NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

REDEFINING ATTACK:
TAKING THE OFFENSIVE AGAINST NETWORKS

by

Zachary H. Staples
Robert J. Michael, II

March 2003

Thesis Co-Advisors: Dan Moran
John Hiles
Rudy Darken

This thesis done in cooperation with the MOVES Institute
Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Redefining Attack: Taking the Offensive Against Networks			**5. FUNDING NUMBERS**
6. AUTHOR(S) Zachary H. Staples and Robert J. Michael, II			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

The Information Age empowers individuals, and affords small groups an opportunity to attack states' interests with an increasing variety of tactics and great anonymity. Current strategies to prevail against these emerging threats are inherently defensive, relying on potential adversaries to commit mistakes and engage in detectable behavior. While defensive strategies are a critical component of a complete solution set, they cede initiative to the adversary. Moreover, reactive measures are not suited to quickly suppress adversary networks through force. To address this shortfall in strategic planning, the science of networks is rapidly making clear that natural systems built over time with preferential attachment form scale-free networks. These networks are naturally resilient to failure and random attack, but carry inherent vulnerabilities in their highly connected hubs. Taking the offensive against networks is therefore an exercise in discovering and attacking such hubs. To find these hub vulnerabilities in network adversaries, this thesis proposes a strategy called Stimulus Based Discovery, which leads to rapid network mapping and then systematically improves the accuracy and validity of this map while simultaneously degrading an adversary's network cohesion. Additionally, this thesis provides a model for experimenting with Stimulus Based Discovery in a Multi-Agent System.

14. SUBJECT TERMS Information Age Warfare, Information Superiority, Stimulus Based Discovery, Targeting, Multi-Agent Systems, Complex Adaptive Systems, Relationships, Networks, Connectors, Tickets, Simulation, Network Centric Warfare, Counter Terrorism, Strategy			**15. NUMBER OF PAGES** 168 **16. PRICE CODE**
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

REDEFINING ATTACK: TAKING THE OFFENSIVE AGAINST NETWORKS

Zachary H. Staples
Lieutenant, United States Navy
B.S., United States Naval Academy, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN NATIONAL SECURITY AFFAIRS

Robert J. Michael, II
Lieutenant, United States Navy
B.S., Texas A&M University, 1994

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE
and
MASTER OF SCIENCE IN MODELING, VIRTUAL ENVIRONMENTS AND SIMULATION

from the

NAVAL POSTGRADUATE SCHOOL
March 2003

Authors: Zachary H. Staples

Robert J. Michael, II

Approved by: Dan Moran
Thesis Co-Advisor

John Hiles
Thesis Co-Advisor

Rudy Darken
Thesis Co-Advisor

James Wirtz
Chairman, Department of National Security Affairs

Michael Zyda
Chairman, MOVES Institute

Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Information Age empowers individuals, and affords small groups an opportunity to attack states' interests with an increasing variety of tactics and great anonymity. Current strategies to prevail against these emerging threats are inherently defensive, relying on potential adversaries to commit mistakes and engage in detectable behavior. While defensive strategies are a critical component of a complete solution set, they cede initiative to the adversary. Moreover, reactive measures are not suited to quickly suppress adversary networks through force. To address this shortfall in strategic planning, the science of networks is rapidly making clear that natural systems built over time with preferential attachment form scale-free networks. These networks are naturally resilient to failure and random attack, but carry inherent vulnerabilities in their highly connected hubs. Taking the offensive against networks is therefore an exercise in discovering and attacking such hubs. To find these hub vulnerabilities in network adversaries, this thesis proposes a strategy called Stimulus Based Discovery, which leads to rapid network mapping and then systematically improves the accuracy and validity of this map while simultaneously degrading an adversary's network cohesion. Additionally, this thesis provides a model for experimenting with Stimulus Based Discovery in a Multi-Agent System.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ABBREVIATIONS AND SYMBOLS

SAC	Strategic Air Command
NRO	National Reconnaissance Office
OPI	Office of Photographic Interpretation
JPME	Joint Professional Military Education
DARPA	Defense Advanced Research Projects Agency
TIA	Total Information Awareness
UNSCOM	United Nations Special Commission
WMD	Weapons of Mass Destruction
IAEA	International Atomic Energy Agency
MAS	Multi-Agent System
TNS	Terrorist Network Simulation
RELATE	Relationships, Environment, Laws, Agents, Things, and Effectors
ISAAC	Irreducible Semi-Autonomous Adaptive Combat
IAGO	Integrated Asymmetric Goal Organization
NCO	Non-Commissioned Officer
TA	Terrorist Agent
DES	Discreet Event Simulation
IID	Independent and Identically Distributed
UI	User Interface
MOVES	Modeling, Virtual Environments, and Simulation
NPS	Naval Postgraduate School
C	Contact
r	Recruit
O	Operator
R	Recruiter

T	Trainer
F	Financier
Lg	Logistician
A	Arms Dealer
L	Leader

ACKNOWLEDGMENTS

The authors would like to thank Mr. John Hiles for his insight, inspiration, and thought provoking discussion that stretched the limits of our imaginations. The thesis all began with owls, mice and the ideas from a great storyteller. John took us in directions never imagined when we began this project. The authors would like to thank Dr. Rudy Darken for his countless help in scoping, redefining, and reworking the ideas in this thesis into a manageable undertaking. His understanding, patience, and experience as an academic associate and thesis advisor were immensely valuable as the ideas and approach for this thesis evolved over its lifespan. The authors would also like to acknowledge ADM Jim Hogg (Ret.), CAPT Bill Glenney, USNR, and the members of the Chief of Naval Operations' Strategic Studies Group XXI who helped open our eyes and minds to the possibilities of the Information Age.

LT Michael would like to thank Dr. Arnie Buss for his insight and knowledge on Discreet Event Simulation and his work on Simkit that made parts of this thesis a reality. Most importantly, LT Michael would like to thank his wife Brenda for her constant love, support, and understanding, whom without surviving graduate school would not have been otherwise possible.

LT Staples would like to thank Dr. Dan Moran for his educated critique and impassioned knowledge of military history. His questions pushed us to formulate Stimulus Based Discovery within a long tradition of military art. Additionally, sitting in class with Dr. John Arquilla provided a keen focus for the challenges of Information Age conflict juxtaposed against the American tradition in Industrial Age warfare. Most of all, I am indebted to my wonderful wife for her unfailing support, and my three children for always greeting me with a smile despite many working weekends and bedtime stories from *Foreign Affairs*.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The terror attacks on September 11th, 2001 announced the arrival of non-state actors as significant players in international security. No longer were terrorists a nuisance or criminal organization operating against the peripheral interests of states. The collapse of the World Trade Center, a smoking hole in the Pentagon and a narrowly averted conflagration at the U.S. Capitol struck at the most prestigious symbols of American wealth, power, and democracy.

Shortly thereafter, in his address the joint session of Congress, President Bush conceded that the war on America, declared years earlier by al Queda, would now be joined with the full might of American military strength. However, making war against networks is significantly different than attacking the state-centric threats the U.S. military fought in the 20th century. Network threats are not bounded by the geographical constraints of national borders. They are not organized along the clear hierarchical channels familiar to military planners. They are seldom motivated by the same factors as uniformed militaries acting in the service of their respective states. And worse, the order of battle for these elusive networks is hidden from view. There are few tanks to count, barracks and command centers to reconnoiter or industrial facilities to target. Replacing these tried and true metrics of an adversary's strength are elusive notions of sleeper cells, transnational identity, religious fanaticism, and a host of other social and organization constructs that the American military has few tools to counter.

To date most attempts to defeat emerging network threats have focused on improving surveillance, increasing database access and structuring existing information to bring possible threats to the fore. These are all worthwhile endeavors, but suffer from a common drawback. Each of these methods relies on

the adversary network to do something observable. Better surveillance can only detect an action if the adversary chooses to act. Better databases can only search those things that were observed, and information structuring is only useful if there are buried observations that would benefit from closer examination. Therefore, techniques in vogue for finding and stopping network organizations are primarily defensive because they rely on an untenable hope that the adversary will make some error along the path to attack and that this error will be detected. However, the authors are not satisfied with this defensive, reactive approach to fighting networks.

The first step in creating an offensive strategy for attacking networks is to understand two critical factors that will define the environment for Information Age conflict. First, the range of possible threats faced by U.S. forces is dramatically larger than the threat spectrum encountered during the Industrial Age. This significant growth in complexity is brought on by the empowerment of individuals and small groups to endanger states in ways that have not existed before. Thus, the range of threats states must account for is no longer limited to the capability of a deranged tyrant. Rather, states are now susceptible to attack by small groups that accrue resources and power independent of national support or loyalties. Second, advances in information and weaponry allow the U.S. military to break the historical link between range and accuracy. Sailors, Marines, Soldiers and Airmen must no longer get close to get accurate. With precision-guided weapons it is now possible to operate targeting and engagement system in separate locations within unique processes, which in turn enables the parallel engagement of hundreds of enemy aimpoints from extreme range. However, the application of this force is rendered useless against networks without a capability to rapidly identify valid targets in the adversary's system.

The challenge of attacking networks is only made more difficult by the incongruence of the existing strategic framework and the Joint Campaign Planning Process to the reality of how networks are organized. In a well-intentioned effort to expose more military officers to classical works on strategy and operational art the professional education curriculum has reduced warfare to a cookie cutter formula centered on industrial threats. This gross simplification for explaining one of mankind's most sophisticated activities does not bode well for inculcating America's warriors with a new mindset to fight networks. Furthermore, the planning processes that exist are not aligned to leverage America's strengths against new adversaries that do not conform to traditional organizations and value systems.

To compensate for this staid approach this thesis looks to new discoveries in network science that demonstrate all human organizations grown over time with preferential attachment will organize themselves into scale-free networks. Like all networks scale-free systems are composed of nodes and links. However, in the scale-free network some nodes, called hubs, acquire an extraordinary number of links while most nodes remain loosely connected. This hub and spokes topology makes scale-free systems extremely robust to random failure, but vulnerable to focused attack against the hubs that hold the system together. America's independent targeting and engagement systems are ideally suited to attack the hubs in such a network, but finding hubs presents a daunting challenge when an adversary is actively trying to remain covert.

To address this challenge of finding hubs in elusive networks, the authors propose a strategy called "Stimulus Based Discovery." Stimulus enhances the capability to detect nodes and hubs by focusing collection in time and space to several likely network stimulus responses. In short, Stimulus Based Discovery converts American firepower superiority into an information advantage and decreases the time between threat perception and ordnance delivery against an

adversary's network hubs. Thus, American forces retain the initiative and put networks on the defense.

A series of case studies is presented to support Stimulus Based Discovery and define four different tactics for stimulating networks. Any network is composed of nodes and links, and both of these can be can be stimulated in two different ways. First, networks can be stimulated by explicitly changing the network with actions such as killing or capturing a node. Second, the network can be stimulated by cognitively distorting the way nodes and links are perceived by humans in the system. Thus, there are four possible stimuli: explicit nodal stimulus, explicit link stimulus, cognitive nodal distortion, and cognitive link distortion. A case study for each tactic discusses how that how particular type of stimulus has successfully revealed nodes in a hidden network, and buttresses the argument that Stimulus Based Discovery is a sound strategy applicable for attack against any network

Finally, the authors realize that theory must be rigorously evaluated prior to implementation. To this end a model was developed to serve as a laboratory for experimenting with the effects of stimulus against a reactive network organization. The simulation is built around a multi-agent system in which each node represents an individual actor in the adversary network. Although the threats susceptible to Stimulus Based Discovery vary across the entire threat spectrum (due to the underlying human social organization), the model is based on a terrorist organization. The terrorists are modeled as a social organization that seeks to conduct attacks coordinated through functional relationships. The model includes recruiting, training, resource gathering, leadership, influence, personality and many other social behaviors that add fidelity to the Stimulus Based Discovery laboratory. The result of this low level decision-making is macro behavior that closely matches theoretical predictions. Thus, the laboratory

provides a realistic capability to further explore Stimulus Based Discovery with both qualitative and quantitative results.

In conclusion, the authors believe the United States' current war with al Queda is a prelude to conflict with many other types of networks. Stimulus Based Discovery is therefore an effort to address this new form of organization by integrating the battle proven concepts of attack and offensive with the inherent vulnerabilities of a network topology. Historical examination and emerging science suggest that Stimulus Based Discovery can be a powerful tool for converting America's firepower superiority into an information advantage over network organizations that defy traditional tools for applying combat power. The laboratory created for this thesis is a first step to exploring the concept in more detail.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THE NEW COMPETITIVE LANDSCAPE

A. INTRODUCTION

John Arquilla, a widely published author on the Information Age jokes, "Two thirds of the earth's surface is covered in water. The other third is covered by papers on Information Warfare." Therefore, yet another thesis on this topic could easily repeat and regurgitate familiar rhetoric that changes are coming and offer another hypothetical of what future conflict might require. However, that is exactly what this thesis is not! LT Michael and I specifically ask a hard question, "Is there emerging science based on hard mathematics that leads to new concepts for winning wars in the Information Age?" The answer we have found is emphatically, yes.

In March of 2000, I attended the Navy's Global Wargame exploring the conceptual requirements and operational procedures for conducting effects-based operations. As a longtime student of military history I was immediately skeptical. Military operations have always been about achieving some effect. The Ancient Greek desire to capture Troy fits the effects-based model if you phrase it, "Leaders of Troy will desire to surrender the city." During the game a naval aviator and flag officer summarized what I was thinking quite succinctly. He said, "I have always found that a 2000 pound bomb has one hell of an effect if you hit the guy your aiming at. I don't know why we are trying to make it so damn complicated." So the strategy proposed here for taking the offensive against networks is not about replacing lethal force with a new-age definition of how to fight peacefully. Rather, redefining attack is about taking the offensive against networks and developing a strategy to find valid targets in elusive organizations.

Implementing the strategy proposed here for attacking networks requires another iteration in the advance of military art. Victors across the ages have

continually integrated new technology with organization and doctrine to produce operating concepts that overpower, outmaneuver and otherwise outperform their adversaries. (Cohen, 1996) Therefore, the strategy proposed here recommends yet another blend of technology, organization and operating concept to produce decisive results against a new form of adversary.

Bearing in mind the technology, organization and concept trifecta, this thesis focuses on concept. Virtually all Information Age power relies in some measure upon advances in technology, however there is already a healthy debate on the technologies for future conflict. Therefore, specific technologies, weaponry and information processing tools are not addressed. This thesis is narrowly focused on two elements of future conflict most obvious now in the pioneering days of the Information Age: the empowerment of individuals and the independence of range and accuracy. From these characteristics, we examine specific scientific ideas that create advantage in this competitive landscape and propose a strategy for attacking network organizations that seeks to militarily suppress this emerging form of organization. Then with the theory established and explained this thesis concludes with a model, which provides a laboratory for testing the proposed network attack strategy.

