking about it. There is a difference between physical science theory and social science theory. Physical science theory works for things that are measurable, repeatable, and can be tested. It uses simplification and reductionism to create predictions of future experiments and the ability to predict the behavior of complicated systems constructed of well-understood components. Social science theory describes human behavior. Many important aspects of human behavior and motivation are not observable, measurable, or capable of division into simple portions that can be solved. Furthermore, human phenomena, including behavior and people themselves, are not identical across time and space and so cannot be subject to the same type of manipulation that physical phenomena can. Social science theory can explain but cannot predict human behavior. In fact, there may be several plausible, even contradictory, explanations of the same behavior that cannot be tested.

Networks can have both technical and human links and nodes. Most network analyses use the physical science perspective to attempt to predict the effect of actions against the links or nodes (even for purely social networks of humans). From the physical perspective there are several ways to attack a network: overwhelm everything, interdict critical nodes or links, establish operational superiority to attack when necessary, or isolate and degrade part of the network. This is likely to work better for technical parts of networks. Attacking networks throughout history seems to indicate that the human parts of networks have been critical in determining the effectiveness

and response of networks to these attacks. These are the things that cannot be confidently predicted.

The concept of individuals as nodes and social interactions as links leads to the inappropriate use of physical science methods to analyze and propose attacks on human networks. Humans and their relationships are complicated phenomena. To fully understand them we must include physiology, psychology, social relationships, and the value (e.g., cultural interpretation) placed on behavior. Network approaches focus primarily on social relationships, often failing to consider the other contributing factors to behavior. Furthermore, our attempts to understand them rely a great deal on our own assumptions and perspectives.

We can view terrorists as networks for many reasons, only one of which is their organization for security. Other reasons include dispersion of their targets, tactics of simultaneous attacks, dispersion of resources including their recruiting base, and their desire to serve a dispersed constituency. Identifying a terrorist network identifies a specific enemy against which to wage international war and helps justify the use of the military against terrorism. WMD terrorism may require a more formal social network and greater integration with physical networks than other types of (*lower-tech*) terrorism. These more formal and physical networks could be more observable and contain critical links and nodes that would be more suitable to attack from the physical science perspective.

Social science theories of terrorism historically have not focused on organizational networks to explain development, recruitment, and action. They have focused more on the psychology of individual terrorists, the socialization of individuals in terrorist groups, and terrorism as communication or as a tool to obtain power and resources. These theories represent different valuable perspectives but cannot be used to direct actions against terrorism with predictable results.

It will be difficult to measure the effectiveness of the war on terrorism since the fundamental human motivations and behavior cannot be observed or measured. A historical perspective of attacking networks suggests that we should expect that the war against terrorism will require a campaign that will not in the short term destroy the functioning of the network outright, we will not be able to attack the technical and human portions of the network separately, and we will underestimate the terrorists' ability to adapt. The greatest effect

may be to divert terrorist resources to defense or repair and we may have greater success against isolated portions of the network.

The National Military Strategic Plan for the War on Terrorism (*NMSP-WOT*) defines terrorist organizations as a network, identifies components of the network, and defines a strategy to attack it. Taken literally, there are several network models that could be constructed, from a purely social network of leaders and foot soldiers to a complicated structure that contains many human and technical links and nodes. There are many assumptions and perspectives we must define to give meaning to the *NMSP-WOT* network. Analysis of a network model (via *physical science* methods) may be useful for attacking technical parts of the network, but the human parts will determine the effectiveness of attacks and the response of the network. Various social science perspectives will be more important in attacking the human parts of the networks, but they cannot be applied to confidently predict the results. The problem of destroying or rendering ineffective networks of terrorists requires a combination of physical and social approaches.

Robert G. Spulak, Jr., Ph.D.
Jessica Glicken Turnley, Ph.D.

Theoretical Perspectives of Terrorist Enemies as Networks

Robert G. Spulak, Jr., Ph.D.
Jessica Glicken Turnley, Ph.D.

Abstract. *We use a synthesis of physical and social science perspectives to discuss terrorist enemies in the context of technical and human networks. Social and physical networks have many similarities, and many differences. And while network analysis can be useful for defeating an adversary's physical networked infrastructure, such as power grids or transportation systems, it is only a piece of a larger toolkit when working with a human system. Indeed, human will and adaptability are critical aspects of a network that might otherwise be viewed as purely technical. We compare and contrast approaches from the physical and social sciences, using networks to highlight the advantages and disadvantages of using the same analytic perspective for significantly different targets. We conclude with a discussion of the networks suggested by the National Military Strategic Plan for the War on Terrorism.*

> "On both the individual and collective levels, war is therefore primarily an affair of the heart. It is dominated by such irrational factors as resolution and courage, honor and duty and loyalty and sacrifice of self. When everything is said and done, none of these have anything to do with technology, whether primitive or sophisticated."
>
> — Martin van Creveld, Technology and War.

Introduction

The network concept is widely used in modern military thought. Enemies, including terrorists, are conceptualized as networks to provide a basis to discuss attacking them. Our forces are described as networks to discuss more effective ways of employing them. The overall purpose of this paper is to provide a broad theoretical discussion of the application and limitations of networks, especially as applied to military action against terrorists. This discussion can then be used to place operational concepts in context and assess

their potential effectiveness as well as assess the scope of the terrorist enemy that may lie outside the network model or operational concepts.

We first briefly describe the pervasiveness of the idea of networks in military thought. We introduce the idea of networks and their characteristics and show that the idea is not new but can be applied throughout history. To introduce a theoretical discussion of networks, we discuss the nature of physical and social science theories. We produce a classification of technical and human networks and discuss how to attack a network, consistent with most current thought that uses the physical science perspective. We describe historical attacks on networks and make some observations about the characteristics and effectiveness of these attacks, especially with respect to the human contributions. This leads to a broader discussion of the nature of humans and how humans participate in *networked* activities. Finally, we apply these lessons to terrorists and the current war on terrorism.

In many ways, modern military thought views enemies as networks. For example, the mission of the Joint Warfare Analysis Center (JWAC) is to provide "combatant commands, Joint Staff and other customers with responsive, effects-based, precision targeting options for selected networks and nodes in order to carry out national security and military strategies of the United States during peace, crisis, and war."[1] Further, "The commanding officer and his staff are responsible for providing planners with full-spectrum analytical products while giving synergistic, effects-based, precision targeting options for infrastructure networks to support planning and execution of military options."[2]

We also are encouraged to view our military forces as networks. Part of the so-called Revolution in Military Affairs (RMA) is to leverage information technologies to allow our forces to fight more effectively as networks. Retired Admiral Arthur Cebrowski, now the Department of Defense Director of Force Transformation, is recognized as the leading advocate of Network Centric Warfare.[3] Network Centric Warfare is defined (promising much) as "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of

operations, greater lethality, increased survivability, and a degree of self-synchronization."[4]

So it should be no surprise that we also view terrorist enemies as networks. In part this is because we identify threats as individual terrorists and need to describe how these individuals operate together to perform terrorist acts. *The National Military Strategic Plan for the War on Terrorism*[5] (*NMSP-WOT*) explicitly identifies our enemies as networks. The *NMSP-WOT* consistently uses the term *network* to describe the "Nature of the Enemy" in general as well as their survivability, critical vulnerabilities, centers of gravity, and key resources. An unclassified Joint Staff briefing on the *NMSP-WOT* explicitly states that, "We are under attack from a global web of enemy networks…" and that, "Terrorist extremist organizations tend to be organized as networks; this makes them more dangerous than if they were organized in a centralized fashion."[6] One of the United States Special Operations Command (USSOCOM) roles in the Global War in Terrorism is "Leading the development and synchronization of plans against terrorist networks."[7]

Networks

Networks are systems or structures that are used to manage dispersion. Theoretically, networks are described in terms of nodes (things that are dispersed) and relationships between nodes (connecting links). Using examples appropriate to war, nodes might be combat units, individual troops, command and control centers, reconnaissance platforms, planning cells, or supply depots, and links might be communication, transportation, doctrine, orders and rules, or laws and traditions.