B. STATE CONTROL OVER THE MEANS OF WAR

The Information Age changes the competitive environment. However, this broad assertion does not lend itself to quantitative comparison. Therefore, a working definition of the specific attributes of competition affected by the information age is necessary for rigorous analysis. The challenge at this stage is daunting. There is by no means a definitive or comprehensive definition of the Information Age, and this thesis is much too short for such a postulation. Furthermore, the ubiquitous availability of information has only begun in the last decade and any attempt to define the Information Age at its inception is merely conjecture about the possible. However, one characteristic seems self-evident

about the world today – empowerment of individuals raises the unpredictable nature of a single human being to the level of strategic influence.

Consider this significant change in light of the past 350 years of western civilization. In 1618 war broke out in Europe when Bohemian Protestants declared independence from the Holy Roman Empire and the ruling Hapsburgs converged on Prague to re-subjugate the heretics and insurgents. Individual princes throughout Germany took sides to advance their political or religious goals. France and Spain entered the conflict to fight for dynastic control, and Sweden fought for religion and territory. The war spread and expanded as weak alliances formed and dissolved in hasty defenses of shifting priorities. The conflict eventually touched every major power in Europe and was fought only to a bitter concession in 1648. The Thirty Years War, as it has come to be known, was fought primarily by mercenary armies for a tangled imbroglio of princely ambitions, religious zealotry and dynastic control. In fact when delegates finally began to meet in 1644 to arrange a peace settlement "after nearly a year of meetings the delegates were still not agreed on the all-important *subjecta belligerantia:* who was at war with whom over what?" (Blitzer, 1967, p. 42) The overwhelming complexity of the situation arose from an indeterminate morass of conflicting authority.

When the Thirty Years War began there was no precedent for who had authority to declare war on whom. There was no international law or accepted norms that identified who was just in their use of violence to pursue political or religious aims. And most of all, there was no consensus on who was a legitimate actor in the conduct of international relations. Princes fought for territory, power or to proselytize their religious views. Religion sanctioned the bloody slaughter of opposing devotees, and dynasties raised armies to extend their influence or weaken their adversaries. Three decades of conflict produced no clear victor and therefore no resolution to the considerable ambiguities of authority. So in the

aftermath of war delegates to the two separate peace processes knew they must take steps to address questions of authority in religion, politics and government. When the final Peace of Westphalia was signed in 1648, its lasting contribution to world security was a strong endorsement for nations states, not individuals, to function as actors in international diplomacy. (Treaty of Westphalia)

Although the compromise reached at Westphalia addressed various political issues of the war, dire consequences in human suffering had a more profound effect. Moderate estimates suggest that the Thirty Years War resulted in one third of the Germanic people dying a violent death or more frequently falling to the excruciating plight of starvation.[1] (Parker, 1984) Losses to the other parties to conflict did not equal one in three dead, but were significant and tragic. With the life and livelihood of the common man so easily snuffed by individual actions of the privileged it is no small wonder that the brilliant political thinker Thomas Hobbes wrote in 1651.

> During the time men live without a common power to keep them all in awe, they are in that condition which is called war; and such a war, as is of every man, against every man…Whatsoever therefore is consequent to a time of war…the same is consequent to the time, wherein men live without other security, than what their own strength, and their own invention shall furnish them… In such condition, there is no place for industry; because the fruit thereof is uncertain: and consequently no culture of the earth; no navigation, nor use of the commodities that may be imported by sea; no commodious building; no instruments of moving, and removing such things as require much force; no knowledge of the face of the earth; no account of time; no arts; no letters; no society; and which is worst of all, continual fear, and danger of violent death; and the life of man is solitary, poor, nasty, brutish and short. (Hobbes, 1960)

Hobbes idea to solve this intractable problem lay in the idea of absolutism – the concentration of power in one supreme authority. The only way to subdue these divisive forces was to impose on them a superior force, a new and rational

[1] Exact death tolls for the Thirty Years Wars vary from 15 to 20 percent all the way to 70 percent in some areas.

political order. This awesome power, which Hobbes dubbed *Leviathan,* was needed precisely because the forces of local and class privilege, tradition, and religious schism were themselves so strong.

The idea of absolutism, although not specifically coined as a term of reference until much later, slowly began to take root in Europe and centralize power into the state and away from individuals. The most apparent manifestation of absolute dominion in the 17th century is Louis the XIV of France. When Louis' religious advisor and powerful prime minister, Cardinal Mazarin died in 1661 Louis assumed the full mantel of power and established absolute secular rule of France. His subsequent installation of bureaucracy instead of aristocracy to run the workings of government brought the entire resources of France under his dominion.

Across the English Channel, absolutism was slower to take hold due to internal strife, but in 1688 the Glorious Revolution installed a constitutional form of government that centralized control with the state. The English Parliament passed the Declaration of Rights, putting forth the terms England was to be ruled by. When William and Mary accepted these terms they were crowned King and Queen of England. Then in the years immediately afterward the mettle of the English system was put to the test in a series of conflicts to check the ambitions of Louis XIV.

War for the succession of the Spanish crown in 1701 tested the newly organized states in a contest that pitted France, Spain and Portugal against a Grand Alliance of virtually every other country in Europe. In this conflict, the scope and magnitude of a successful field army required a sophisticated governmental organization that could harness the industry and more importantly the finances of the state at large. In fact, the English constitutional system proved more effective than even Louis' authoritarian bureaucracy. "William III [of England] could draw upon the resources of his country more

effectively than any other sovereign of his time. Parliament voted him funds not only by raising taxes, but also by borrowing money from the newly established Bank of England. William thus got more money, and got it faster, than he could ever have raised through taxation alone." (Blitzer, p. 167) In the end, the mass mobilization of Europe resulted in the defeat of France and the treaty of Utrecht in 1713. (Wolf, 1970)

The 17th century and the wars that defined it, mark a turning point in history because the shift toward secular government reduced the states accountability to religion. By 1748 the Pope would formally relinquish authority in civil matters declaring:

> For Forms of Government let fools contest; Whate'er is best administer'd is best. (Essay on Man, pp. 303-4)

Furthermore, the consolidation of power with absolutism diminished the effect of capricious princely ambitions on the general welfare of man. However, the problem of a bad king remained a burden and the vice of Leviathan. John Locke wrote in *Two Treatises of Civil Government*

> …it is evident that absolute monarchy, which by some men is counted for the only government in the world, is indeed inconsistent with civil society, and so can be no form of civil government at all. The first and fundamental positive law of all commonwealths is the establishing of the legislative power. (Second Treatis, p. 90)

The net result of these tectonic shifts in the way power was gathered and administered is that individual actors were left off the stage of international relations. When the treaty of Westphalia was signed in 1648 it began the transition from dynastic to bureaucratic states in the international system. (Treaty of Westphalia) This first step followed by the emergence of absolutism and a military requirement to harness the entire state resources to wage war meant that strategic threats were immaterial if not connected with the authority

of the state. By the end of the 18th century power to act in the international system resided with state actors and not individuals.

Our world has been defined by this state-centric model ever since. As recently at 1945 and the establishment of the United Nations the concept of state sovereignty is highlighted key to preventing conflict and the inevitable human suffering it entails. The United Nations Charter affirms the notion of state sovereignty as a method to regulate interstate diplomacy and reduce the possibility of war. In addition, numerous other conventions on international law completed within the United Nations continue to reinforce the ideal of sovereignty.

Strategic threats in this state centric environment have materialized almost exclusively when ambitious rulers took control of states and turned their nations' capability against their own citizens or outside their borders. Quick recapitulation of the last century's most notorious individuals bears this out. Hitler, Stalin, and to a lesser extent Hussein, Pinochet, Idi Amin, Pol Pot, Qadafi and others presented a threat to their fellow citizens and in some cases the world only after they ascended to the helm of power in their respective state.

Furthermore, success in interstate conflict during this period has been directly linked to a nation's capacity for industrial production because the machines and armaments of war were absolutely essential to a successful campaign. Carl Von Clausewitz wrote of early 19th century conflict that "Because war is an act of force, committed against a living, reacting opponent, it produces three interactions that, in theory, lead to three extremes: maximum use of force; total disarmament of the enemy; and maximum exertion of strength." (Clausewitz, p. 78) Similarly, Russell Weigley's seminal work *The American Way of War*, argues the U.S. military perspective on conflict has always gravitated toward destructive war. "An army strong enough to choose the strategy of annihilation should always choose it, because the most certain and probably the

most rapid route to victory lay through the destruction of the enemy's armed forces." (Russell, 1997) Fighting in this total, destructive fashion in the industrial age required the complete devotion of state resources to manufacturing the tools of war. Anything less failed to achieve the proven strategy of destruction and mayhem required for victory. Therefore, in the Industrial Age an individual that did not control the state's means of production could not create the manufactured goods required to pose a strategic threat.

In summary, the last three centuries have slowly eroded the capability of one person or a collection of people to create and sustain strategic threats without first taking control of a state. From the beginning of the 18th century an individuals' lack of access to the resources and manpower of the state made it nearly impossible for a sole individual to threaten an entire nation. Admittedly strategic threats have emerged in this period from dictators and tyrants, but only after those men successful captured the reins of state power. Therefore, the requirement to seize control of a state in order to pose a strategic threat created large barriers to individuals with malicious sentiment against a particular state. Sadly, those days are probably gone because systemic changes inherent to an Information Age empower individuals to compete with states. This rise of power among individuals and small groups undoubtedly forms one of the structural elements of future conflict.

C. EMPOWERMENT OF THE INDIVIDUAL

An information-enabled world gives power to individuals. John Arquilla and David Ronfeldt note "The rise of networks means that power is migrating to nonstate actors". (Arquilla and Ronfeldt, 2001) In *The Lexus and the Olive Tree*, Thomas Friedman makes a similar statement that "states don't represent the real power structure anymore. The relevant power structure is global. It is in the hands of the Superpowers and the Supermarkets." Friedman goes on to explicitly state that any entrepreneurial individual can become a dynamic player in world markets. (Friedman, 2000) The source of this change is a growing

interconnectedness among people all over the globe, often called "globalization." However, the very networks that make the international fluidity of capital, goods and services available to a global economy the conduits of finance, supply and organization for criminal and terrorist networks to move onto the international stage.

Information Age opponents can accrue resources and international political power independent of states. Then these transnational organizations can use that power to create a significant threat against a state. Osama bin Laden is the archetype for this "Super Empowered Angry Man" (Friedman) that threatens the international system by coordinating a transnational organization through information age tools such as global transportation and the Internet. Nongovernmental organizations can take many benevolent forms including international environmental protection activists, relief organizations and political campaigns such as the International Campaign to Ban Landmines. However, the same liquidity of capital, ease of transportation and smooth flow of international service that create a foundation for benevolent work can also be turned to nefarious purposes.

> Globalization and interdependence have not only encouraged the emergence of 'upright global citizens' but have facilitated the rise of transnational criminal organization which pose new challenges to both national and international security. (Williams, 1999)

Even more troublesome, growing reliance on information tools and a generally poor understanding of information security open a state's computer infrastructure to the threat of small hacker groups or individuals. "The hacking threat is constantly evolving, elusive, and becoming more dangerous" (McClure, 2001) However, the number of people required to conduct even the most sophisticated attacks remains small. Hacking is a contest of intellect and social engineering whose only barrier cost to entry is practice, a bright mind and a devious purpose. James Adams describes a plausible trajectory for hacking as a

devastating new form of warfare in his book, *The Next World War*. (Adams, 1998) If Adams and others prove remotely accurate then it will is not be outside the bounds of reality to consider catastrophes such as GPS attacks that cause commercial airplane crashes, control system hacks in nuclear reactor plants, mass flooding caused by dam gate hacks, economic chaos caused by erasing the New York Stock Exchange, or hackers selling technical drawings for modern nuclear weapons stolen from U.S. computers. This short list of possible attacks is merely representative of an infinite set of actions ranging across the threat spectrum of direct violence, economic warfare, agricultural deprivation, and weapons of mass destruction. The distinguishing characteristic of these attacks and any other is that the limits of disruption are only bounded by the limits of imagination and technical acumen.

The idea of a small group of hackers wreaking mayhem and perhaps destruction upon a nation is a significant departure from the reality of the state dominated security environment. An empowered individual is not subject to the restraints inherent in a state based international system. Even a dictator must hold together a coalition of supporters, and is bound by the requirement to protect their interests. Despots and tyrants have often committed atrocities, but in doing so they knowingly risk their position, power and wealth if they destabilize their support base. Even Saddam Hussein, the late 20th century's icon of supreme dictator, holds together his Tikrit based tribal coalition with preferential policy and lavish schemes to pump resources into his support base. (Ritter) The information age villain is released from the constraints of coalition maintenance because he can act in isolation or very small groups of likeminded radicals. This opens the floodgate of possible options and creates an environment where planning cannot be based on a rational actor model. Replacing this model is a frightening notion that we will face threats from the wildest reaches of the criminally insane mind. Thus, an important characteristic of information age conflict is that individuals and small groups can pose strategic

threats to states, and the range of options available to these small groups is dramatically larger than the threat set encountered in the Industrial Age.

D. THE INDEPENDENCE OF RANGE AND ACCURACY

The threat set facing nation-states is more complicated than it has been over the last few centuries, but the United States also enjoys a significant new capability brought on by the Information Age. There is now an independence of range and accuracy that has never existed before. This independence liberates the delivery of ordnance from the difficult task of aiming the weapon. In turn ordnance delivery and targeting have developed into highly specialized skills that can occur in different locations synchronized by advanced communications. The sum effect of this evolution is precision engagement from extreme range and without warning. The challenge is finding an operational concept that leverages the power of independent targeting and engagement into a capability for thwarting the attacks of empowered individuals.

For centuries, getting accurate has always meant getting close. For example, if you wanted to kill a specific individual in the Stone Age you would have to get close enough to touch him or throw a rock. Then the advent of aimed weapons such as the Mongol horn bow introduced a capability to accurately engage beyond the reach of hand held weapons. Muskets and then rifled guns increased the distance between combatants even more. However, in each of these advances the ultimate distance was still limited to the visual range of the soldier or sailor that would carry out the lethal action. Then in the twentieth century there was a fundamental shift in the way targets were acquired and engaged that separated the person choosing and aiming the weapons from the soldier or sailor that would fire the ordnance.

This separation between targeteer and shooter began in 1905 with the first use of indirect fire by the Japanese army during the siege of Port Arthur. In the Russo-Japanese war the Japanese Navy chose not to attack the Russian position

in Port Arthur. Therefore, the Japanese Army was forced to conduct a rearguard action against the port stronghold before advancing north against the main Russian force. To accomplish the siege of Port Arthur the Japanese army officers introduced an artillery innovation. They inclined their guns to fire over the top of the mountains adjacent to the port and the shot fell on the reverse slope defenses. The tactic weakened the Russian defenders with little risk of return fire, and the Japanese Army successfully captured the port. Previous to this attack, field artillery and naval guns had always been used in a direct fire mode where the gun commander had visual contact with his target. Indirect artillery fire was the birth of separating the targeteer with binoculars from the shooter that would fire the ordnance.

Thirty-five years after the battle for Port Arthur the growing separation between targeting and engagement can be glimpsed again in World War II. The Italian air power theorist Giulio Douhet observed the bloodshed of World War I and considered airpower the weapon to avoid stalemated conflict. (Douhet, p. 57) Douhet foresaw the future of the bomber's ability to deliver firepower against targets deep in the interior of a nation and he predicted that civil society would demand their nation to surrender in the face of sure destruction. (Douhet, p. 58) World War II witnessed Douhet's theory put to the test with the unrestricted allied bombing of Japan and Germany. Regardless of Douhet's accuracy about the effects of airpower, the processes surrounding the employment of these bombers further separated targeting from the operator that flew the bombers.

Advanced bombsights made air power possible and required specialists to operate. Development of an effective bombsight made it possible, or at least probable, to hit a target on the surface of the earth from high altitude. Thus, large fleets of bombers envisioned by Douhet became a popular tactic for engaging valuable industrial and civilian targets.

Specially trained photo interpreters were the next critical step toward specialization of targeting and delivery. Contrary to general opinion, it is very difficult to determine what a reconnaissance photograph shows without a trained photo analyst. "The intelligence on an image may not be self-evident; it may require interpretation by trained photo interpreters who can 'see' things on the image that the untrained person cannot." (Lowenthal, 2000) To the untrained eye, trucks can be easily mistaken for infantry vehicles and cattle paths misidentified as roads. Simple environmental factors like long shadows and snow can completely disguise an enemy army that would leap out of the picture to a trained analyst. Intensive training is required to see these details, and the specialists that emerged in World War II were the first of this new breed of specialists that worked well removed from the bombers that flew the missions. Contrary to the sea captain that used optics to sail his ships into a better firing position, neither the bombardier nor the photo interpreter knows how to fly the bomber. They were specialists at converting their observations into targets but not at operating a fighting platform. This specialization marks a turning point when optics and targeting changed from a skill that every military officer was expected to conduct into a role for experts with unique skills.

The Cold War accelerated this trend of increasing specialization. When World War II ended image analysis became the primary tool for peering behind the iron curtain and trying to determine the trajectory of Soviet intentions. In the early days, the United States employed an aggressive strategy of high altitude over flights of the Soviet Union with sophisticated cameras. Later when the Soviet Union launched Sputnik in 1957 it opened a whole new domain for the development of optics. "The U.S. collection array was largely built to respond to the difficulties of penetrating the Soviet target – a closed society with a vast land mass, frequent bad weather, and a long-standing tradition of secrecy and deception." (Lowenthal, p. 20) Space was the new frontier and America's cameras were quick to man the outposts of this netherworld. Satellites provided

a platform that could not be shot down like Gary Powers' U2, and provided a guaranteed opportunity to look at the Russians at least once a day, every day. The strategic community instantly monopolized this capability. Spaced-based optics augmented by aerial reconnaissance provided a flood of raw imagery that required interpretation.

Analysts by the hundreds were sequestered at Strategic Air Command (SAC), the long secret National Reconnaissance Office (NRO) and the even less well-known Office of Photographic Interpretation (OPI) to interpret this deluge of raw imagery. These analysts developed hundreds of targets for nuclear weapons and gave our leaders strategic insight into Soviet activity. However, the knowledge created by this multitude of specialists was cordoned into special plans for nuclear war that remained secret from the conventional military. (McKenzie, 2000) The Cold War need for draconian security was real, but concentrating targeting specialists in strategic missions isolated their highly capable skills.

It is the introduction of cruise missiles finally brought modern targeting expertise to general tactical forces. The American military first invested in cruise missile research based on the German V-1 design immediately following World War II, but the early effectiveness of ballistic missiles overshadowed nascent cruise programs because ballistic missiles were better suited to strategic nuclear deterrence. Thus, cruise missile research faded from vogue until Egyptian forces attacked and sank the Israeli destroyer Elath in 1967 with a modified Soviet Styx missile. (United States Tomahawk Cruise Missile Program) The U.S. Navy rekindled early interest in cruise missiles and deployed the Harpoon missile in its initial operational capability ten years later in 1977. (Harpoon Fact Sheet) This weapon system can be targeted from organic information collected from the launch ship, but the preferred method requires offboard sensors to target. Then in 1983 the Tomahawk Cruise Missile entered initial operational capability with

the fleet, providing the first conventional naval ordnance that relied exclusively on offboard targeting support. These cruise missiles were co-developed with the Air Force to provide a common sea launched and ground launched intermediate nuclear option in 1984 with conventional land attack missiles coming online in 1986. (United States Tomahawk Cruise Missile Program) The operational concept for conventional Tomahawks was envisioned to be limited strikes against high value strategic targets. Strategic targeting centers would provide ships their missions to load into the missiles with very limited information available to the shipboard personnel about the targets for their missiles. Due to the overwhelming success of Tomahawk missiles in the 1991 Gulf War demand grew for a Tomahawk missile that was more responsive to operational commanders and could be targeted on local information.

Requirements for lower operational control of Tomahawk cruise missiles and a concomitant desire to decrease the response time of manned aircraft strikes an American vision emerged for an interconnected battlefield. This concept, coined a "System of Systems" by then Vice Chairman of the Joint Chiefs of Staff, Admiral Bill Owens. (Owens, 2001) Since the "System of Systems" was first proposed it has moved through many different conceptual refinements, but the core vision remains the same – a desire to process and structure information that allows targeting to function independently of engagement. Thus targets are planned with great accuracy independent of the attack platform that will deliver ordnance.

Over the last twelve years the technology and organization necessary to bring this vision to life has evolved. Mass production of precision-guided munitions, further refinement of the Tomahawk missile and a host of new image collection capabilities provide a technological foundation for the complete separation of targeting and engagement. New targeting processes and a willingness to allow lower level discretion for the delivery of precision ordnance

has resulted in much faster response times to targeting information. It is now possible to attack specific objects with great precision from extreme range. Insight gained from data analyzed far from the battlefield can now have direct effect on the tactical situation. Thus, the second definitive characteristic of conflict in the information age is an American capability to engage almost any target, anytime.

The remainder of this a thesis examines how America can leverage the power of independent targeting and engagement to control the dramatically broader threat set posed by empowered individuals. Recall that individuals or small groups may not emerge as threats until their attacks are already in progress. At that critical moment, the application of independently targeted firepower may blunt the obvious attack. However, a process to emasculate the organization behind an attack is not proven. In order to apply firepower advantages, targets must be found. Similar to the United States' battle with Al Queda, the challenge is learning whom the adversary is and where they are located. Since adversaries in the information age will not likely mass on the battlefield in a 20th century formation, new strategies are required to attack networks that blend into the fabric of 21st century civilization.

II. WHAT TO ATTACK AND WHEN

If the systemic characteristics of Information Age conflict are a dramatically larger threat spectrum brought on by the empowerment of individuals, versus an American capability to engage with complete independence between range and accuracy then the central question follows. How can a capability to independently target and engage militarily suppress the networks of empowered, diabolical individuals?

A. HOW WE'VE ALWAYS DONE IT

Every nation would form a unique answer to any question about the proper application of coercive force because the way a country fights is inextricably linked with national identity and a particular conceptualization of war. American answers to questions about warfare draw upon our heritage, culture and perspective. However, our perspective and the intellectual choices we have made about the nature of war define the lexicon and organization for the answer. Therefore, an examination of the American military perspective on conflict is the right place to critique *the way we've always done it*.

The United States' capability to focus coercive power has evolved from the American perspective on war. Our political leaders and high-ranking warriors advocate specific intellectual choices about the nature of conflict. In turn, these choices create an American perspective on war and provide a common reference for decision-making in security issues. This chapter challenges the continued applicability of these choices at the core of American war making, and suggests that fundamental reform is necessary for victory in a system defined by empowered individuals and the independence of range and accuracy.

In 1986 Congress passed the Goldwater-Nichols Department of Defense Reorganization Act and began the democratization of security studies for the

U.S. Armed Forces. The new law mandated that officers receive Joint Professional Military Education (JPME) to be eligible for flag or general rank. (Goldwater-Nichols Department of Defense Reorganization Act of 1986) Prior to the Goldwater Nichols Act, formal education in security studies was available exclusively at service war colleges, national defense universities and security studies programs at a few civilian universities. However, this resident student model was insufficient to meet the Goldwater-Nichols requirement that all officers receive graduate level security education. Implementing Goldwater-Nichols required exporting military academics to a highly dispersed student audience that already "did more before nine in the morning than most people do all day."[2] To compensate, all of the service war colleges rolled out non-resident programs and distance education to teach the basics of strategy, policy, national security decision-making and joint operations. Students in the JPME program are exposed to the classics of strategic thinking and are encouraged to reach their own conclusions. However, there is an undeniable "check the block" mentality that pervades much of the curriculum material and has led inevitably to a simplified pedagogical approach to teaching warfare in just three courses.

To condense the study of war down to a three-course endeavor, curricular choices have been made that are consistent in their approach and versatile in application but oversimplify one of humanity's most complex activities. JPME begins with classic works by Clausewitz and Sun Tzu complemented by healthy injections of American politico-military history. A course in resource allocation and decision-making is added to this foundation and then the program ends with operational lessons from joint warfighting in the 20th century. The explicit framework across each of these courses is a three level model of warfare. At the top of this model strategy blends ends, ways and means into coherent plans for exerting coercive force. Subordinate to strategy is operational art that addresses the interaction of space, force and time to produce combat that leads to strategic

[2] U.S. Army recruiting slogan from mid 1980's.

objectives. Such battles are then won by superior tactics, which govern the interaction of forces engaged with an adversary. This logical and versatile framework produces a rote, almost obvious, answer to the question, "What wins wars?" Effective tactics win engagements. Engagements woven with operational art win campaigns. Campaigning with a good strategy wins wars. However, Oscar Wilde remarked, "The pure and simple truth is rarely pure and never simple." (Winokur, 2002) Unfortunately, the truth about winning wars is also impure and complex leaving much to be desired from the schoolbook answer linking tactics, operational art and strategy.

Suspend disbelief momentarily and examine the possibility that there is no predictable connection between strategy, operations and tactics. Success at one level of conflict may have no impact or even negative consequences on the level above or below it. For example, overwhelming tactical victory is no guarantor of strategic success. The United States never lost a battle in Vietnam and inflicted casualties on the adversary in a 50:1 ratio, yet America lost the Vietnam War. Israel and Great Britain seldom prevent tactical actions by the Palestinian Liberation Organization or the Irish Republican Army, yet there is no independent state of Palestine or Northern Ireland that heralds strategic success as a result of numerous successful tactical operations. The doctrinal answer for cases that do not fit the logical progression from successful tactics to fulfilled strategy is that the strategy must be wrong. However, equally false is the assumption that proper strategy is a guarantor of success. For example, the world may never know the strategy of the Taliban in Afghanistan, but America's apparent victory in 2002 is not irrefutable evidence that U.S. strategy was better. Only time will tell whether America's decision to pursue a global conflict with terrorists and an invasion if Iraq with strained international support will prove to be a good strategy.

The three level conflict model also fails to account for the disproportionate result of actions that do not fit neatly into strategy, operations or tactics. For example, insignificant or ineffective actions at the tactical level of conflict can have far reaching strategic impacts. In 1968, a single company of American soldiers under the misguided leadership of Lt William Calley killed approximately 300 civilians in the Vietnamese village of My Lai. Calley's actions were unquestionably reprehensible, and had no impact whatsoever on the tactical military parity between the United States, North Vietnam and the Viet Cong. However, when the details of this action exploded in the U.S. press Calley's bad decision-making and murderous tactics had a significant strategic impact on the war. (Public Broadcasting Service) Although Calley's crimes may be an extreme example they are still representative of disproportionate effects across the fictitious boundaries assumed to exist in the three level conflict model. General Charles Krulak artfully made this point as commandant of the Marine Corps in his concept of a 'Strategic Corporal'.

> In future wars, tremendous capability and lethality will be in the hands of the young corporal. Combine that with the immediate "CNN effect," and it turns some of those actions into strategic actions. That young NCO needs to be highly trained because what he does or fails to do may literally impact national policy. (Krulak, 1998)

The "Strategic Corporal" has such a powerful effect on all levels of war precisely because the levels themselves are an artificial construction inherent in the intellectual choices about conflict. This artificiality is inculcated into American officers, but Information Age conflicts will more than likely not conform to a three level construct.

Sun Tzu admonishes if you "know the enemy and know yourself, the victory is not at risk. If you know the Heaven and you know the Ground, the victory is complete." (Tzu, Sun) However, the ability to "know" is first predicated on an ability to map new information into an existing mental

framework. Unfortunately there is an adage, "If your only tool is a hammer, every problem looks like a nail." Thus, the current education system for military officers is arming them with a hammer to tackle complicated problems that might require new tools and specifically a new cognitive model in order to "know" Information Age opponents. This leaves a vast majority of American military officers with an education in strategy that is poorly aligned with the nature of future opponents.

Furthermore, how can a military system and bureaucracy spawned under a three level model create orders and plans that lead to victory in wars defined by a different set of rules? Unfortunately, the problem of how we have always done it is reflected in the exhaustive process for articulating military options. The remainder of this section will analyze the detrimental effect an illusory three level conflict model has had on the American military planning process and the misalignment between current doctrine and future requirements.

The axis of Information Age attack may not be apparent until the threat is imminent. The nature of the threat itself is uncertain. And, an attacker's very identity may not present itself until after an attack begins, or could remain cloaked forever.[3] However, the current Joint Planning Process emphasizes gathering information before conflict begins, analyzing it and presenting options that lead through objectives all the way to conflict resolution. The output of this process should be a scheme to synchronize the requirements necessary to put the plan in motion. Joint Publication 5.0, *Joint Doctrine for Campaign Planning* declares the fundamentals of a campaign planning include the following characteristics.

- Identify any forces or capabilities that the adversary has in the area.
- Identify the adversary strategic and operational centers of gravity and provide guidance for defeating them.

[3] For example, Moonlight Maze, a sophisticated computer network attack spanning several years was never officially attributed to any individual or organization.

- Clearly define what constitutes success, including conflict termination objectives and potential post hostilities activities. (Chairman of the Joint Chiefs of Staff, 2002)

How can the forces of the adversary be identified and quantified when the very identity of the adversary remains concealed? How can centers of gravity be determined when the motivations, organization and resources of the adversary are hidden from view? How can objectives be set and post hostilities considered when the scope and strength of the adversary may not be fully known? The very nature of this process demands a great deal of information up front that will probably not be available when an Information Age threat materializes from a previously unsuspected region of the world or worse, is shielded by the fog of cyberspace. In this dynamic environment, anticipating all possible moves by the adversary is no longer a plausible planning tool.