Actual physical networks exist because the nodes are dispersed in location or function, and they must be linked to function together. Some things by nature must be dispersed. These include truckloads, shiploads, and aircraft loads, or services for a wide geographic area (power, water, and communications). Other things may be dispersed because of operational limitations, such as limited range, speed or firepower of individual platforms, logistical support, or vulnerability.

For example, Second World War air bases in North Africa were dispersed because of the limited range of aircraft. These bases had to be linked to supply, repair, and direct the operations of the aircraft.

The dispersion of German and Italian airbases led Lt. David Stirling to consider their vulnerability (because of their isolation), resulting in the creation of the British Special Air Service (SAS), originally for the purpose of attacking them.[8] In this case the aircraft themselves were the most vulnerable part of the network and the SAS destroyed over 250 on the ground.

Or consider the age of fighting sail (Figure 1). In this case, firepower had to be dispersed on many ships because of the limited capacity of a single ship.[9] The links between ships for fighting the fleet included the "single fleet line ahead" doctrine and fighting instructions delivered by visual signals (flags from the commodore's ship). Beyond that, however, these ships had to be acquired, manned, supplied, and defended, so the overall network included ports, naval infantry, merchantmen and overseas possessions. The sailing fleet practiced *network-centric warfare*.

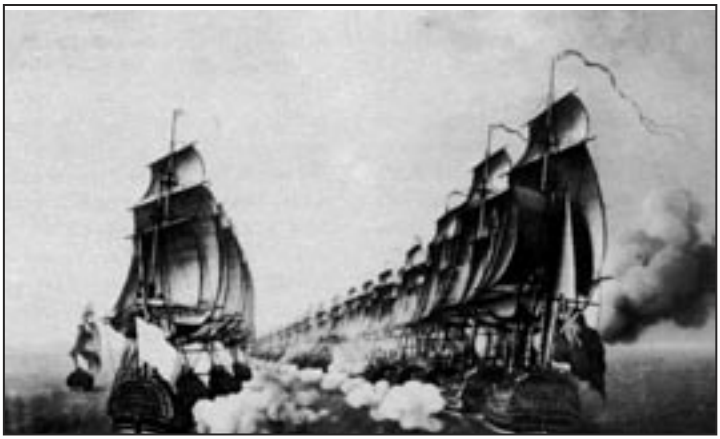

Figure 1. The age of fighting sail.

Throughout history military forces have become more and more dispersed. The Macedonian Syntagma (Figure 2) fought shoulder-to-shoulder with pikes and shields. The common term "a good right-hand man" originated in the fact that soldiers held their shields on their left, so a good man to your right protected you. Advances in technology throughout history have led to greater dispersion through the increased lethality of weapons and improved communications and transportation.[10] For example, ships could no longer fight "single fleet line ahead" as enemy firepower could demolish the whole fleet. Radio enabled dispersion of the fleet by making it possible to communicate beyond visual range. By the Second World War, S.L.A. Mar-

shall could talk about the "isolation of the battlefield" where small groups and individual soldiers were fighting.

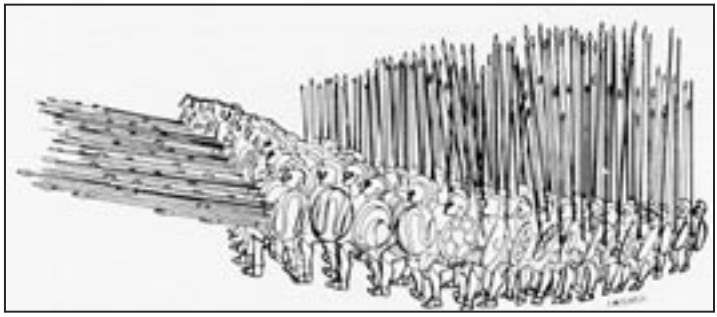

Figure 2. Macedonian Syntagma.

In spite of current popular trends in military thought such as network-centric warfare, military forces throughout history can be viewed as networks created by the needs of war. Modern forces have more and more characteristics of networks created by the greater dispersion of forces and improvements in communications, but the trend has existed throughout history. Thus it will be possible to learn lessons from history, especially regarding the human aspects of networks that do not depend on the state of technology.

The Nature of Physical and Social Science Theories

The purpose of theory, in general, is to describe and explain the world and guide us in how to think about it. The goal in discussing the theory of terrorist networks is to provide this understanding and guidance to more effectively plan to defeat the terrorists. However, at the outset, we must distinguish between physical science theory and social science theory. Some of the most powerful tools for analyzing and understanding networks are applications of physical theory. However terrorism, as well as war in general, is a human social activity that cannot be understood by physical science methods. We must consider both sources of understanding to deal with terrorist networks.

The physical or "hard" sciences[11] have the mission to produce an understanding of reality in some objective and demonstrable sense. That is, the goal is to arrive at a description or model (a theory) that conforms extremely well to measured reality and that can be used to make predictions that can be tested. To demonstrate that something

is true, one important principle is simplification. That is, the problem is simplified to the point that it can actually be solved exactly or some physical object or process can be measured well enough to distinguish between competing hypotheses. Thus the physical scientist arrives at a tiny slice of "truth." The physical sciences are successful for systems that are measurable and repeatable and for which the scientist can arrange a simple experiment to test the prediction of a theory. The measure of success of a physical science theory is the published comparison with reality, tested and repeated by other scientists.[12] There is no need for consensus or democracy. Although individual scientists may cling to their points of view for a time, a theory must be abandoned if it fails the test. An inadequate theory will eventually be replaced by a closer approximation to the truth.

To broaden the applicability of these tiny slices of truth, the hard sciences appeal to reductionism: the assumption that splitting the world into tiny slices, solving those slices, and assembling the solutions produces a broader solution that solves the larger problem. This works extremely well for physics and engineering and such.[13] Development of physical science theories throughout history has led to their applications in the familiar sophisticated technologies that make modern life possible. The danger lies in applying simplification and reductionism to systems that do not obey physical laws or that are too complex for this approach to succeed.

The social sciences attempt to understand human behavior. Much of human behavior is not simple, observable, measurable in quantitative terms, nor can it be divided into parts that can be separately solved. The social and behavioral sciences are referred to as "soft" sciences precisely because they lack characteristics of measurement, repeatability, and prediction. Some branches of social and behavioral science, described as *quantitative*, apply mathematical models and statistics to describe and analyze certain parts of human behavior. However, these tools and methods should not be used in exactly the same ways they are in the physical sciences. Mathematical statistics, for example, deals with ensembles of identical objects. The reductionist approach in the physical sciences allows us to say that certain elements are *identical* in certain essential aspects. In human environments, even though the behavior manifest in a particular instance may *look like* the behavior manifest in another, the behavior that we observe is only one part of the significance of

that event.[14] While the events have certain similar aspects, there are others that are dissimilar. Identifying which are significant in terms of crafting a response is a complex endeavor. Furthermore, since mathematical models and their sister methodologies have been devised to deal with identical objects, we abstract certain aspects of the humans and their behavior when we deal with them in these types of models (e.g. we determine that what is important is religion, or race/color, or age, or education, or …). These selection criteria are external (or exogenous) to the model. The researcher determines their importance based on some theory of human behavior. However, when these models are used these criteria and the theories upon which they are based are often not questioned nor made explicit. We will return to this point later.