John Arquilla and David Ronfeld have drawn an extended analogy between industrial age processes that try to control for the maximum number of variables with the linear threats presented in classical chess. (Arquilla, 1997) In chess, pieces move in predetermined patterns and traverse across the board in linear segments. The goal of the game is isolation and imminent capture of a single high-value piece, the King. To accomplish this goal an opponents defensive forces must usually be attrited to allow sufficient maneuver room for pressuring the King's terminal defenses and subsequently checkmating his position. In a chess game "there are about 10^{40} possible positions; in most of them, one side is hopelessly lost." (Beeler, 1972) With the power of modern computing this finite number of possible moves can be optimized and computers now defeat the human chess world champion. (Newsweek, 1999) For military officers versed in air power theory this sequential process is clearly reminiscent of integrated air defense rollback followed by strategic attack and the subsequent checkmate of an opponent's critical infrastructure causing capitulation and acceptance of political demands. (Worden,)

Arquilla and Ronfeldt artfully contrast this style of fighting with the Asian game of Go. In Go, there are no high-value pieces. Each individual piece has the same value and action can occur anywhere on the board throughout the game. This uncertainty about initial conditions and non-linearity of movement create orders of magnitude more possible board positions in Go than in chess. (Worden) Furthermore, the number of positions on which the game can turn in the losing opponents favor is also dramatically higher. This explosion of complexity brought on by the nonlinear rules of Go leaves computers at a disadvantage to a human play with only modest amounts of skill. Such modest players routinely defeat the best computers, which cannot apply deterministic mathematics to the sheer volume of possible solutions. In fact a significant reward still exists for the first person to design a Go program that can beat a top-level player. (Russell and Norvig, p. 139)

The exploding level of uncertainty in Go and the inability to coordinate operations based on past observations is eerily similar to the new competitive landscape for conflict. Go contains an enormous increase in the number of threat options available compared to chess and parallels the exponential increase in threats brought about by the empowerment of individuals. Furthermore, the ability of Go players to set pieces anywhere on the board is reminiscent of independent range and accuracy. Go suggests that brute force optimization, reliant on exhaustive planning, is inappropriate for dealing with high uncertainty.

In conclusion, the way we have always done it no longer seems like an optimal solution for fighting networks. Although it is now possible to strike whenever and wherever desired, there are two serious gaps in the application of this force. First, the American model of conflict leads to a rigid concept of warfare that is increasingly irrelevant. And second, the existing planning process is not aligned with the nature of the adversaries America will likely face.

B. DEALING WITH UNCERTAINTY

Military planning in the Information Age is beset with challenges. There are a host of information requirements that will not be met, and yet a very real mandate to employ force. Carl Von Clausewitz wrote that "everything in war is very simple, but the simplest thing is difficult. The difficulties accumulate and end by producing a kind of friction. . . . This tremendous friction . . . is everywhere in contact with chance, and brings about effects that cannot be measured, just because they are largely due to chance." (Clausewitz, 1984) However, the application of precision firepower requires the selection of precision targets despite friction and uncertainty. The challenge therefore, boils down to finding targets in an organization that is not arrayed on the battlefield, but rather the organization is lurking in cyberspace or integrated into global civilization.

Recall that a core feature of Information Age conflict is a very limited ability to predict what will be attacked, when attacks will come, and worse, who is committing attacks in progress. For example, the international denial of service attack by the computer viruses NIMDA caused "damage that was estimated in the billions of dollars" according to Richard Clarke, chairman of the President's Critical Infrastructure Protection Board. (Schwartz, 2002) However, "the creator of NIMDA, which attacked computers and installed 'back doors' for subsequent hacker attacks, has never been identified." (Schwartz, 2002) While simple denial of service attacks may not warrant military action, the ability of such perpetrators to remain anonymous in indicative of the elusive threats that American forces will soon be called to confront. The success of such actors to execute successful attacks and remain concealed creates a bleak outlook on the ability to "know." Such failure to discover targets demands an exploration of emerging science with the goal of discovering mathematics to shed light on the dark uncertainty created by empowered individuals.

Ideally, science would reveal a process for applying American advantage in firepower to overcome the shortfalls of an irrelevant perspective and an ill suited planning process. Despite the uncertainty created by empowered individuals the authors of this thesis wanted hard science to provide the foundation for a targeting strategy applicable across a greatly expanded threat spectrum. However, the presence of human beings is the only feature common to every fantastic threat that might emerge.

At first, presence of human beings seemed obvious, and somewhat useless. Of course, there are going to be human beings behind future attacks, but this doesn't provide much of a foundation for the application of force designed to reveal the identity of those humans. However, diligent research on this subject revealed that network science and the emerging field of network mathematics can illuminate natural laws of human organizations that are exploitable for targeting.

In 1998, Hawoong Jeong created a web robot to map out the World Wide Web for Albert-László Barabási's research group at the University of Notre Dame. (Barabási, p. 220) Barabási was researching networks and wanted to know what the structure of the Internet looked like. However, when Jeong's robot returned it painted a picture that ran counter to fifty years of theory. The network returned by Jeong's robot revealed

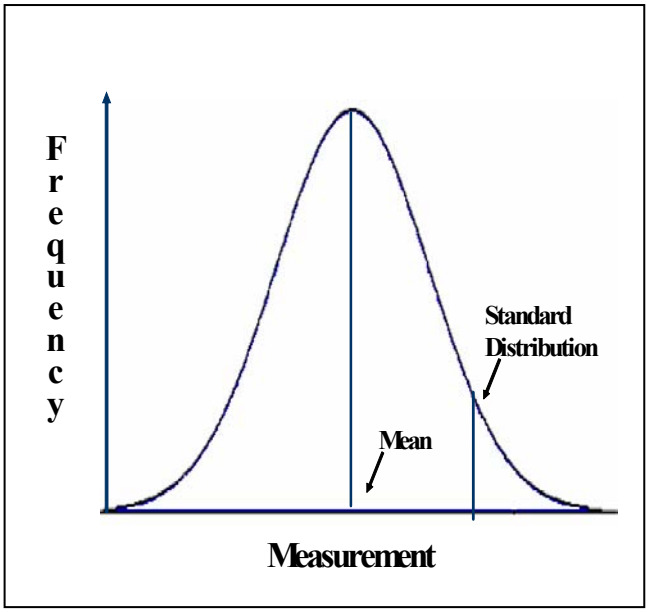
> …a hierarchy of hubs that keep these networks together, a heavily connected node closely followed by several less connected ones, trailed by dozens of even smaller nodes. No central node sits in the middle of the spider web, controlling and monitoring every link and node. There is no single node whose removal could break the web. A scale-free network is a web without a spider. (Barabási)

The term scale-free used by Barabási is worth further explanation. Most natural systems exhibit some scale. For example, human IQ is one of the most well known distributions. The median or average IQ is 100 and the standard

deviation is 15. (Devore, 2000) Similarly, human height ranges between an absolute maximum of 7.5 feet and a minimum of 3.5 feet. Distributed among these extremes the majority of men and women fall in the middle. This means is that human height and IQ have a scale, with most individuals normally distributed in the middle of the scale and a much smaller number of individuals at the extremes of intelligence and height.

> Measurement errors in scientific experiments, anthropometric measurements on fossils, reaction times in psychological experiments, measurements of intelligence and aptitude, scores on various tests, and numerous economic measure and indicators. Even when the underlying distribution is discrete, the normal curve often gives an excellent approximation. In addition, even when the individual variables themselves are not normally distributed, sums and averages of the variables will under suitable conditions have approximately a normal distribution. (Devore, p. 159)

Normally distributed systems are so prevalent in nature that we often take them for granted. However, changes to this norm would be immediately apparent. For example, if human height were a scale free system, then every once in a while you would meet a 200 foot tall person. In keeping with this tradition nearly all science of networks prior to Barabási's work had assumed nodes in a network conformed to a normal distribution. Some nodes would be a little more connected to others, but all of them would fall within some random scattering around an average. Imagine the surprise among Barabási's team when their web robot returned a graph that



overturned everything that had been previously assumed about network topology.

Since Barabási's breakthrough work in 1998 networks are pervading every element of scientific discussion and even pop culture. "At the heart of Internet research and cell biology, the questions are similar. The first step is to map out the network behind these systems. Then from these maps we need to infer the laws that govern the network." (Barabási, p. 193) In popular culture the Six Degrees of Kevin Bacon game, in which players try to link any actor in Hollywood to Kevin Bacon through associations with other actors, was immensely popular at college campuses and even morphed into an extremely trafficked website. (Barabási , p. 62) Similarities exist between college drinking games, the Internet and cancer research because Barabási's findings highlight new fundamental characteristics of the natural world.

Figure 1. Normal Distribution.

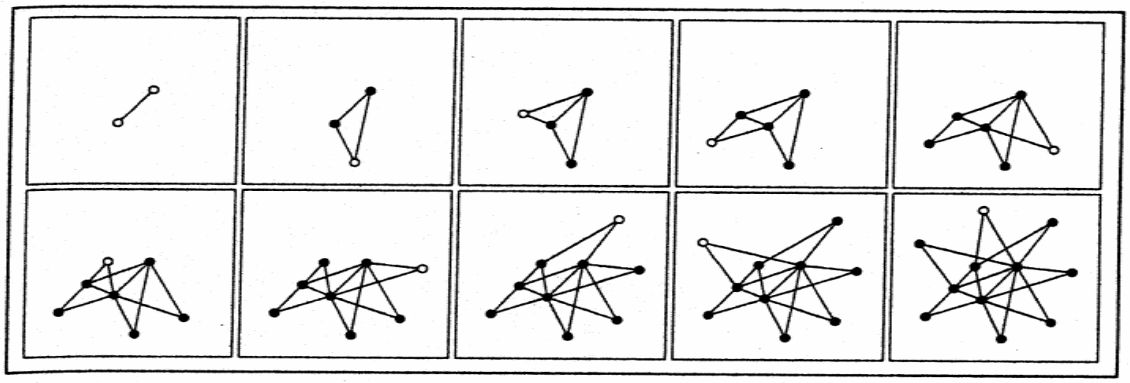


Figure 2. The Birth of a Scale Free Network.

The scale-free topology is a natural consequence of the ever-expanding nature of real networks. Starting from two connected nodes (top left), in each panel a new node (shown as an empty circle) is added to the network. When deciding where to link, new nodes prefer to attach to the more connected nodes. Thanks to growth and preferential attachment, a few highly connected hubs emerge. [From :Barabási, 2002, p. 87]

Scale-free networks are created when systems grow over time and have a preferential attachment system for new nodes. (Barabási, p. 86) Two

characteristics govern scale-free systems. First, all nodes in the system cannot be present at the organizing moment. Rather, nodes are added in succession and the network must grow over time. Second, when new nodes join the system they do not randomly connect. Instead nodes have a preference for attaching to a particular node over others. These preferred nodes are said to have "high fitness." (Barabási, p. 96) Together these two governing rules determine that most natural systems have a network topology.

> Networks are by their very nature the fabric of most complex systems, and nodes and links deeply infuse all strategies aimed at approaching our interlocked universe. (Barabási , p. 222)

So when looking for commonality to describe the nature of emergent threats in Information Age conflict, inevitable human involvement provides a network topology. Well before Information Age threats organize for the final execution of their attack they must organize, train and prepare. Whether the threat is cyber attack, terrorism or economic sabotage human beings behind the attack must develop plans, study the target and gather resources. Bonnie Erickson's study of secret societies reveal that this activity is coordinated among individuals with trusted prior contacts. (Erickson, pp. 188-210) Each successive contact within a closed system adds a new link in the social network of the attacking organization. Because these organizations are built over time, the growth criterion for scale-free networks is satisfied. Secondly, the authors propose that new members joining an organization have a natural desire to attach themselves with the most influential member. For example, a new recruit into Al Queda would more than likely aspire to work at Bin Laden's right hand. This gives Bin Laden a very *high fitness* in the system and satisfies the criterion that a preferential attachment system probably exists in future adversaries. With the two criteria met for scale-free systems American military planners now know a great deal about the organizing principles behind the immediately visible attackers.

Following the terror attacks on September 11th, 2001, Valdis Krebs, a management consultant who normally uses network theory to analyze corporate communications produced a map of the terrorists' "covert network using data available from news sources on the World Wide Web." (Krebs, 2003) His work clearly shows a scale-free system with Mohammad Atta as the dominant hub.

Figure 3. September 11th Highjackers Organization (From: Valdis, Krebs).

Krebs' work is chilling validation that terrorist organizations form scale-free networks. However, as Barabási's shows, any system that grows over time and has preferential attachment will form a scale-free network. Since Information Age threats will be composed of individuals that plan and organize before they reveal themselves, discoveries about the strengths and weakness of the scale-free topology provide critical insights necessary to fight in the Information Age. Therefore, a strategy for targeting networks will create a foundation for attacking the wide variety of threats plausible in the Information Age.

Finally, it is an important point to mention that Krebs' network map was built over the course of several months following one of the most intensive investigations the world has ever seen. It is completely feasible that the pace of learning acceptable for Krebs will not be fast enough to respond to future threats. Therefore, any targeting strategy for networks must not only illuminate ways to defeat these organizations, but also provide a way to learn about them faster.

C. TARGETING NETWORKS

When Information Age threats are discovered a nation-state has several instruments of power at its disposal. These tools include political, economic, military and law enforcement actions. However, when the damage is great or the threat is grave military force must provide a final decisive tool against external threats. The American people should expect no less than it military be capable of "defending the of engaging "all enemies both foreign and domesting." Therefore, military forces must ready themselves for war against networks; wars in which traditional notions of territory, victory and battle may not apply. To address this threat the aforementioned network structure of potential adversaries provides a common similarity between the diverse threats that could materialize in the near future. This section will address the inherent strengths of networks and then focus on the ineluctable weakness of scale-free systems – reliance on hubs for connectivity. This weakness presents a salient targeting fundamental

and the appropriate focus for network attack. However, it also introduces another challenge. If hubs are the target, how do you find hubs?

It is not an accident that natural systems form scale-free networks. This organizational form presents an enormous advantage in a dangerous world. Loosely connected nodes make up the majority of a scale-free network. Then connecting many nodes, the system hubs act as the gateway connecters between different parts of the system. When random failure occurs in a scale free system there is a high probability that one of the nodes will fail and not a hub.

> If I blindly pick ten balls from a bag in which there are 10 red and 9,990 white balls, chances are ninety-nine in a hundred that I will have only white balls in my hand. Therefore, if failures in networks affect with equal chance all nodes, small nodes are far more likely to be dismantled, since there are many more of them. (Barabási , p. 114)

The result of this resilience is that scale-free systems are extremely fault tolerant. Whether the system under random attack is cancer, a pack of water buffalo or the Internet the scale-free topology ensures that the system will survive the loss of many nodes. However, concentrating responsibility on the hubs to support the network also creates a serious vulnerability of network systems under deliberate attack. "Taking out a hierarchy of highly connected hubs will break any system." (Barabási , p. 121)

For example, the Internet is extremely fault tolerant. At any given time there are hundreds of malfunctioning electronic routers responsible for passing messages. However, the system continues to provide uninterrupted service because the hubs of the Internet route traffic around the failing nodes. On the other hand deliberate attack against the hubs of the Internet could bring the entire web to its knees. In October of 2002 an attack attempted to do exactly this. The article explaining the attack highlights this vulnerability. "Most of the Internet's traffic must pass through one of several dozen core routers, and if they

were somehow crippled simultaneously, the Net would grind to a halt." (Sullivan, 2003) The question remaining addresses whether hub attack against a human organization will produce the same detrimental failures?

Kathleen Carley of Carnegie Mellon University notes that isolation strategies against network organizations produce significant performance degradations. (Carley) Going back to Valdis Krebs' map of the September 11th highjackers he points out

> We do not know all of the internal ties of the highjackers' network, but it appears that many of the ties were concentrated around the pilots. This is a risky move for a covert network. Concentrating both unique skills and connectivity in the same nodes makes the network easier to disrupt – once it is discovered. (Krebs, p. 14)

Although these examples show that disruption decreases organization performance, the term "decreased performance" may not have the same military appeal as "unconditional surrender." However, military planners must learn to adapt expectations for conflict termination to the reality of new adversaries. In the United States' global war with Al Queda it is highly unlikely that a surrender document or peace treaty will ever be signed. The war aim is suppression, annihilation and decreased organizational performance. Similar to attacks on the Internet, the goal is to bring Al Queda to its knees, but we may never fully eradicate the organization. Therefore, the American military must constantly seek to employ the advantages of independent range and accuracy against the universal weakness of scale-free networks – the hubs.

With network hubs identified as the target for American firepower, the next question is "Where are the hubs?" Krebs suggests that the best possible course of action for this task is to identify possible suspects then observe them to see where those leads connect. (Krebs, p. 15) Additionally, he is adamant that the "best method is for diverse intelligence agencies to aggregate their individual

information into a larger emergent map." (Krebs, p. 15) However, in a military context this strategy is not satisfying.

Krebs opinion is plagued by the failure to apply military thinking to a problem that has traditionally been regarded in criminal terms.

> In other words, our leaders (and we as their citizens) have in the past been, and in disturbing numbers remain, prepared to treat terrorists as being on par with smugglers, drug traffickers, or, at most, some kind of political mafiosi, rather than what they have in fact been for almost half a century: organized, highly trained, hugely destructive paramilitary units that were and are conducting offensive campaigns against a variety of nations and social systems. In truth, international terrorism has always been what its perpetrators have so often insisted: a form of warfare. And although American leaders and the international media were more than willing after the September 11 attacks to announce that the United States was in fact at war, a truly unified, comprehensive and resolute military strategy for conducting war was slow in formulation and has proved difficult to maintain. Confusion and arguments over terms and concepts, goals and strategies, have hampered the prosecution of America's response from the start. (Carr, 2002)

The authors contend the reason for confusion and the lack of coherent strategy is due to a missing cognitive framework in the U.S. military for fighting networks, and a planning process that is not aligned for iterative battle against a dynamic system. Therefore, the problem in Krebs' solution is that it yields too much initiative to the adversary.

One of the first things every midshipman learns in their initial year at Annapolis is that you never yield the initiative. (Clark, 2001) When mining a huge database or waiting to "see where it leads," significant observation of the network is only possible when the nodes act. Thus the adversary has the initiative because they are setting the timetable for observable opportunities. Krebs even points out that "unlike normal social networks, strong ties [between nodes] remain mostly dormant and hidden to outsiders." (Krebs, p. 14)

Furthermore, the adversary determines the conditions, timing and method of communication. With so many advantages leaning toward the adversary even a first year midshipmen should figure out that this tactic is too dependent on a cooperative target to form the foundation of a coherent **military strategy** for defeating networks.

Krebs is not alone in his opinion that better surveillance and better databases are the keys to defeating future adversaries. The Defense Advanced Research Project Office (DARPA) recently received funding to build a Total Information Awareness (TIA) system that will "demonstrate innovative information technologies to detect terrorist groups planning attacks against American citizens, anywhere in the world." (DARPA) Senator Richard Shelby, Vice Chairman, Senate Select Committee on Intelligence hailed TIA as

> …precisely the kind of innovative 'out of the box' thinking of which I have long been speaking – and which American have a right to expect from their Intelligence Community in the wake of a devastating surprise attack that left 3,000 of their countrymen dead. (Shelby)

However, reactive measures like data mining and better surveillance allow the adversary to control too many variables. Furthermore, it leaves the U.S. on a permanent defensive, awaiting the next attack or move the adversary. This is not only an uncomfortable waiting game. It also runs counter to the last fifty years of strategic thought that prizes the offensive.

The balance between offense and defense in warfare has occasionally shifted advantage from attackers to defenders and vice versa. Beginning in the mid 1800's defense had a clear advantage on the battlefield. For example, the gruesome losses of the Union Army attacking Lee's Army of Virginia during the American Civil War were a bellwether of the defensive strength afforded by rifled guns. Later, in World War I the absolute failure of maneuver on the battlefield and the subsequent stalemate between trenched forces was a direct

result of a defensive machine gun's to cut attacking infantry units to bits. However, when the German army pioneered the integration of radios, aircraft and tanks and a new organizational structure into Panzer divisions maneuver gave advantage back to the offense. This was convincingly demonstrated by the rapid fall of France in 1940 despite millions of French francs poured into defensive fortifications at the Maginot Line. There is no evidence to suggest that new technology or doctrine has shifted advantage back to the defense. In fact, this thesis has adamantly argued that America's unique advantage in the Information Age is the ability to take the offensive with independently operable targeting and engagement systems. Therefore, ceding the initiative to terrorists, hackers or other network adversaries is tantamount to taking the strategic defensive, waiting patiently for them to make the first move. This is not to suggest that better surveillance and advanced databases are not useful tools, but rather a defensive strategy does not address the threat. Power in the Information Age resides in maintaining the offensive: finding a way to attack while learning about hidden nodes.

Another key statement from Krebs' outstanding work on the September 11th organization is "The less active the network, the more difficult it is to discover." (Krebs, p. 14) Obviously the antithesis to this statement also holds true. The more active the network is, the easier it is to discover. However, this is not the steady state for a covert network. Covert networks actively pursue secrecy and thus communicate only when absolutely necessary to coordinate activity. (Baker and Faulkner, pp. 837-860) Therefore, stimulus that creates higher network communication activity has a concomitant effect of increasing the observable signal strength of network participants. Because communications across the network will more than likely travel through one or more hubs to reach its destination, the secret to finding hubs is to get the nodes communicating.

The authors term this targeting strategy "Stimulus Based Discovery." We claim that networks can be stimulated to reveal their topology and in so doing provide a map of targets for the application of force. Additionally, the authors claim that stimulus based discovery leads to targeting information faster than stand-off observation or other methods that rely on the adversary to communicate at their leisure.

Stimulating a network and forcing nodes to compensate for changes in the environment enhances the effectiveness of an observation system because the search parameters can be narrowed. For example, eliminating a terrorist network's financier would force cell operatives to seek out other methods of acquiring money. This could take several forms such as credit card fraud, bank robbery or attempts to make contact with financiers they are unfamiliar with. Whereas it might be very difficult to intercept communications between a terrorist cell leader and a financier with whom he shares a long personal history the difficulty of detection is reduced if the cell if forced to conduct visibility activities to raise finances. In this example there are already systems in place to detect credit card fraud and armed robbery, and these higher "signal strength" activities are more easily detected than covert communications between old friends. Similarly seeking out a new financier requires adding new links to the network that therefore makes the network more detectable. With a stimulus based strategy as the organizing principle for redefining attack, a tool like TIA becomes very important in detecting the results of stimulus.

The options for orienting intelligence collection are large, but when the network is stimulated by U.S. action the search for observable activity can be focused, and with the addition of only a few scaling parameters the likelihood of detection should improve. In March of 2003, this exact phenomenon was on display in the high profile hunt for the leaders of Al Qaida and the capture of operations chieftain Khalid Shaikh Mohammad.

> Officials at the National Security Agency also listened attentively to their vast global array of electronic eavesdropping satellites, waiting for an expected flurry of e-mails and cell phone calls among Al-Qaida members. Authorities watched for the movement of cell members seeking cover, particularly those believed to be direct contact with Mohammad. (Myer)

In this case discovery then fuels more accurate stimulus creating a chain of stimulus/reaction pairs leading to a quicker map of the network topology.

The questions in this thesis began with an examination of two characteristics that will define Information Age warfare. First, the list of possible threats faced by future U.S. forces will be dramatically larger than the state-centric threats of the Industrial Age. This additional complexity is brought on because the flow of power to individuals allows small groups to endanger states in a way that has not existed for over three hundred years. Second, advances in information technology and refined processes for the application of force allow U.S. military units to break the historical link between range and accuracy. With precision-guided weapons it is now possible to operate targeting and engagement system in separate locations within unique processes. However, the application of this force could be rendered less effective without new concepts to identify valid targets among networked adversaries that will likely be misunderstood by Industrial Age metrics.

Unfortunately, in a well-intentioned effort to expose more military officers to classical works on strategy and operational art the professional education curriculum has reduced warfare to a cookie cutter formula. This gross simplification does little to inculcate America's warriors with a new mindset to fight networks. Furthermore, the planning processes that exist are not aligned to leverage America's strengths against new adversaries that do not conform to traditional measures for evaluating an adversary state. To compensate for this shortfall, new findings in network science demonstrate that human systems built over time self-organize into scale-free networks. These networks are composed

of nodes and links with some high fitness nodes, called hubs, that acquire an extraordinary number of links while most nodes remain loosely connected. Scale-free systems are extremely robust to random failure, but are susceptible to focused attack against the hubs that hold the system together. America's independent targeting and engagement systems are ideally suited to attack the hubs in such a network, but finding the hubs presents a daunting challenge.

Current efforts to find the influential members in a network organization rely on improvements to existing systems in information management and surveillance. However, this solution contains two significant flaws. First, this approach cedes initiative to the adversary, and second, it requires a defensive strategy when there is no evidence to suggest defense is the stronger form of warfare in the Information Age.

Another way of finding hubs proposed by the authors is called, Stimulus Based Discovery. In this form of learning, hubs are found by stimulating the network to increase the amount of detectable activity. This detection enhances the capability to detect nodes and hubs by focusing collection in time and space to the likely network response to stimulus. And most of all, Stimulus Based Discover retains the initiative and puts the adversary network on the defensive.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CASE STUDIES IN STIMULUS BASED DISCOVERY

Stimulus Based Discovery seeks to map the hubs and nodes in a network faster than standoff observation. Rather than put surveillance in place and watch a suspected node to learn its connections, Stimulus Based Discovery requires the observer to act in a way that forces a reaction from the node under observation. The exact nature of this reaction may be unknown, but several possible reactions can usually be anticipated. Thus, surveillance tools can be focused to look for the expected reactions, and increase the likelihood of detecting denied information. Moreover, the observer is now actively setting the pace and schedule for observable events and putting his opponent on the defensive.

Kenneth Waltz states the value of a model in political science is based on its ability to explain or at least predict. (Waltz, 1979) Therefore, if Stimulus Based DiscoverY is to be seriously considered as a theory and strategy for Information Age conflict it should explain several historical case studies. This chapter establishes the validity of Stimulus Based Discovery by using it to explain past events. However, before addressing specific examples, it is important to discuss exactly what stimulus consists of in the context of this theory.

Stimulating the adversary network has already been defined as some action that increases the ability to detect and map the nodes and hubs in scale-free networks by generating increased observable activity in the system. There are many forms stimulus can take, but it must be directed at either nodes or links. For example, stimulus applied to a terrorist network might eliminate one of the terrorist nodes and thereby force the system to adapt to the loss. Affecting a link could mean denying the communication signal between two nodes by jamming or destroying the communication infrastructure required to complete the message. Both of these examples require explicit denial or removal of the node or link. In these examples the physical terrorist agent is removed or the

actual communication system is suppressed. Therefore, one way of affecting nodes and links is to change explicit physical reality. An explicit effect destroys or disables a node or link.

Nodes and links can also be cognitively distorted as well as eliminated from the explicit physical world. While explicit stimulus of nodes and links can have outstanding results for network discovery, cognitive distortion attacks on the network generates equally positive results in mapping the nodes and hubs of a scale-free system. Therefore, there are four different ways to stimulate a network. The four method; explicit nodal stimulus (quadrant I), explicit link stimulus (quadrant II), cognitive nodal distortion (quadrant III) and cognitive link distortion (quadrant IV) are each depicted below.

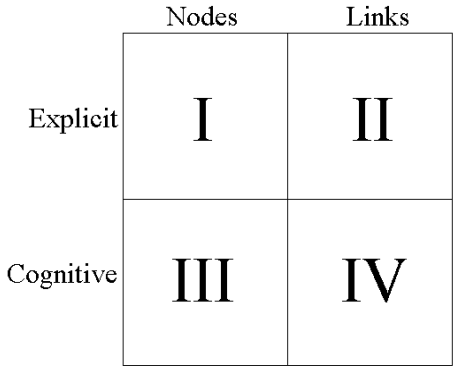


Figure 4. Stimulus Matrix with Four Possible Tactics.

Examples later in the chapter will examine case studies from each quadrant, but as an introduction to the idea of explicit and cognitive stimulus consider the following example. Suppose you were the target of a Stimulus Based Discovery attack with the objective of eliminating your professional network. Also assume that surveillance inside your office is denied for some reason (simulating a difficult to penetrate organization). So simply watching you at work is not an option for mapping your network. With direct observation at work unavailable, you can still be stimulated with a tactic from each quadrant

and this will lead to a map of your organization's structure. For example, an explicit nodal stimulus, such as killing or kidnapping you (quadrant I) would stimulate your professional network. Later that day this stimulus would cause another node to emerge from a co-worker or superior that calls your house to find out why you didn't show up for work. Similarly, you are probably linked to your job by the car you drive to the office. If that car were explicitly disabled (quadrant II) you would probably call your boss to tell them you were going to be late, and if you had a client meeting or worked in a team of other employees you would probably call them too. This stimulus would force you to communicate and present an opportunity to add another node or two to the map. To conduct this communication, you might e-mail, call on your house phone or even use your cell phone. Explicit link stimulus could also include disabling one or more of those communication systems to funnel your connection onto to the exact path, such as your cell phone, which has the most penetrated surveillance. Thereby enabling the highest fidelity intercepts of the people you communicate with and adding your closest links to the network map.

Now consider how you could be stimulated in the cognitive domain. If you were somehow convinced through a false weather report or a deceitful phone call that you did not have to come into work this morning (quadrant III) then cognitively distorting reality perceived by your node would generate the same result as explicitly disabling you. Someone at the office that knows you do not really have the day off will inevitably call to inquire why you are not at work. If surveillance is ready to intercept this communication then the distortion between your perception of reality and the explicit reality known by other nodes (your co-workers in this case) serves to successfully add another link to the map.