… these criteria and the theories upon which they are based are often not made questioned nor made explicit.

A second way in which social science differs from the science of the physical world is in its inability to test theories. For ethical reasons, human systems cannot be manipulated in the same way that physical systems can. We cannot apply remedies for social problems to one group, but leave another untouched as a control group, to see what would happen without the intervention. A large body of theory in the social sciences is based on case studies where the researcher develops an a priori construct of what should happen based on historic evidence and then "observes" a current event (or other historical examples) to see if that construct can explain it. It is common for multiple and often conflicting theories to exist for the same acts.

Simplification and reductionism cannot be applied to human systems, meaningful and repeatable measurements are extremely difficult (humans and societies are each unique and much that is significant is not observable), the theories have limited ability to make testable predictions, and simple experiments to test specific predictions are difficult to arrange. Thus there are often multiple and competing theories to describe the same reality and objective tests cannot be used to distinguish between these theories. A theory's explanatory power, not its predictive power, is its measure of goodness. Therefore, although certain types of social theory may use techniques and approaches from physical science, we must be aware

of the limitations of the transference of such tools and understand as much about what they do not tell us as about what they do.

We will use both physical science and social science perspectives to discuss terrorist social networks. We use simplification and reductionism to create a model or description of such networks. This simple description, while accurate as far as it goes, has limited applicability in discussing real terrorist networks.

Description of Technical and Human Networks

The classic conception of a network includes discrete nodes and discrete links that connect these nodes. Nodes can be assigned functions and links can be assigned to provide flows such as communication. Even when the links and nodes are human, these kinds of networks are typically analyzed using physical science perspectives (Figure 3). For example, in this simplification, mathematical tools such as graph theory are applied to identify critical nodes and links, the removal of which would disconnect the greater portions of the network. Physical models of the network are created incorporating flows and functions and an attempt is made to predict the result of specific actions planned to cause the network to fail to function in a specific way. This is the basis of the current emphasis on *effects-based targeting*.

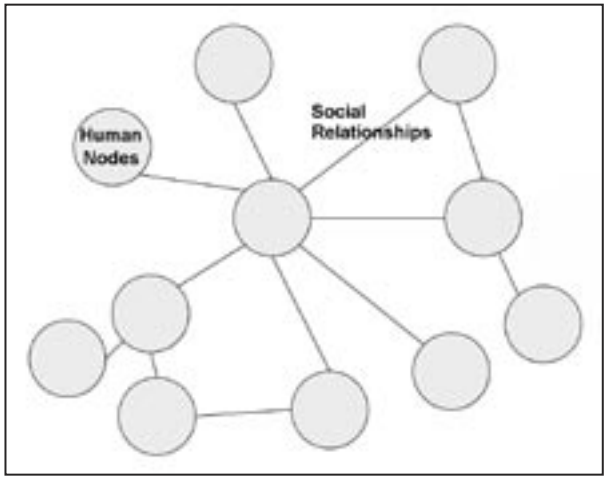

Figure 3. Representation of a "social network" of individual humans.

A typical example of the physical science perspective is: "All countries are systems; collections of many interlinking nodes. Each of these nodes—individuals, physical facilities, groups, or even symbols—affects other nodes, some more so than others. A careful and methodical analysis of the target systems could clearly identify the

relatively small number of critical nodes that, if destroyed or disabled, would cause the physical and psychological systems to cease to function."[15] Note that the author assumes that a country is a network, that the network contains both human and physical nodes, that the network can be analyzed and understood by physical science methods, that there are a small number of critical nodes, and that the effect of destroying these nodes can be predicted.

Obvious goals in the war on terror would then be to eliminate the critical nodes of the terrorist network or to interdict the critical links between nodes. Attacks on physical networks are often conceptualized as destroying nodes and links.[16] Extension of this perspective to terrorist networks leads to conceptualizing attacks on such networks as eliminating nodes (killing or capturing individual terrorists) and interdicting links (operations against communications systems, including bank transactions, etc.).

The limitations of this approach are obvious, especially applied to warfare. It is almost impossible to assess in retrospect the effect of a particular attack, battle, or campaign when studying history. How much more difficult must it be to try to predict such things, especially when the human will and capacity for adaptation will be of great importance? One cause of this limitation is our inability to perform meaningful measurements. The only truly important measure is whether the war is won or whether greater strategic goals are accomplished. In the case of Operation Iraqi Freedom one enemy network, the Iraqi Army, was easily destroyed and the war was won but perhaps it would have been better to leave it intact to assist other strategic goals.

Non-human entities, which we refer to as technical entities, are much more amenable to measurement and prediction than human entities. Thus in discussing networks we divide the world into human and technical so that the more appropriate theoretical perspective can be used for each portion. There are four possibilities: technical nodes with technical links, technical nodes with human links, human nodes with technical links, and human nodes with human links. These possibilities are illustrated in Figure 4.

The examples in Figure 4 illustrate the various possibilities. A power grid by itself could be thought of as technical nodes (power generators, computerized switches, transformer yards, and electrical meters) connected by technical links (power lines, data transmission).

An example of technical links between human nodes is the combination GPS/radio that can automatically display the locations of fellow hikers. Mailmen could be thought of as human links, sorting and transporting mail between technical nodes (post offices, mailboxes). And social organizations such as the Boy Scouts could be thought of as human nodes (the scouts and leaders) connected by human links (social interaction).

Nodes / Links	Technical	Human
Technical	Power grid	GPS hiker tracker
Human	Mailmen	Boy Scouts

Figure 4. Classification and examples of links and nodes as technical or human.

Note that our description has some definitions that we impose upon the network to give it meaning. We see a group that we define as *Boy Scouts* and we make some assumptions that such a group has *scouts* and *leaders*. Anyone who did not know what Boy Scouts are would not make such assumptions. We further define the nodes (scouts and leaders) by only a subset of all available attributes. Leaders are adult, probably (although not strictly) male, and probably have a son. That they are Christian or Jewish or Muslim or Buddhist or Hindi is not an attribute of relevance here although there is an expectation, usually not strictly enforced, that Boy Scouts will be *religious* (note the nuances of interpretation). Nor are their height, hair color, education level, and a host of other attributes, that would be relevant in other settings, important. However, once again, the determination that these attributes and not others are important is external to the network itself. It is part of our definition of a node or a link. When we turn to unknown groups such as terrorist organizations (or should we say organizations that use terrorism as a tactic) we should be very careful about the types of attributes we select as significant. The movie *Battle of Algiers* illustrates how dangerous a mistake can be when the French assumed that all the insurgents were male.[17]

Any real network will most likely be a combination of these reductionist possibilities. For example, the concept of a power grid can be expanded to include human components such as the operators,

customers, repairmen, managers, shareholders, and political and military leaders. In addition to the purely technical aspects of understanding the critical links and nodes to attack in the physical network, the effectiveness of attacking a power grid may depend on how the operators respond to limit the damage or redirect power (this could be a function of physiology, psychology, social issues such as training, and cultural constructs such as the importance placed on various aspects of the response), the time it would take for repairs to be made, and the priority of resources political or military leaders may make available to substitute for lost capability. Thus non-observables such as human will and adaptability, and values such as our cultural assignment of the importance of hospitals over residences in terms of power allocation, and the like become critical aspects of a network that might otherwise be viewed as purely technical. These aspects of human behavior do not fit well in a mathematical construct of links and nodes.