Finally, you are linked to your coworkers and superiors on many different channels in both the physical and the intangible realm. These links include telephone connections, e-mail correspondence, and even the highway that leads

from your home to your office. Suppose a link between you and your business associates was exploited to create a cognitive reality that was not aligned with the explicit situation (quadrant IV). For example, e-mail could be sent to everyone in your address book announcing your sudden resignation. Many in your company receiving the e-mail might not even know who you are, and they would quickly delete the mail. However, your boss and your closest co-workers would most assuredly be concerned with your sudden shift in attitude. Many would immediately write back to you or call you on the phone to discuss your situation. You might tell them it was all a hoax, but if surveillance were in place the map would already include each respondent and perhaps some additional information that annotates your relationship with them based on the tone of their reply.

In the opposite case, where stimulus based techniques are not employed, the learning process is more likely to proceed at a slower pace with less certainty about connections. If your home phone were covertly tapped along with your e-mail then surveillance teams would listen for clues that demonstrate who you are connected with at work. However, if you are like most people you do not call work in the morning unless something is out of the ordinary and you do not call after you leave because you just spent all day there. If they watch who you go to lunch with you might spend that time with an associate from a different department that has nothing to do with your professional network, or worse, you may go to the gym everyday and grab a sandwich on the way back without talking to anyone about who you know at the office. There are literally millions of situations that could arise in a surveillance problem, but it follows logic that Stimulus Based Discovery maps a network faster and more accurately. However, logic alone does not demonstrate the theory in practice. Therefore, case studies follow for each type of stimulus discussed in the previous example.

A. MEDELLÍN DRUG CARTELS (QUADRANT I)

In 1989 the U.S. Central Intelligence Agency and U.S. Special Forces began covert operations in Columbia to assist the national government's effort to enforce the rule of law on the cocaine cartels. "In the fall of 1989, the U.S. embassy in Bogatá was not sure exactly how the Medellín cartel worked, or even who was in charge" (Bowden, 2001). The leading assumption was that an individual named José Rodríguez Gacha was in charge of the cartel. Therefore, Gacha was the first target for U.S. covert surveillance in Columbia and was quickly located by U.S. Special Forces communications operatives. Gacha's location was passed on to Columbian National Police who, despite a bungled first attempt, successfully killed Gacha with assault helicopters. This action explicitly removed Gacha from the cartel network.

Although it was not intended, Gacha's death provided an ideal stimulus in the leadership network of the Medellín cartel. "His death prompted a torrent of phone calls to and from Pablo Escobar" (Bowden, p. 83). The cartel was reacting to the stimulus and reorganizing itself after the loss of a key participant. In this flurry of activity it became clear that Gacha was an important member of the cartel, but certainly not the kingpin.

> The more [U.S. Special Forces] listened over the next few weeks, the more they realized that Pablo [Escobar] had been the man in charge all along. Always deeply concerned about his public image, he had evidently been content to let Gacha be perceived as the chief bad guy (Bowden, p. 84).

This example demonstrates several important characteristics about Stimulus Based Discovery. First, U.S. information on the cartel was minimal and the little bit that was known pointed to the wrong person as the network hub. Second, prior to the stimulus ties between Gacha and Escobar were strong but dormant. And, as pointed out by Valdis Krebs in his discussion of the September 11th highjackers, strong ties in criminal organizations are likely to remain

"dormant and hidden to outsiders." (Krebs, p. 14) Therefore, prior to Gacha's death, Escobar was able to mount a successful misinformation campaign by ensuring that the abundance of information continually pointed to Gacha as the cartel hub. Only when the network was stimulated, did Pablo Escobar emerge as the cartel leader. Stimulating the Medellín drug cartel by explicitly removing a node exposed the structure that Pablo Escobar was trying to keep masked.

B. STATE SPONSORED TERRORISM (QUADRANT II)

Terror networks represent one of the clearest examples of strategic threats that organize and prepare outside the bounds of the state-centric model. However, it is common knowledge that many states encourage, and in many cases support terrorist organizations. Therefore, a link exists between some states and the terrorist networks they sponsor. President George Bush brought this point to the forefront of America's ongoing war against terror in his September 20th, 2001 speech.

> We will pursue nations that provide aid or safe haven to terrorism. Every nation, in every region, now has a decision to make. Either you are with us, or you are with the terrorists. From this day forward, any nation that continues to harbor or support terrorism will be regarded by the United States as a hostile regime. (Bush, George)

The strong stance against state sponsored terrorism is justified because nations that provide safe haven for terrorists link these network threats with the resource gathering capabilities of states. The combination of a state's resources and a terrorist organization's ability to strike key interests of its adversaries is a dreadful combination. Therefore, the United States has constantly sought to eliminate these links.

> On the late evening of 15 April and early morning of 16 April 1986, under the code name El Dorado Canyon, the United States launched a series of military air strikes against ground targets inside Libya. The timing of the attack was such that while some of the strike aircraft were still in the air, President Reagan was able to

> address the US public and much of the world. He emphasized that this action was a matter of US self defense against Libya's state-sponsored terrorism. In part, he stated, "Self defense is not only our right, it is our duty. It is the purpose behind the mission...a mission fully consistent with Article 51 of the U.N. Charter. (Global Security Org)

President Bush's clear denunciation of state sponsored terrorism and President Reagan's attack on Libyan support for terrorism both demonstrate explicit suppression of a link between states and terrorists represented by quadrant II activity in the stimulus based discovery tactics matrix. This suppression has the obvious goal of removing a terrorist organization's ability to gather resources from a state, but also demonstrates stimulus based discovery.

Once terrorists can no longer rely on a state to funnel finances, logistics and arms to their organization, they must satisfy those requirements through other methods, which increase the ability to detect nodes in the terror organization. For example, following President Bush's clear demand for an end to state sponsored terrorism the President of Pakistan, General Pervez Musharraf, met with his top advisors to discuss Pakistan's options. The General realized that U.S. dedication to the war on terrorism left no room for Pakistan's longtime support for militant Islamic groups that routinely invaded Indian held Kashmir.

> [Musharraf] made his second major policy change, vowing to rid his country of Islamic extremists who for years have relied on clandestine financial and military support from the army. (McCarthy, 2002)

The result of Musharraf's policy was that radical groups no longer received illicit funding directed to them by the state. Left without state sponsorship network organizations faced an interesting paradox. To raise resources they had to forego secrecy and make public or semi-private requests for resources. In Pakistan this manifested itself in the mosques and bazaars on the northeast frontier with Kashmir.

> Every Friday at lunchtime, as men gather at the mosques near Mardan for prayers, a Lashkar commander makes an impassioned speech about the fight in Kashmir and openly collects thousands of rupees in donations. (McCarthy)

Network commanders coming out of the mountains to make personal pleas for resources clearly demonstrates the effectiveness of explicit suppression on the link between states and network threats. In the Pakistan case, the flow of net resources to the terrorists is not overwhelmingly disturbed, but nonetheless, nodes in the network are revealed that would have remained deeply buried without breaking the link between the Pakistani government and the radical network.

C. OPERATION 'SHAKE THE TREE' (QUADRANT III)

Following the U.S. led victory in the Gulf War to liberate Kuwait the UN Security Council passed Resolution 687 on April 3, 1991. This resolution set forth the formal terms for a permanent cease-fire and required Iraq to renounce and condemn terrorism, repatriate all prisoners, restore all seized and stolen property, establish a fund based on oil revenues as a source for reparations payments to Kuwait, accept a continued arms and economic embargo (except on food, medicine, and essential civilian needs), and accept international verification of its WMD program eradication. This final element required Iraq to accept the destruction, removal, or dismantling of all biological, chemical and nuclear weapons; all research, development and support facilities associated with these weapons; all stocks of chemical and biological agents; all ballistic missiles with ranges exceeding 150 kilometers; and all production and repair facilities associated with the manufacturing of such missiles. It linked Iraqi compliance to Iraq's ability to export oil and other materials by stating that once the Security Council verified that Iraq had completed the required actions, the UN prohibitions against the export of commodities and products originating in Iraq would have no further force or effect (Cordesman, p. 290). Saddam Hussein

accepted Resolution 687 on April 6th, prompting the Security Council to declare a formal cease-fire on April 11.

To assist in the implementation of Resolution 687 the UN established United Nations Special Commission (UNSCOM) for the purpose of planning, coordinating and executing the destruction of Iraq's weapons of mass destruction. Rolf Ekéus, a life-long civil servant known for his diplomatic skills, and no-nonsense attitude, was chosen as the executive chairman for UNSCOM. Ekéus reported directly to the UN Security Council and had broad authority to act independently. His staff, composed of experienced inspectors and technical experts, created a force of inspectors focused on the verifiable disarmament of Iraq. Robert Gallucci, Ekéus's deputy chairman, points out that the inspections carried out under UN Security Council Resolution 687 were not the same as IAEA safeguards inspection. "Those inspections were quite unique and they followed from the peace of the victor" (Gallucci, p. 8). Early on it was clear that UNSCOM was putting together a new breed of non-proliferation inspections and would settle for nothing less than complete Iraqi compliance with the UN Security Council.

From the beginning, Iraq began to deceive UNSCOM and IAEA in an effort to retain control of key elements in their WMD programs. "As early as April 5, 1991, Iraqi forces were detected salvaging equipment for missiles and weapons of mass destruction, as well as cleaning up suspect sites" (Cordesman, p. 291). The pattern of Iraqi deceit and deception and reports from UNSCOM that Iraq was not fully cooperating resulted in the passage of a stronger UN Security Council Resolution on August 15, 1991. However, the extent of Iraq's deceit was not revealed for the world until August of 1995, when Lieutenant General Hussein Kamel defected to Jordan. Kamel had been a supervising minister for military industry and had led part of Iraq's weapons of mass destruction program. He was also Saddam Hussein's son-in-law. Kamel

cooperated fully with the media, foreign government intelligence agencies and UNSCOM. "He revealed how Iraq was misleading the United Nations weapons inspectors through a systematic program of deception and concealment" (Ritter, p. 47). Despite an Iraqi 'full, final and complete disclosure' of its WMD program only weeks earlier, Iraq promptly invited Chairman Ekéus back to Baghdad to discuss new information. Eventually these talks led the Iraqis to deliver over a million pages of documentation to UNSCOM that were reportedly stored at the now defected Kamal's house. Kamal's statements and his document cache indicated once and for all that Iraq was successfully concealing its activity and that the current method of inspection was not effective.

Ekéus, UNSCOM's chairman, estimated that he had been unable to make a definitive accounting of Iraq's weapons of mass destruction because their work was marginalized by a secret Iraqi concealment organization. From the Arabic, it was called the Apparatus of Special Security, and Saddam Hussein's younger son, Qusay, directed it. Reporting to the umbrella group were the inner core of the president's protective agencies: the Special Security Organization, the Special Presidential Guard Unit and Special Republican Guard (Gellman, p. 8).

The concealment organization was obviously not a declared agency of the Iraqi government and therefore its nodes and links could operate from the shadows to thwart UNSCOM's progress. To combat this elusive adversary UNSCOM gradually turned its attention away from direct inspection of sites and facilities to an indirect study of the concealment organization.

American Scott Ritter headed the unit tasked with uncovering the secret Iraqi organization. The remainder of the unit consisted of a support staff in New York with field agents deployed in Baghdad. Ritter planned to use this unit to observe the Iraqi's observation to stimulus. Ritter developed a plan to execute what this thesis calls "cognitive nodal distortion" (quadrant III) because Ritter intended to create a difference between explicit reality and reality as it was

understood by his Iraqi handlers and the Apparatus of Special Security. The Iraqi nodes' perceived reality consisted of routine weapons inspections that they had successfully outmaneuvered for five years. However, Ritter's explicit reality would consist of an extensive surveillance array to detect the communications occurring in the hidden organization. The goal was to conduct a "series of large-scale inspections to elicit a detectable Iraqi response from the organization that was hiding Iraq's secret arsenal" (Ritter, p. 136). Ritter dubbed this tactic "Shaking the Tree" and planned to put into practice in UNSCOM inspection 143. This plan integrated the work of inspectors on the ground, surveillance aircraft overhead and a new element – sensitive communications scanners (Ritter).

"Shaking the Tree" in UNSCOM 143 did not turn up a smoking gun. However, the 143 did set a baseline of data demonstrating how Iraq responded and it helped to focus efforts on the Special Republican Guard. Soon thereafter, "Shaking the tree" demonstrated the real power of Stimulus Based discovery in June of 1996. That month UNSCOM 150 targeted a Special Republican Guard complex tipped off from UNSCOM 143. UNSCOM 150 was blocked from their inspection site and a standoff ensued. The Iraqis would not allow inspectors into the complex and the UNSCOM inspectors would not back down. Meanwhile, the sophisticated collection plan enabled UNSCOM to listen in on the radio communications of the Iraqi concealment organization as they sanitized the complex.

Unfortunately, Iraq was maneuvering politically with members of the United Nations Security Council and there was decreasing support for aggressive inspections. While the United States and Great Britain favored aggressive disarmament, the other three members of the permanent five – Russia, China and France – were less enthusiastic. Direct confrontation with Iraq could provoke a situation in which the Security Council could lose credibility. With three of the permanent members favoring diplomacy over confrontation it

was not productive to have UNSCOM provoking situations that created untenable political complications. Iraq used this division in the Security Council to compel Ekéus into a negotiation on the terms of inspection, titled Special Modalities. This agreement provided Iraq with concessions on prior notification and limited access to certain sites. The Clinton administration was displeased with Ekéus's concessions and political tensions continued to mount. Therefore, when Ekéus's term expired in the summer of 1997, Washington strongly supported the appointment of Richard Butler as the new Executive Chairman of UNSCOM.

Fortunately, Butler was a lifelong arms control proponent of arms control and his direct, often caustic nature ensured that UNSCOM would not be deterred by Iraqi intransigence. Butler went so far at to formally create the UNSCOM counter concealment unit in August of 1997 (Ritter, p. 136). However, political maneuvers by Iraq had dulled the impact of UNSCOM inspections and in November, Iraq declared that it would no longer cooperate with the inspectors. But, when the Security Council issued a clear warning the Iraqis withdraw their objection and on November 20th Iraq again claimed that it would allow unfettered UNSCOM access. Despite claims for renewed cooperation any pretext of mutual respect between the inspectors and their handlers was now gone. The UNSCOM relationship with Iraq was now openly adversarial.

After a false start in December of 1997, UNSCOM was back in Iraq in March of 1998. The targets of this inspection were several Special Republican Guard and Special Security Organization facilities. The Iraqis were superficially cooperative, but the concealment organization was dutifully working to prevent any weapons disclosure. However, this was another "Shake the Tree" operation in which Ritter and his team distorted perceived reality in the minds of the Iraqis. While the nodes in the Iraqi concealment organization believed this was just another inspection to find contraband, it was in fact a targeted stimulus to

illuminate the hidden nodes in Iraq's apparatus for special security. The communications intercepts confirmed that that the Special Security Organization was getting orders from Presidential Secretary Abid Hamid Mahmoud to remove and destroy documents prior to the arrival of inspectors. According to Scott Ritter, the lead inspector:

> This spectacular piece of real-time information confirmed two things; the involvement of the presidential secretary and the SSO in concealment activity, and that the communications monitoring program could develop information that would have a meaningful impact on the inspection (Ritter, p. 187).

Unfortunately, "Shaking the tree" created political problems due to the success of the technique. Iraq realized that its complete duplicity was being reconfirmed with each passing inspection and the Security Council found itself backed into a corner by the confirmation of Iraq's refusal to comply with UN Resolutions. This confrontation resulted in the August 1998 Iraqi proclamation that all cooperation with UNSCOM would cease. The United States and Great Britain responded with a four-day military strike, but no clear resolve to bring the Iraqi crisis to conclusion and "Shaking the tree" was over.

In this case study, "Stimulus Based Discovery" is successfully executed by creating distortions between the reality of weapons inspections perceived by nodes in the Iraqi Special Security Organization and explicit reality which was focused stimulus operations to reveal the hidden organizations topology. This distortion led the Iraqis to behave in a manner that was observable to UN forces and these observations led to nodes deep within Saddam Hussein's declared government. Thus revealing that Presidential Secretary Abid Hamid Mahmoud was a central hub responsible for Iraqi's weapons of mass destruction concealment.

D. D-DAY (QUADRANT IV)

On June 6th 1944 Allied Forces of World War II launched the largest invasion in the history of warfare. By day's end an armada of five thousand ships put more than two hundred thousand soldiers ashore on the northern coast of France. The invasion to retake Europe was underway. However, in every large human undertaking those in the vanguard experience isolation while lighting the path for others. The invasion of Nazi Europe was no exception. On D-day the task of going in first fell to America's 82nd and 101st airborne divisions whose paratroopers would jump into the night sky above France and secure the Allied right Flank near the town of Ste. Mere Elise.

Gusty winds, German anti-aircraft fire and poor navigation by Allied pilots resulted in the American paratroopers getting spread across 35 miles of the French countryside. In the dark night, the paratroopers' first task was to link up with their fellow soldiers. To accomplish this task each paratrooper carried

> …a few cents worth of tin fashioned in the shape of a child's snapper. One snap of the cricket had to be answered by a double snap. Two snaps required one in reply. On these signals men came out from hiding, from trees and ditches, around the sides of buildings, to greet one another. (Ryan, 1959)

In network parlance, the "click-click" of the tin snapper was a link between paratrooper nodes. The clicking sound linked isolated paratrooper to their units and allowed the dispersed and disoriented soldiers to come together.

If a vital "clicker" link were distorted then it might be possible to learn about undiscovered nodes in the paratrooper network. Unfortunately for many paratroopers the bolt-action on the German soldiers' guns made a nearly identical sound to the tin clicker. In the confusion surrounding the initial jumps many paratroopers fell prey to a German trap by walking toward what they thought were friendly "clicks." (Edwards and Morrison, 1994)

When a paratrooper incorrectly perceived the German gun breech noises as friendly soldiers they responded by double clicking their own crickets. Instantly the Wehrmacht soldier that just loaded his rifle understands reality with great clarity. From his perspective there is an armed man in the dark clicking some ridiculous toy. He knows it is not another German so he fires and the encounter is over with the young American lying dead probably having never fired a shot. The link distortion stimulus caused the paratrooper to reveal himself.

German soldiers exploited the link connecting paratroopers to one another by distorting the perceived reality of the rally signal. Thus, this short example shows a network stimulated to reveal its nodes by distorting the perceived reality associated with its linking mechanism.

This chapter examined four case studies that show Stimulus Based Discovery is a valuable strategy to learn about concealed networks. It works at the highest levels of policy severing states from terrorists. It works in tactical engagements when troops are stimulated to reveal their location. It works in the jungles of Columbia against criminal networks, and it works in international policy dealing with intransigent states like Iraq. In every network there is an opportunity to employ one of the four tactics: explicit nodal stimulus, explicit link stimulus, cognitive nodal distortion or cognitive link distortion.

There are dozens more examples of stimulus leading to accelerated discovery, but the case studies presented here were chosen specifically to highlight the broad applicability of this theory across different forms of coercive force and diplomacy in which a nation engages. The goal was to develop a theory with enough flexibility to provide a common approach for dealing with the vast uncertainty sure to be presented by Information Age threat.

The first two chapters argued for Stimulus Based Discovery as a tool to counter a broader threat spectrum with America's advantages in range and

accuracy. The nature of future conflict will demand military forces that can hunt down and find network adversaries on a global battlefield densely populated with non-combatants, and independent range and accuracy provide the firepower to deal with those threats once located. However, the task of discriminating threats from neutrals is quite challenging. In response to this problem, the authors look to network science that shows all organizations grown over time with preferential attachment form scale-free networks. These networks are both simultaneously fault-tolerant and susceptible to attack if hubs can be identified. Therefore, the authors demonstrate that Stimulus Based Discovery will reveal the location of networks hubs faster and more accurately than passive standoff observation. Furthermore, a passive approach is reminiscent of law enforcement tactics and fails to take advantages of time-tested principles of war available to military forces.

Redefining attack in this context means stimulating networks through one of four tactics to learn where hubs are located and then taking the offensive against those hubs. Taking the basic considerations of network adversaries, with special emphasis on terror networks, the authors next build a model of network development. This network model self-organizes into a scale-free system as predicted by Barabosi and is an ideal laboratory for putting the theory of Stimulus Based Discovery to the test.

IV. IMPLEMENTING A LABORATORY FOR RESEARCHING STIMULUS BASED DISCOVERY

A. INITIAL IMPLEMENTATION APPROACH

During the scoping of the problem of representing the story of terrorist agents planning, preparing, and executing terrorist missions, the authors examined the recent thesis dissertation work of Brian Osborn on the Story Engine. The Story Engine provides a framework for creating interactive stories that have multiple pathways and non-deterministic endings (Osborn 2002). The original thoughts with regards to targeting terrorist networks were to describe the desired end state as the ending scene in a story, determine what the possible scenes throughout the story were and what the starting scene was, and then create the ability to create a story line backwards from the desired end state to the starting scene. In creating this backwards story line, if a scene had multiple scenes that could follow that scene, the scene would be considered a hub in the story line graph. These hubs would become the focus point for concentrating on driving the story line to the desired ending or endings.

Several major issues prevented the authors from effectively using the Story Engine and drove them to a more basic approach. First, by using the Story Engine, the authors would have to determine all of the discreet story scenes for the entire story line, a daunting proposition at best, given that life itself is not defined by discreet, repeatable events, or scenes in one's own life's story. Second, the Story Engine was designed for user interaction around a single user character, when what the authors wanted to describe and model was a whole organization of main characters, with their own life cycles, or story lines. Lastly, after reading Barabasi's work on networks, it became clear that to model a complex adaptive organization such as a terrorist organization, then software designed for complex interactions would need to be used, which drove the authors towards a Multi-Agent System design.

B. MULTI-AGENT SYSTEMS

1. Introduction

A Multi-Agent System (MAS) are systems of multiple entities, known as agents, which interact with each other (Woolridge, 2002, p. xi). Agents are autonomous entities that act on its own behalf or on the behalf of its owner to accomplish its own goals and objectives. Agents exist in some environment, which they can sense, use that information to make some decision, and then take some actions within that environment. (Woolridge, 2002, p. 15). While an agent could be a simple control program, the type of agent used in MASs is an intelligent agent. Intelligent agents generally fall into one of three categories: reactive, proactive, and social. Reactive agents simple take actions in direct response to their perception of the environment. Proactive agents have some form of goal-orientation that drives their interaction with the environment. Lastly, social agents are able to interact with other agents and even humans to accomplish their goals and objectives. Multi-Agent Systems typically deal with this third type of agents, those that interact with each other (Woolridge, 2002, p. 23).

Experts describe terrorist organizations as complex, highly interconnected yet cellular networks of operatives. The high degree of interconnectivity among the members of the organization and the counter-intuitive macro-behaviors of the system as a whole that result from decisions at the individual level accurately characterize the complexity of these systems. As a parallel to complex adaptive organizations, software engineers have highlighted the now widely known truism that interaction between software components drives the definition of complex software. Multi-Agent Systems of social agents then become an effective approach to modeling these complex interactions between entities in the system (Woolridge, 2002, pp. 226-7]. Trying to understand a complex adaptive system, a top-down reductionism approach gives rise to uncertainty about how to design the expected macro-behaviors. As such, MASs are designed from the

bottom-up, relying on the micro-decisions of the agents drive the evolving macro-behavior of the system. Jacques Ferber created a design methodology for creating MASs (Ferber 1999). In his design methodology, a MAS is described by the components Environment, Objects, Agents, Relationships, Operations, and Laws. The notation shown in Figure 5 summarizes Ferber's design methodology.

$$MAS = \{E, O, A, R, Ops, Laws\}, \text{where}$$

E=Environment

O=Operations

A=Agents

R=Relationships

Ops=Operations

Figure 5. Multi-Agent System Design Framework.

The next sections describe how Ferber's methodology was applied to the design of the hypothetical terrorist network. Additional concepts of incorporating procedural knowledge, known as tickets and frames, as well as a means for agents to communicate with each other, known as connectors, are introduced.

2. Environment

In a MAS, the environment describes the physical or logical space that the agents live in. In choosing the scope of the environment, the designer must consider what the level of detail for the model is. The environment defines the boundaries of the system. In the Terrorist Network Simulation (TNS), the environment is the logical space of the terrorist agents and the connections and

communications with each other. No physical environment is modeled in this simulation.

3. Objects

The objects in the environment are the things that interact and can be interacted upon. To determine the objects, the designer uses a method found in object-oriented design. The designer performs a lexical parse of the problem statement to find the nouns in the problem statement. From that set of words the objects in the environment are determined. Those objects included in the design are those relevant to level of detail defined in the environment. In the TNS, the only objects in the system are the agents themselves, which are described below.

4. Agents

Agent in a MAS are the active objects. They are the objects that can sense the environment, make some decision based on that sensory input and a decision structure, and finally take some action within the environment. Each agent maintains some representation of the environment, also known as the external environment to the agent. The representation kept by the agent is known as the agent's internal environment. The internal environment provides a representation of the agent's state. Each agent has attributes that define the agent's behavior. In the TNS, each agent is a terrorist agent whose attributes are its personality, roles, goals, sensors, and mental map. Each of these attributes as well as the agents themselves is described in further detail below.

5. Relationships

In Ferber's MAS design methodology, relationships are the interactions that take place between and among objects and the environment. Agents interact with objects, the environment, and with each other. Objects can interact with each other and the environment as well. Each relationship describes the rules for forming relationships, the allowable actions within the relationship, and the rules for dissolving relationships. In the TNS, relationships play a key role for allowing agents to communicate with each other. The relationships are classified

into two general types of communications: requests and commands. Relationships are expounded upon further below.

6. Operations

MAS operations define the system-level processes and procedures that take place. The operations describe the objects and agents involved in the process and how the operations are encoded in the system design. The TNS models the process of terrorists progressing from individuals contacted by recruiters to join the organization, turning into recruits and operatives, and then planning, rehearsing, and executing terrorist missions. The majority of the operations in the TNS are captured in the relationships between the agents through an adaptation of the RELATE architecture created by Kim Roddy and Michael Dickson (Roddy and Dickson, 2000). These operations are operator recruiting, recruiter recruiting, trainer recruiting, recruit training, organizing a mission cell, cell operations, and resource bartering.

7. Laws

Laws describe the limits of the MAS. Laws might include the laws of physics such as gravity, or spatial and temporal constraints. Laws are inviolate rules that the agents must live by. Since the TNS has no physical environment, no physical laws are needed, but since the simulation model terrorist agent actions that take place over time, some limit is placed on how much an agent can accomplish in any given time period. The TNS is turn-based, so each agent can only act upon one goal in each turn.

8. Connectors

Connectors allow one type of interaction between agents. Connectors follow a biological metaphor of proteins interacting with a cell that was developed by John Hiles of the MOVES Institute at the Naval Postgraduate School (NPS) (Hiles et. al., 2002). His work has been implemented in Brian Osborn's Story Engine (Osborn, 2002, p. 55). Connectors are described by their type and their state of being extended or retracted. Connector types are

receptors and stimulators. When a receptor connector is in an extended state, it can connect with a stimulator that is also in an extended state. When the connectors connect, then several actions take place within each agent based on the type of connection made. Actions that take place include the exchange of information, the issuing of actions or orders for the other agent to carry out, or the transformation of one or both of the agents into another state or type. These actions are carried out in the form of procedural knowledge known as tickets.

9. Tickets

Tickets encapsulate the procedural knowledge that an agent has. This idea again was developed by John Hiles while at the MOVES Institute. The concept of tickets is explained in greater detail in Brian Osborn's dissertation work on the Story Engine (Osborn, 2002, pp. 68-71), so only a brief description of their functionality is included here. Tickets incorporate atomic actions an agent can take, typically in a sequential manner. Tickets are not limited to sequential actions; however, those used in the TNS are all sequential in nature. Tickets are designed to either complete each intended action, or to have those actions interrupted through interaction with other agents. The TNS incorporates tickets of both types. Each ticket consists of one or more frames, each of which is an atomic action the agent can perform.

10. Frames

A frame in a ticket encapsulates an atomic action, another component of John Hiles' framework for giving agents procedural knowledge (Hiles at. al., 2002). Frames consist of either of an action, a connector, or another ticket. Actions encapsulate reusable functions performed by the agents such that ticket composition is accomplished by selecting the associated actions into the desired order necessary to accomplish some procedure or process. Connectors are included in a frame so that their state can be changed and connections can be made with other agents. The TNS makes extensive use of tickets, frames, actions, and connectors and each are described in further detail below.

C. NETWORK CONCEPTS

The TNS incorporates the key characteristics of scale-free networks in its design.

1. Growth

Growth in the network is accomplished through a discreet event simulation that introduces new agents in an arrival process, which is discussed in detail below.

2. Preferential Attachment

To create preferential attachment in the network, the authors used the idea that agents when given a choice would connect to the agent that was most influential, those agents that had "high fitness" (Barabasi, 2002, p. 96].

3. Rich-Get-Richer

The TNS incorporates the rich-get-richer phenomenon by rewarding the agents for actions they take and goals they complete. The amount of reward is proportional to some characteristic of the agent's personality, so that the higher the characteristic, the higher the reward. This reward scheme creates a non-linear growth in the agent's overall worth in the system. In the TNS, those agents who are the most influential become the rich and therefore garner more resources and create missions that other terrorists desire to join. The simulation makes the assumption that agents do not become jaded or discouraged by their experiences, thus turning down missions, but instead they always prefer to join missions with a higher level of fitness. Modeling the effect of bad experiences by the agents is left for future work.