A terrorist network is more likely to resemble the Boy Scouts as a purely social organization than it will resemble a technical network such as a power grid. Terrorist networks may contain technical components, such as technical communications, weapons, transportation, training camps, banking, etc., that might be understood and attacked using the physical science perspective. However, much of the network will consist of individuals and their associations. Unfortunately, theories of individual or social behavior lack the predictive power of physical theories. Simply applying social models to the human parts of a network in an analogy to using physical models for the technical parts of the network will not work. Portraying terrorist groups as social networks (as in Figure 3) presents an untrue impression that the analysis has the accuracy and predictive power of physical theories. That is, the representation as a network implies simplification, since the nodes are individual terrorists and the links are specific interactions that are analyzed in isolation, and reductionism, since the network and its behavior are assessed based on the simple relationship of links and nodes, neither of which may be possible when dealing with humans.

We also must beware of the tendency to treat human networks as something that exists in a similar form over time. In fact, human (social) networks are constantly changing. One of the characteristics distinguishing a net-centric organization from a bureaucratically

structured organization is its fluidity.[18] We come from a culture that functions predominately along bureaucratic lines. Our strong beliefs in the rule of law and basic human equality give predominance to these types of corporate organizations. When dealing with cultures with other strong bases for social organization, such as the predominance of kinship relations or patronage ties, we must recognize that these organizational structures (social networks) are highly fluid in nature. The diagram we draw today may well be outdated by tomorrow. Clearly this is also much less true of technical networks. Anything involving large capital investments such as infrastructure systems such as power grids, water systems, or experimental facilities change slowly.

From a theoretical point of view, then, it is important to distinguish between the technical parts of a network and the human parts. The technical parts may be amenable to analysis and attack from the physical science perspective.[19] Any real network will also contain important human elements. These elements may be easily separated from the technical elements but more likely the technical and human will be intertwined.

Physical Science: Theory of Attacking Networks

A network by definition is a collection of nodes and links even if these nodes and links are considered to be human elements. We describe here a *theory* or classification of ways to attack networks. There are at least four ways to attack a network. The first is to overwhelm the entire network. The second is to interdict critical nodes or links. The third is to establish operational superiority and interdict nodes or links when necessary or convenient. And the fourth is to isolate and degrade a portion of the network to reduce its efficiency. These methods are illustrated conceptually in Figure 5.

Note that these reasonable ways of attacking a network assume that the network is a static entity whose structure after the attack will be the original less the parts that have been attacked and that the effects of an attack can be predicted to guide the choice of the kind and locations of the attack. They also assume that enough is known about the network (even its very existence) to make these kinds of analyses possible.

It is appropriate here to insert a comment about intelligence. We cannot apply theory without data. The whole issue of adequate in-

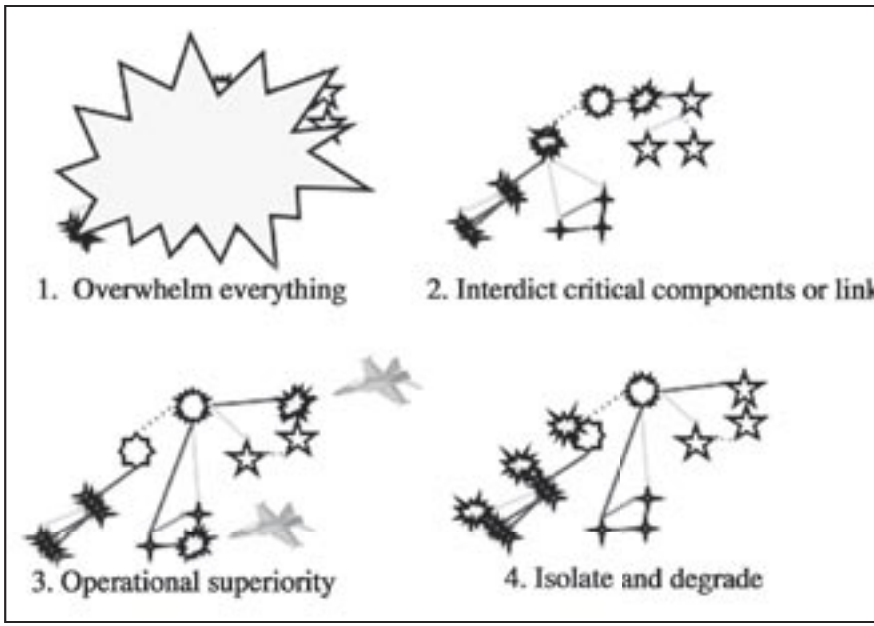

Figure 5. Attacking networks.

formation is itself a major limitation of the operational concept of attacking networks. Our experience has been that we often don't know about the existence of terrorist network or that we have not placed a priority on understanding it until we are attacked. We didn't know the extent of Saddam's nuclear program before Desert Storm. We didn't know the status of Iraqi weapons of mass destruction before Operation Iraqi Freedom. However, some methods of attacking networks may require less information. Attacking critical nodes requires a high level of understanding to identify critical nodes and predict the consequences of an attack. But overwhelming everything or establishing operational superiority may not require as much accurate information about the network.

Once again using the age of fighting sail, we can illustrate the four methods of attack. A larger fleet with more cannon was a decisive advantage in a single fleet line ahead engagement. A 3/2 advantage was enough to destroy the enemy fleet, overwhelming everything. Critical nodes in the fleet included the commodore's flagship that issued fighting instructions and key resupply bases. Operation-

al superiority could be gained by establishing sea control with faster better-armed ships. Tactics used to exploit operational superiority included breaking the enemy's line, doubling lines, and attacking ports and merchantmen at leisure. Since the network included isolated ports and overseas possessions, these could be isolated and degraded by privateering, terror, and attacking sources of supplies and raw materials.

The question is how well does this classification account for attacking real networks, especially since real networks are not such neat collections of nodes and links? We will now describe some historical examples of attacking networks to demonstrate the relative effectiveness of such attacks and the influence of human elements. Note that this is an example of applying social science theory through historical case studies.[20] Our conclusions are influenced by our choice of case studies, the perspectives through which we view history, and many other exogenous factors.

Social Science: Attacking Real Networks in History

During the Vietnam War, the United States bombed the network of North Vietnamese fuel facilities.[21] This led the North Vietnamese to disperse their oil reserves. They placed storage tanks near major highways and 55-gallon drums along roads, in cities, towns, and rice paddies. In another example, their electrical power plants that were destroyed in the spring of 1967 were replaced by more than 2,000 portable generators. A critical network that was not attacked was the extensive dike system because of the perceived political cost of attacking civilian infrastructure.

In the Second World War, a critical node in the German war effort was assessed to be the Ploesti, Romania, oil refining facilities.[22] Destroying Ploesti was predicted to destroy one-third of Hitler's oil production and shorten the war in Europe by six months. Twenty-three heavy bombing raids, totaling 9,173 bomber and fighter sorties, dropped 13,709 tons of explosives. Although 13 kilotons is roughly equivalent to the atomic bombs dropped on Hiroshima and Nagasaki, resulting in heavy damage to several facilities, they were repaired by battalions of Russian slave laborers and remained operating at 20 percent of capacity. Twenty percent may not seem like much, but the message is that 13 kilotons of conventional explosives was not enough to overwhelm the capacity for repair.

Another critical node was thought to be the German ball-bearing industry. Paul Nitze, who participated in the United States Strategic Bombing Survey conducted after the war, relates that "not one end item of German war production had been delayed a single day by virtue of attacks on the ball-bearing industry. The buildings of the ball-bearing plants had been blown into rubble, not once, but time after time... While the cost to the Germans to restore ball bearing production was high, involving the dispersal of factories and even the building of underground plants, they were able to offset the damage within the time they had to repair their losses."[23] On the other hand, massive Allied bombardment caused extensive German civilian casualties and destruction of civilian infrastructure. By late 1944 the German economy was severely damaged but the German Army was able to continue fighting until May 1945. Civilians in Britain, Germany, the Soviet Union, and Japan all suffered greatly and generally became more resolute under direct attack. Stalin tolerated sieges of Soviet cities and more than 20 million deaths without surrendering. Dresden and Tokyo were firebombed causing massive destruction and loss of life with little strategic effect.

In the age of fighting sail, a major network was the Spanish Armada. The network consisted of the Spanish fleet, Spanish shipyards, client states that supplied some ships, treasure ships from the New World that funded the fleet, and many ports where provisions were stockpiled.[24] Sir Francis Drake was sent to attack the network in 1587. His orders were to disrupt shipping between the Mediterranean and Spanish ports, distress enemy ports, seize ships from the East and West Indies, and harass the Armada if at sea. Drake raided the port of Cadiz (Figure 6) and

Figure 6. The defense of Cadiz.

burned 31 merchant vessels. He attacked Portuguese ports, in one case destroying the seasoned wood to be used for barrel staves on Spanish ships. Therefore the Spaniards had leaky barrels, spoiled food, and contaminated water. Drake sailed into the Atlantic and the threat to the treasure ships caused the Spanish fleet to deploy, returning with worn vessels and sick crews. These actions did not defeat the Armada but delayed it sailing against England. Germany had an atomic bomb project in the Second World War. Since the Allies did not know how little advanced the German atomic bomb project was, the attempt to defeat Germany had to seriously consider the potential for an atomic defense. This network included the German scientists, research institutions, and material production. Because of their research focus, heavy water was the key to the German bomb

Figure 7. The Norsk-Hydro heavy water plant at Ryukan, Norway.

project and the Ryukan, Norway, heavy water plant really was a critical node (Figure 7).[25] It was predicted that successfully destroying the plant would delay German heavy water production two years.

There were four attacks on German heavy water and its production. The first (unsuccessful) attack consisted of a glider assault with 34 engineer commandos. The gliders crashed and the survivors were killed by the Germans. When the Germans discovered that the Norsk-Hydro plant was the objective, they increased their forces in the area to ~300 men and established antiaircraft defenses.

The final assault team for the first successful attack—the demolition of the heavy-water production cells at the Norsk-Hydro plant on February 28, 1943—consisted of nine men, a four-man demolition party, and a five-man covering party. The operators parachuted into Norway. Since the Germans expected another relatively large commando attack, the enemy was not alert against a small force.

Access to the plant was controlled by two guards on a bridge over a 600-feet-deep gorge. To bypass the bridge, the operators skied and walked until they descended into the gorge and crossed the icy river. They ascended the gorge and walked to the plant, gaining access to the grounds by cutting the chain on a railway gate. The door to the plant could not be forced, but two men entered the plant through a cable tunnel (a known alternative), and two men entered by breaking a window. There was one night watchman who was detained. They laid the charges which exploded while they were still on the grounds. There was no immediate reaction by security forces and the operators withdrew.

Damage from the demolition attack was repaired in only two months instead of two years. The plant was unsuccessfully bombed by the Allies, which caused the Germans to decide to move the equipment and heavy water to Germany, crossing Lake Tinn by ferry. The ferry was chosen for attack by the Special Operations Executive (SOE) operators because the Germans were expecting another attack on the plant and had increased security with two companies of SS troops. It had been estimated that it would take at least 40 well-trained and heavily-armed men to now directly attack the plant, with no hope of escape.

Moving the heavy water and equipment by ferry created a new vulnerability. The second successful attack—the sinking of the ferry—was executed by only three men. An operator rode the ferry prior to the shipment date of the heavy water. He determined both the best place to place a charge and the time for the explosion. In the early morning of the day of the shipment, before the heavy water arrived by rail, three operators boarded the docked, unguarded ferry. While one operator engaged the night watchman in conversation, the other two men planted an improvised charge consisting of 8.4 kg of plastic explosive, clocks, and 9-volt batteries below the floor along the keel. They left by 0400. The explosion occurred at 1100, when the ferry was in the middle of the lake, and it sank in 300 meters of water.

Another enemy network was the equivalent of six German infantry divisions dispersed among the Aegean islands (Figure 8). This network was attacked to prevent the redeployment of these troops to reinforce the German defense against the Allied invasion of France. There were three phases that were implemented with small-unit raids using small boats of the Special Boats Service (SBS), including indig-

Figure 8. The network of Aegean islands.

enous craft, and Greek sympathizers, operating from the Turkish coast. In the first phase, cumulative attacks on shipping were designed to reduce the available tonnage to the point where the Germans could no longer evacuate their garrisons. The second phase involved harassing attacks on outlying garrisons, forcing the Germans to dedicate and expose to attack shipping for reinforcement, evacuation of wounded, and investigation. The third phase was specifically designed to create friction: "Every island would now have been raided, every island would be waiting for our next visit. Short of food, and short of mail, with leave at home a distant memory, with horizons bounded by a few square miles of rock and scrub, the disgruntled garrisons would toil up nightly from their comfortable billets to the trenches which they had dug on bleak hillsides, there to keep vigil."[26]

These historical examples illustrate several *truths* about attacking real, militarily significant, networks. First, attacking a network rarely destroys the function of the network outright, although there may sometimes really be a critical node. Second, the ability of the human enemy to adapt and repair or replace the network is almost always underestimated. Third, the major effect of attacking a network is to reduce its effectiveness through reduced efficiency and diversion of resources devoted to defense or repair. Fourth, successfully

attacking a network often requires a sustained campaign, against either a single critical node or multiple elements of the network. Fifth, it is rarely possible to separate the technical and human parts of a network and consider them separately. Sixth, isolated parts of the network are more effectively attacked. Finally, attacks aimed at civilian infrastructure networks or that cause civilian collateral damage are likely to stiffen the resolve of the enemy or reduce the sympathy of the population to our cause.[27]

The Nature of Humans

This brings us back to a point we made earlier. While understanding social networks is an important part of understanding how humans operate in groups, networks are only one dimension of such understanding. Any human action, for example, may be parsed as the result of the confluence of (at least) four very complex levels of analysis. The first is physiological—every individual is biological being and his biological state at any moment in time has an impact on behavior. The second is psychological. The particular orientation of any individual will influence his response to environmental conditions. The third is social. Each individual is embedded in a structure of relationships with others. Those relationships embody elements of power, affect, and other dimensions. The fourth is cultural. The social relationships, psychological orientations, and physiological states are given some sort of value and meaning by the group within which the individual moves. The individual then is located in some physical environment which gives him access to certain types of resources and takes on value from the socio-cultural complex within which the individual moves. This complexity is illustrated in Figure 9. Note that any behavioral event is a simultaneous manifestation of factors from all illustrated dimensions, further constrained by the physical environment within which the event takes place. Also note that not all these factors are observable.

The nodes in social networks are actors. The links are the structure of the social relationships between and among them. What is missing from this construct is the value placed upon behavior—the cultural dimension. For example, we could draw a communication link between two individuals based on the number of contacts over a given time period. But the significance of that communication is cultural. Greater frequency does not necessarily mean greater in-

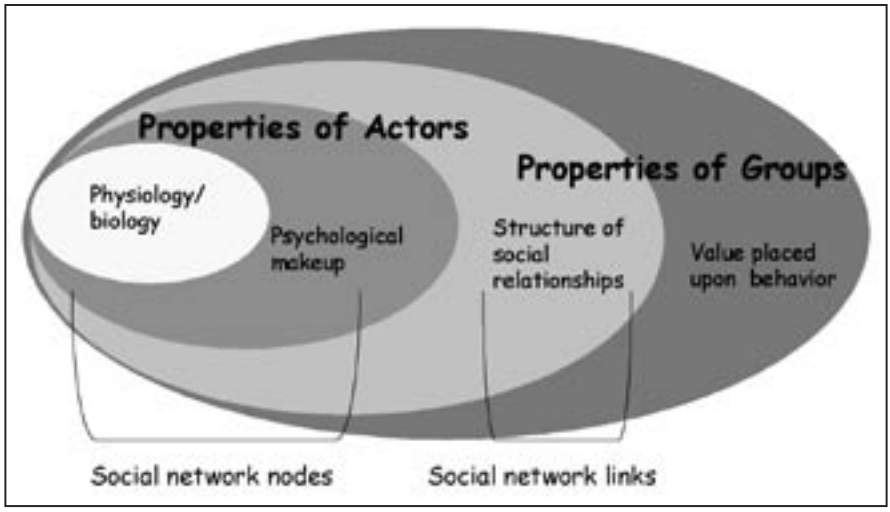

Figure 9: Behavioral factors

vestment in or importance of the relationship.[28] Also missing are the inactive links—links that can be created or (re)activated if an existing link is broken. A large part of the willingness to do this stems from the importance of the link to the actor—another non-observable.

We should also keep in mind that relationship-based organizations such as social networks and rule-based organizations such as bureaucracies are not mutually exclusive. Many in the military have a *go-to person*—the individual who, by virtue of personal knowledge and social ties, can make things happen by working relationships in the military world. By the same token, even strongly relationship-based organizations have bureaucratic or functionally defined aspects. Families can have patriarchs (or matriarchs for that matter) who serve as head of the family. As one individual dies another will replace him. The amount of influence the person in the position exercises may be personality-dependent, but the position exists independent of the person who occupies it.

Terrorist Networks

To ask the obvious question, why are networks a useful tool for understanding terrorism? We can identify many characteristics that fit well into the network concept and we are disposed by the trends of military thought to think in networks. The use of network structures

to respond to perceived vulnerabilities is the most oft-quoted motivation we attribute to terrorists as networks. For example, Russell Howard asserts that "in response to improvements in counterterror capabilities and increased cooperation among governments, global terrorist groups such as al Qaeda have adopted networked structural models instead of hierarchical structures."[29] But large numbers of individual terrorists, multiple enemies, dispersion of targets among western states, the tactic of multiple simultaneous attacks to multiply terror effects, dispersion of the recruiting base, dispersion of sources of resources, desire to show worldwide reach and service to their constituency of worldwide Muslim extremists, and establishing the unpredictability of the location of attacks are also reasons that we could use a network model.

The idea of a terrorist network may be useful to identify the enemy ("terrorist network" instead of "terrorism") against which we can wage international war. Terrorism as criminal political violence could be viewed as a law-enforcement problem. Fighting terrorism as an international criminal activity includes law enforcement, diplomacy, international cooperation, and foreign assistance. The role of the military is to support these activities. However the fundamental purpose of the military is to wage and win the nation's wars. A specific terrorist network as an enemy in war would require all of the actions described above and a primary role for military force. This may be especially justified if the threat is not low-level political violence that could remain in the domain of law enforcement but is catastrophic terrorism that can be viewed as waging war on US civilians. Waging war involves the politics of war that may remove many operational restrictions against a terrorist enemy but will also likely involve violation of other states' sovereignty, capturing or killing enemy personnel, interception and destruction of foreign vessels and aircraft, seizure of foreign assets, and acceptance of collateral damage and accidental innocent casualties.

Are terrorist organizations really networks as we understand networks in the largest sense? As we have seen, the concept of a network and how to attack it fits better into the physical science perspective that doesn't account for much of the human qualities of combatants throughout history. It will be useful to take a broader perspective of social organization.

Different dominant organizational structures work well in different environments and for different social ends. Networks, because of their flexibility and adaptability, are advantageous at a tactical level. They allow adaptation to rapidly changing circumstances, including significant changes in organizational purpose. Rule-based organizations, like bureaucracies, are strategically advantageous. Changes in individuals in top positions do not necessarily mean significant changes in organizational direction or purpose. These types of organizations can last over time, and survive significant personnel change. They also can organize more efficiently and effectively to manage and execute complicated projects with a high degree of division of labor. The predominance of network over rule-based relationships in the Islamic fundamentalist groups may be a contributing factor to the predominance of low-technology weapons (including suicide bombers) and the absence of more sophisticated weapons that require more lasting and structured social organization to develop and deploy.

Networks' are indeed important in the war on terrorism. That said, we need to recognize the difference between social and technical networks and the consequences these differences have for plans to disrupt them. We also need to keep in mind that social networks are only part of the human story. Our adversaries—like us—are much more complicated than "the [social] ties that bind." Links may be amorphous and hard to identify or attack effectively or without collateral damage. The philosophical and ideological motivations for terrorists (the value they place on behavior) may be created and communicated by others who have no direct social or structural link to the terrorists themselves. The Unabomber worked alone but was linked and motivated by a philosophy of anti-technology and environmental extremism that he held in common with others. Timothy McVeigh and Terry Nichols identified with an anti-federal government philosophy. Islamic extremists are linked through a common ideology created by certain Islamic scholars (living and dead) and promulgated through various mosques and schools that also serve non-extremist constituents.

Technical networks will be more (but not perfectly) amenable to analysis and attack with predictable outcomes because of the applicability of physical science methods. Social networks will be difficult to identify, understand, analyze, plan attacks against, or predict the outcome of attacks. Application of physical science methods against

social networks may be misleading and inappropriate. John Arquilla, et al., explain the evolution of terrorists toward social networks in explicitly technical terms: "The information revolution is altering the nature of conflict across the spectrum" and "Information technology (IT) is an enabling factor for networked groups; terrorists aiming to wage netwar may adopt it not only as weapon, but also to help coordinate and support their activities."[30] Thus the concept that "It takes a network to fight a network"[31] is also based on the view of terrorist organizations as social networks but is a strategy based on the physical concept of operational superiority for speed of response to dispersed threats and response to changes in the enemy network that imply a need for a dispersed attack (a network).

One aspect of terrorism that may be more amenable to analysis and attack may be weapons of mass destruction (WMD). WMD are more likely to require an identifiable and relatively stable structure to garner and maintain control over necessary resources and the weapons themselves. WMD require more technical resources including technical people with critical skills and a bureaucratic structure may more effectively characterize the complex social infrastructure needed for the development of WMD than does a network. An interesting analog is the emergence of monumental architecture in civilizations only after they developed food resources necessary to feed specialized non-food-producing technical classes and developed bureaucratic structures from what had previously been kin-based networks. Finally, the catastrophic consequences of WMD terrorism are more likely to justify use of military force.

This is not to say that social networks are unimportant in the War on Terrorism, but that they are only part of the story just as physical networks are only part of the story. Disrupting these networks can have a significant effect on social activity.[32] There is a cost to constructing new links, activating old links, or assuming a different role in a social network. However, the willingness to invest in this cost is a function of other factors. Consistent with our description of social science theories there are several different ways to analyze terrorists and their relationships.

In the terrorism literature there are at least four general schools of thought: psychological, sociological, communicative, and power-based.[33] The psychological approach looks for a particular personality constellation or composite of psychological factors that characterize

the terrorist (this approach has fallen out of favor lately). The sociological approach focuses on the sense of self-identity and the paths to social actualization that marginalized groups such as terrorist organizations afford some individuals. In this explanatory frame, an individual trades loyalty to the group for social and moral security and the chance of success. To some degree, Sageman's work falls under this approach with his focus on disaffected individuals.[34] The sociological approach focuses on the milieu which spawns or supports terrorist groups. The interest in *failed states* or, as Barnett[35] puts it, the *gap* or unconnected states, falls into this camp. The communicative explanations see terrorism as a type of street theatre, albeit a rather grisly type. And finally, the power-based constructs see terrorism as a tool used by disenfranchised groups to gain access to power and resources. The later two (communicative and power-based) are instrumental in nature, that is, they see terrorist groups as a means to an end. The two former approaches (psychological and sociological) are causal and explanatory frames, seeking to understand why these types of groups emerge and the forces that keep them functioning as groups. The more powerful treatments of terrorism use elements from both the instrumental and causal camps, and from both approaches within each. The value of these theories is not that any may be demonstrated to be true (or false), but that each represents a different perspective form which to view human behavior. But since these theories do not result in predictions with which we can confidently predict behavior in individual cases, they also cannot be used to accurately direct actions to accomplish specific desired goals.

Application to the National Military Strategic Plan for the War on Terrorism

The National Military Strategic Plan for the War on Terrorism (*NMSP-WOT*) has three elements: protect the homeland, disrupt and attack terrorist networks, and counter ideological support for terrorism.[36] Disrupting and attacking terrorist networks is described as, "These offensive efforts of the strategy are designed to disrupt terrorists' ability to execute their attacks effectively or sustain their ideology. These efforts include killing and capturing key enemy leaders and foot soldiers, destroying training centers, and denying enemy access

to each of the eight categories of resources critical to the enemies' operations." The eight categories of resources (types of nodes and links) are identified as: leadership, safe havens, funds, communications and movement, weapons, foot soldiers, access to targets, and ideological support. Thus the *NMSP-WOT* appears to define the network and the strategy to attack it. Note, for example, that the *NMSP-WOT* assumes that there are critical nodes or links: "key enemy leaders and foot soldiers" and "resources critical to enemy operations."

The next step might be to construct a model of the terrorist network to apply the tools that have been developed for analyzing social or physical networks. It is important to keep in mind that any model is just a representation of reality and there may be many different representations. One possible model we could construct is terrorists as a purely human or social network with nodes consisting of leaders and foot soldiers linked by purely social relationships (as in Figure 3). In that case, the eight categories of resources would be attributes of the nodes or links. But there are many reasons one might want to incorporate physical components in the network itself. Recall John Arquilla's thesis, that the terrorist network is enabled to some degree by technological links. The definition of Network Centric Warfare includes both human and technical links and nodes. Terrorist foot soldiers might be thought of more as human links, like mailmen, delivering weapons to physical targets. In some cases, such as WMD, the weapons and the technical means to develop them may be the critical nodes that would be most effectively attacked. And we have argued that the physical parts of the network may be more amenable to analysis, prediction, and attack due to the nature of physical theory. (The danger in the latter case is in neglecting the human parts of the network.)

Figure 10 shows one possible notional simplified representation of a terrorist network with both human and technical elements suggested by the *NMSP-WOT*. Obviously there may be many more nodes of each type. The links may be "communications and movement" or "leadership" or both. There may be many more links between any of the types of nodes.

Referring to our theory of networks (technical and human) and our discussions of social science theory, we see that this presentation of the network itself contains human actors as well as technical

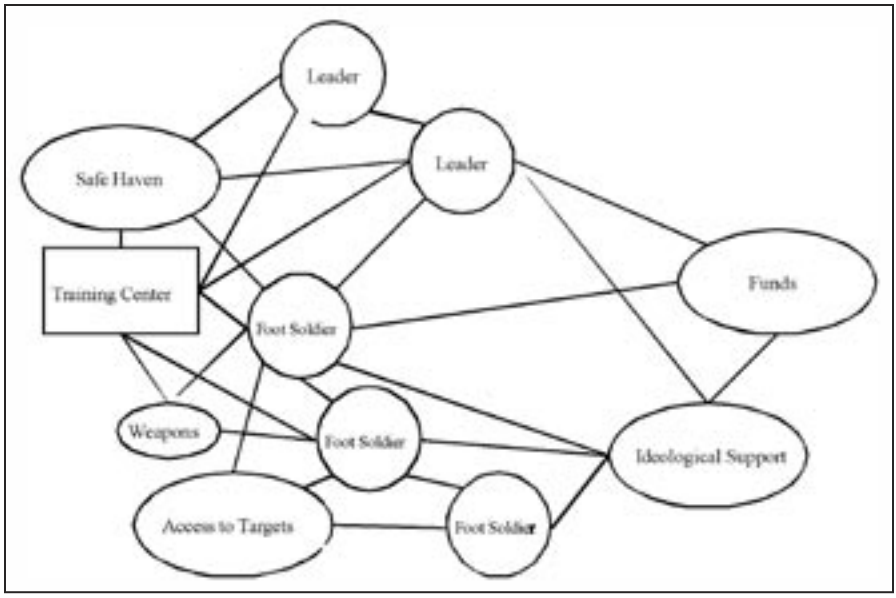

Figure 10. Notional terrorist network as suggested by the NMSP-WOT.

or physical entities, and makes assumptions about factors that are external (or exogenous) to the network.

The human actors or nodes are *leaders* and *foot soldiers*. These are people with different types of attributes. Leaders (we assume) have leadership qualities that could be an attribute of a leader—or it could be what is transmitted from a leader to a foot soldier to cause the soldier to follow. This example illustrates a couple of the earlier points we have made with regard to the limitations of social networks. What does leadership look like? How would we know if someone *had it* (i.e., was a leader) or was *transmitting* it? And do we know how leadership is manifest in the adversary culture? It may well be manifest through behavioral traits very different than those we would recognize. The restriction of the network to these two types of people also begs the question of the role of people other than leaders and foot soldiers in keeping terrorist organizations alive. Let's look at a node like a training center. A training center is a physical place. Do we know any of the attributes of that physical place? How do these vary from culture to culture—or over time? A training center also has personnel, some of whom may be permanent (trainers or cadre), others who may be transient (trainees). How do these relate

to leaders and foot soldiers, who are the only people we have in our schema? And how about communications… what and where are the physical means by which information is transmitted? The medium is an important part of any communication but the communication infrastructure does not appear here. Ideological support is shown as another node—a *resource* in the *NMSP-WOT*. However, such support is generated by people who are neither leaders nor foot soldiers—and who are not represented in our network. We also need to know both about the ideology of concern (what are its key tenants and how might they be interpreted?) and about the mechanisms of support. Is it through provision of materiel and/or safe havens? Is it through non-interference … a sort of passive support? Furthermore, attacks on ideological support may actually justify and strengthen it. This type of construct does not illustrate how completely terrorist organizations are embedded within a larger society, and the importance of the larger society's interaction with them. Finally, even the technical parts of the network (sources of funds, communications and movement, and weapons) may have significant human contributions. For example, funds denied from one source may be easily replaced. One mode of communication may be replaced by another.

The language of the *NMSP-WOT* leads us to construct a network that operates on several logical levels at once. This is conceptually good, as the environment within which we wage war operates simultaneously on several logical levels. However, it precludes us from applying many of the analytic techniques of formal network analysis to the schema, for these require what might be termed an *impoverished network*—one which operates on only one dimension at a time. At best, we may conceive of a moment in *terrorist time* as the intersection of many different networks of many different types. The *NMSP-WOT* schema also highlights the need for exogenous or external definitions of key elements (such as *leadership* or *ideological support*) that will locate the network in some specific space and time. We should therefore heed the lessons of physical attacks against technical and human networks.

To recap, attacking a network rarely destroys the function of the network outright, although there may sometimes really be a critical node. The ability of the human enemy to adapt and repair or replace the network is almost always underestimated. The major effect of attacking a network is to reduce its effectiveness through reduced

efficiency and diversion of resources devoted to defense or repair. Successfully attacking a network often requires a sustained campaign, against either a single critical node or multiple elements of the network. It is rarely possible to separate the technical and human parts of a network and consider them separately. Isolated parts of the network are more effectively attacked. And, attacks aimed at civilian infrastructure networks that cause civilian collateral damage are likely to stiffen the resolve of the enemy or reduce the sympathy of the population to our cause.

Given these lessons, networks can be useful tools in the war on terrorism. As with our earlier model of human behavior that illustrated the interaction of the biological, psychological, social, cultural, and external environment in any event, so can networks of various aspects of terrorist activities illuminate (although not predict or illustrate with certainty) key nodes and connections. In the fashion that these networks are discussed by the *NMSP-WOT*, the networks can be constructed and conceptually (mentally) manipulated only. This limits us to relatively simple networks, given the limitations of the human mind. If we wish to accommodate greater complexity or size (numbers of nodes) by working computationally, we need to *impoverish* the network, breaking it into constituent networks of similar logical orders such as communications infrastructure or social networks. Keep in mind that the types of links in social networks (the things connecting people) can range from abstracts such as *ideological support* to concrete items such as weapons. If we take the former route and use abstractions such as ideological support, we must carefully define a) what ideology we are dealing with, and b) what *support* looks like behaviorally. We also need to recognize that (to continue to follow our example) to fully understand ideological support we also need to understand the communications infrastructure. And the communications infrastructure itself has a physical and a social aspect.

Conclusions

The term *network* is used to describe a wide variety of phenomena, including terrorist groups. Networks are structures that are used to manage dispersion and are described by nodes (things dispersed) and relationships (or links) between nodes. There are many reasons for dispersion, including vulnerability, limits on operational capa-

bilities, and service to geographical areas. Military forces throughout history have become more dispersed due to increased lethality of weapons and improved communications.

In the past social and physical networks have been analyzed using similar tools. We have argued two points. First, applying approaches from the physical sciences to human phenomena will give false results because the phenomena in question are fundamentally different. As a result, social theory is different in kind from theories about physical systems. Second, there is no such thing as a purely physical network. Each of the physical phenomena, whether they are nodes or links, has a human dimension.

The National Military Strategic Plan for the War on Terrorism (*NMSP-WOT*) defines terrorist organizations as a network, identifies components of the network, and defines a strategy to attack it. Taken literally, there are several network models that could be constructed, from a purely social network of leaders and foot soldiers to a complicated structure that contains many human and technical links and nodes. There are many assumptions and perspectives we must define to give meaning to the *NMSP-WOT* network. Analysis of a network model (via physical science methods) may be useful for attacking technical parts of the network, but the human parts will determine the effectiveness of attacks and the response of the network. Various social science perspectives will be more important in attacking the human parts of the networks, but they cannot be applied to confidently predict the results.

We thus suggest that the problem of destroying or rendering ineffective networks of terrorists requires a combination of physical and social approaches. Our theoretical discussion provides a context with which to assess practical approaches for attacking terrorist networks.

Endnotes

1. Joint Warfare Analysis Center, United States Joint Forces Command website www.jfcom.mil/about/com_jwac.htm, accessed July 2005.
2. Joint Warfare Analysis Center website www.jwac.mil/mission.asp, accessed July 2005.
3. David S. Albers, John J. Garstka, and Frederick P. Stein, Network Centric Warfare (Washington, D.C.: C4ISR Cooperative Research Program, 2000).
4. Ibid, p. 2.

5. Chairman of the Joint Chiefs of Staff, National Military Strategic Plan for the War on Terrorism, 4 March 2005. All quotations and references to the NMSP-WOT are from sections marked "unclassified."
6. Joint Chiefs of Staff, "The National Military Strategic Plan for the War on Terrorism (NMSP-WOT)", 29 March 2005.
7. Ibid.
8. E.g., Robin Hunter, True Stories of the SAS (London: Virgin Books, 1995).
9. Wayne P. Hughes, Jr., Fleet Tactics (Annapolis, Maryland: Naval Institute Press), Chapter 2.
10 T. N. Dupuy, Understanding War (New York: Paragon House, 1987), Chapter 13.
11. Scientists would quibble with our definition of hard sciences as equivalent to physical sciences since physical sciences usually mean physics, chemistry, etc., as distinguished from the "hard" biological sciences (that we include here in the physical sciences).
12. It must be noted that many ideas about physical reality are ultimately proved wrong, otherwise there would be no need for the scientific method. Greek philosophers, for example, created plausible (but incorrect) explanations for natural phenomena and the great advance was when the scientific method was created to test ideas against reality. Since social science theories cannot be tested in the same way, it is almost certain that many of our ideas about human behavior are wrong.
13 But there is some dispute: there is an interesting book, The Tao of Physics, that argues that even for physical systems the whole is different than the sum of the parts.
14. A homemade bomb on a bus carrying black schoolchildren to a predominately white school in the American South is a very different event than a homemade bomb on a bus in the Gaza Strip or in Baghdad.
15 John L. Petersen, "Plan for the 21st Century Now," U.S. Naval Institute Proceedings, August, 1991, p. 53.
16. Although there has also been discussion of information operations against information systems.
17. Gillo Pontecorvo, director, "Battle of Algiers," 1967.
18. It is important to keep in mind that bureaucratic or corporate structures also have operative social networks. These social networks may or may not parallel the power and influence paths of the bureaucratic structure.
19. Or perhaps not. Chaos theory deals with physical systems that are non-linear. One result is the "butterfly effect" where the smallest difference in initial conditions for the system will grow exponentially to produce dramatically different results.
20. Strictly speaking, our illustrations lack the rigor of true history (e.g., we use secondary sources).
21. Mark Clodfelter, The Limits of Airpower (New York: The Free Press, 1989).

22. James Dugan and Carroll Stewart, Ploesti (New York: Bantam Books, 1963).
23. Paul H. Nitze, From Hiroshima to Glasnost (New York: Grove Weidenfeld, 1989), p. 32.
24. Samuel A. Southworth, ed., Great Raids in History (: Castle Books, 2002).
25. E.g., Per F. Dahl, Heavy Water and the Wartime Race for Nuclear Energy (London: Institute of Physics Publishing, 1999).
26. John Lodwick, Raiders from the Sea (Annapolis: Naval Institute Press, 1990), p.106.
27. We could also infer that terrorist attacks against us have had the same results that we identify for attacking networks. We now place more emphasis on internal security (the Department of Homeland Security) and in military operations we have experienced a diversion of resources away from offensive action to force protection.
28. Think of the number of times one may call a mortgage broker when buying a house, vs. the number of times one may have called a commanding officer in the same time period.
29. Russell D. Howard, "Understanding Al Qaeda's Application of the New Terrorism – The Key to Victory in the Current Campaign," in Terrorism and Counterterroism, Russell D. Howard and Reid L. Sawyer, eds. (Guilford, Connecticut: McGraw-Hill/Dushkin, 2004), p. 80.
30. John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information-Age Terrorism" in Terrorism and Counterterroism, op. cit., pp. 95, 98.
31. Ibid, p. 95.
32. Sendero Luminoso apparently had a real critical node, Guzman. In a more significant example, the communist terrorist networks in Europe (Red Brigades, etc.) were eliminated after the fall of communism due to many social factors, probably including discredited ideological goals and the elimination of safe-havens, sources of financing, and technical support.
33. See, for example, Jessica Glicken Turnley and Julienne Smrka "Terrorist Organizations and Criminal Street Gangs," Advanced Concepts Group, Sandia National Laboratories, 2002.
34. Marc Sageman, Understanding Terror Networks (Philadelphia: University of Pennsylvania Press, 2004).
35. Thomas Barnett, The Pentagon's New Map (New York: GP Putnam's Sons, 2004).
36. Chairman of the Joint Chiefs of Staff, op cit.