D. MODEL DESCRIPTION

The Terrorist Network Simulation brings together a wide array of concepts to produce a dynamic complex adaptive system that mimics a plausible terrorist organization. The simulation incorporates Barabasi's ideas on scale-free networks and weaves those ideas into the individual agents and their interactions with each other. The simulation is designed from the bottom-up, so

no global control is placed on how the network forms. The TNS borrows the concepts generated in the RELATE architecture and then modifies the way relationships are managed between agents for a networked environment. The authors borrow and extend on John Hiles' concepts of tickets, frames, and connectors in a network environment on Project IAGO (Intelligent Asymmetric Goal Organization) and these concepts are used extensively for creating the actions and interactions of the agents (Hiles and Lewis, 2002 and Hiles, 2003).

1. Adapting the RELATE Architecture

To create a network simulating individual terrorist agents, these agents needed to interact with each other heavily for the express purpose of accomplishing missions set forth by the leaders of the organization. Kim Roddy and Mike Dickson of the Naval Postgraduate School created the RELATE architecture in 2000 expressly for facilitating the development of applications that relied on relationships and interactions between autonomous agents. The RELATE (Relationships, Environment, Laws, Agents, Things, and Effectors) architecture provided a base set of Java classes to develop a relation-centric program. The architecture provided the majority of what was needed to create the model of a terrorist organization. Most of the interfaces were extended to add Java methods particular to the TNS, such as `TNSGoal` extending the RELATE interface `Goal`. Each of the goal objects in the TNS then implemented the `TNSGoal` interface, gaining methods from the superclass and the TNS subclass. These extensions of the RELATE architecture allowed for casting of RELATE objects to TNS objects to use the additional functionality in the TNS. A few exceptions are noteworthy in the extension and implementation of the RELATE architecture. Several of the instance variables of the `Agent` class were initially declared `private`, and in the TNS implementation they were changed to `protected` to allow for easier access to those variables by the `TerroristAgent` class that extended `Agent`. The other noteworthy exception

was the nearly complete re-write of the other concrete class in the RELATE architecture, the `RelationshipManager`.

In the RELATE architecture, agents could only exist in one instance of any given relationship type. For instance, in Roddy and Dickson's thesis, they created a replication of Andy Ilachinsky's ISAAC (Irreducible Semi-Autonomous Adaptive Combat) framework (Ilachinsky 1997), called JACOB that simulates land combat. In this scenario, an agent can belong to a squad, company, and army, and only one of each of these organizational groupings. This paradigm worked fine for JACOB and other simulations that used the relationships to categorize levels of organizational affiliation. In the TNS, relationships precipitated the formation of the Observer, or Publish-Subscribe pattern, which relied on the listener model paradigm to register and de-register listeners of connectors. In the listener model, the only entities that should hear an announcement from another entity are that entity's listeners. So in the development of the TNS, the authors came across the scenario where the management of the listener model and the current implementation of the `RelationshipManager` were at odds with each other. In the RELATE architecture, determination if the conditions had been met for a relationship to form was delegated to the individual `Relationship` objects. In determining if a given `Agent` could form a relationship, the individual `Relationship` objects looked at which agents that particular `Agent` object in question knew about through its sensors and then examined if the conditions were met for creating a *single* relationship object for all qualifying agents to be added to.

A similar mechanism was used when adding an `Agent` to an existing `Relationship` object. The problem for the TNS arose when the individual `Relationship` objects needed to determine those agents that *should* belong to the relationship and therefore become a registered listener or broadcaster. The solution was to only allow relationships between agents that were maximally

connected to each other in the network. If agents were directly linked to each other in the network, then they knew about each other, and since they knew about each other, they had to potential to hear one another's connectors.

As a result, the `ConditionsMet` method of the `Relationship` interface was abandoned and the `RelationshipManager` was modified to check for maximally connected relationships between agents. Each turn of the simulation each agent would check if any new relationships should be created with the other agents it knew. If any two agents should belong in a relationship, then the agent whose turn it was would check to see if it had a `Relationship` object of that type. If it did, then it checked to see if the `Agent` in question was in one of those relationships, and if not, to check if that `Agent` *would* be maximally connected to a relationship *if* it was added. If it would be maximally connected to the agents in the relationship, then the agent was added. If it could be maximally connected to any of the relationships, then a new one was formed and the two `Agent`s were added to the relationship. If the agent checking relationships did not have a `Relationship` object of the particular type, then it checked with the `Agent` in question to see if it had one. If it did, then the `Agent` checking relationship tried to see if it would be maximally connected with the other `Agent`'s relationships and added itself if it was. If neither `Agent` had a `Relationship` object of the particular type in question, then a new was dynamically created using Java's capabilities of reflection and the two agents were added to the relationship.

A similar issue arose when the authors needed to remove agents from relationships. The structure proposed in the `Relationship` objects as evidenced by the work on JACOB did not satisfactorily destroy the right agents from the right `Relationship` objects, so the authors returned to the principle of maximal connectedness with the added idea of keeping track of which types of agents could belong to which relationship types. Each turn an agent would

determine if the relationships it was in were "appropriate," in other words, did the relationship have at least one other agent in it that was an allowable type, and were all the agents in the relationship of the allowable types. If neither query proved true, then that agent removed itself from the relationship and the last agent to delete itself from a relationship destroyed the `Relationship` object and updated the master list of `Relationships` being maintained by the `RelationshipManager`.

The last modification to the core RELATE architecture was to allow agents to keep a list of the individual `Relationship` objects for each relationship type. In the original RELATE architecture, each agent could only have one `Relationship` object of any given type, so this functionality needed to be added to the `RelationshipManager` and all associated classes that accessed an agent's collection of `Relationship` objects. With the modified RELATE architecture at the core of the TNS operation, the individual agents could successfully interact with each other to accomplish their objectives.

2. Terrorist Agents

Terrorist agents are the key components of the TNS. Each agent represents an individual that takes on different roles in the organization and has particular goals related to those roles. Some of the roles carry with them particular needs and capabilities, but the majority of the functionality remained the same across roles. Each agent can take on more than one role and the authors' implementation reflects this fact for the most part, but this initial implementation did not attempt to allow agents this ability for the simplicity of code creation. Instances where future work is needed to finish this development are noted below. Each agent has its own personality to set it apart from other agents and to affect its interactions with other agents in the simulation. The last key component to the terrorist agents is the agent's mental map. Figure 6 below shows the relationship between the software objects related to the terrorist agents.

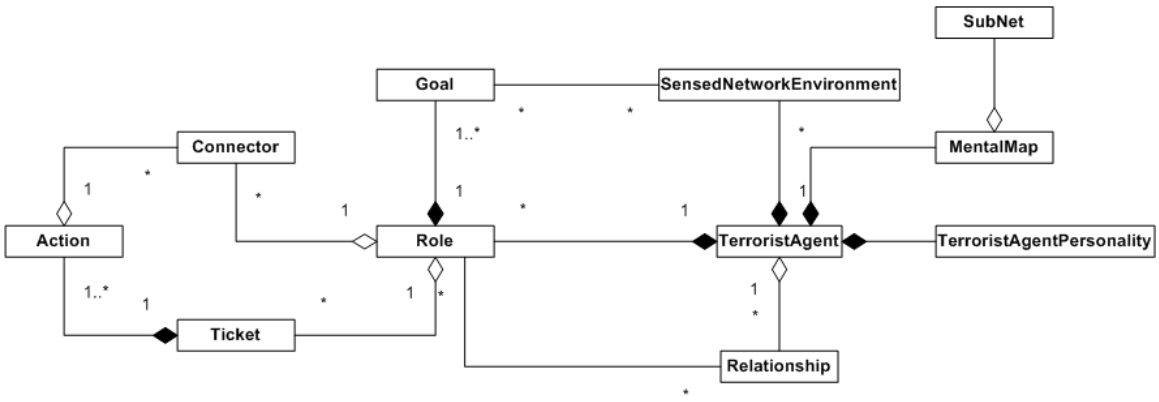


Figure 6. Terrorist Agent Software Components.

a. Roles

Roles represent an array of character types, such as individuals looking for a cause to join, influential individuals in the community seeking out those types, specialists in the various tools of the terrorist trade, experienced operators with the nuts-and-bolts knowledge of running operations waiting to pass on their knowledge and wisdom, to experienced and influential masterminds dreaming up a wide range of devious plots to inflict upon the civilized world. Each role carries with it a set of goals specific to that role and these will be expounded upon below.

b. Goals

A goal is an objective the agent seeks to accomplish. For some of the roles, these goals are checked off as they are completed so that the agent may change role types or to track the agent's status on the progression toward a larger goal such as carrying out a mission. Each agent has a variable goal apparatus that allows that agent to act upon the most important goal at any turn in the simulation. Each goal is associated with a particular behavior the designer desires the agent to exhibit. Each goal has a means to score it against its other goals and therefore select the highest weighted goal, hence the term "variable" used in describing the goal apparatus. Lastly each goal has an associated set of actions the agent can take to accomplish the goal. In the TNS, each goal uses a Ticket with associated Actions to accomplish the goals.

c. Personality

With the agent's role or roles, the personality gives each agent a distinct character. In the RELATE architecture, each personality is unique to the specific application, and in the TNS, each agent has personality traits of allegiance, experience, and influence.

(1) Allegiance. An agent's allegiance value models the agent's dedication to the organization. Agents with higher allegiance are more likely to perform certain actions out of their devotion to the organization. For young contacts and recruits, the agent's allegiance determines how much time a recruiter has to spend with that agent testing the agent's mettle for joining the organization.

(2) Experience. The agent's Experience value models how skilled the agent is in conducting terrorist-related activities. For specialists, such as arms dealers, financiers, and logisticians, the experience value determines the departure point for how much of a resource the agent can produce in a given turn. For leaders, the experience value helps determine how attractive of a mission the leader can devise and what the resources will be needed for the operation. Experienced agents can create more elaborate, more seductive missions due to their experience and influence, and therefore draw more agents to join on the lucrative missions.

(3) Influence. The agent's influence value is the ultimate determination of where the agent falls in the organization's pecking order. Influence combines with experience for leaders creating missions. Influence is also used to determine whether or not an agent is willing to communication with another agent or is willing to pass on a message coming from another agent. Influence and experience also combine together in the specialists to create the notion of status with respect to answer a leader's request for the specialist to provide a resource. For instance, if the leader's mission is below the stature of the specialist, then the specialist will ignore the leader's request.

d. Sensors

Each role also includes zero or more sensors that can detect other agents of a given type of role as explained below. The sensors are simple cookie-cutter type sensors that use the locations of the agents in the logical space to determine if detection takes place.

e. Mental Map

The mental map is the agent's mental space of how it perceives the network environment based on whom that agent knows directly and indirectly knows about (Fauconnier, 2002, 102). A mental map is the agent's own worldview. The agent evaluates its goals and acts upon them largely based on the agent's mental map. An agent's mental map likely differs from the explicit map of the network, or the ground truth of who knows whom in the organization.

f. Sub-Network

To complement the mental map, a helper class known as the `SubNet`, or sub-network, kept track of the edges or links within the individual agent's mental map of the network. Where the mental map tracks exactly who the agent knows and knows about indirectly, the mental map delegates the task of tracking which agents know which other agents in the mental map. The sub-network accomplishes this task using another helper class called an `AgentPair`. A pair is simply a class the captures the fact that two agents are linked to each other and therefore know each other. The sub-work only contains unique pairs, so both agent pairs {A, B} and {B, A} would not exist in the sub-network, but instead just one would. Agent pairs also have one other characteristic, a history value.

The purpose of the history value is to place a value on the relationship a pair of agents have had. Any time two agents interact with each other, the history value between the two agents is incremented, attempting to provide some notion that strong relationships develop over time through

interaction between two people. Each turn, the history values on all of the agent pairs in the simulation are decremented by one. When the history value of a given pair falls below zero (the initial value is some non-zero value), then the relationship has drifted apart and the link between the two agents is broken, both explicitly within the network, but also with both agents' mental maps. This feature models the fact that people eventually drift apart if they do not interact or communicate with each other. While the rate at which people drift apart is based on individual differences, this model provides a generic approach that approximates the desired behavior. In the TNS, operators who have been conducting mission with leaders and not interacting with the recruiter who initially convinced them to join the organization, the relational link between the operator and the recruiter eventually breaks. With this effect in the network model, the emerging networks more appropriately resemble plausible scale-free terrorist networks. The sub-network also becomes a useful tool for graphically rendering a representation of the network.

g. Life-Cycle

Most agents start out their life in the simulation as a contact, the disgruntled youth mentioned above. Along comes a recruiter, such as a mullah running a madrassa in the Arab world or a bar tender in Ireland looking for IRA recruits. The recruiter attempts to entice the contact to join the organization and if the contact does, he become a recruit. A recruit's objective in life is to become a full-fledged operator and carry out terrorist missions. Before a recruit can reach that state in life, the recruiter needs to check out the recruit for his trustworthiness to join the organization. The recruiter will take a small number of recruits out and perform a small mission, such as maybe knocking over a convenience store to determine if the recruits have what it takes to earn a place within the organization. Once the recruits are deemed worthy, the recruiter sets them up with a trainer to get them up to the minimum level of proficiency necessary to carry out missions.

Once the recruit has been trained, he becomes an operator. From this point, his world opens up as to his possibilities for make a name for himself in the organization. The first goal for an operator is to get in touch with a leader who needs muscle for pulling jobs. The operator can find leaders either through the trainer who just trained him acting as a proxy, or by putting his feelers out through the organization, by basically asking around. Once an operator has found a leader to join, he becomes part of the leader's terrorist cell. Operators rehearse and execute missions gaining experience and/or influence after each mission. Operators generally have good working knowledge and therefore can advance into trainers to pass their wisdom down should the conditions exist for the operator to do so.

Leaders can promote operators though when the situation arises that the leader needs a particular resource such as money and the leader doesn't know a financier to provide him this critical component. The leader orders an operator to become a financier, a small-time one at best, but the newly appointed financier starts gathering resources for the leader. Specialists, such as the arms dealer, financier, and logistician, have usually gained some status in the organization, and may decide to become their own leader should they get bored or ignored by the other leaders in the system. Additionally, if a specialist becomes disavowed from the organization due to lack of contact with other agents, then the specialist will advance himself to a leader to create his own splinter cell. Agents do not promote or advance into recruiters, as they are influential types with local knowledge recruited by leaders to feed the organization new blood. As such, recruiters are introduced into the system on their own. For a contact to climb up the organizational ladder to hopefully become a leader, missions and targets must exist so that operations can be carried out.

3. Targets and Missions

Targets and missions form the core objective for the organization as a whole, even though leaders own the targets and missions and shepherd them through to completion. Targets specify the requirements for mission accomplishment, such as how many resources are needed and how long the operatives will need to rehearse and execute the mission to bring it to completion. Missions keep track of the current status of accomplishing an attack on a target, therefore missions hold the status of the different levels of resources, how many and which operators have joined the mission, and how many turns the cell has rehearsed or executed the mission. Each target has characteristics of impact, stability, and draw.

a. Target Impact

The target impact models the relative worth of the target. The bombing of the World Trade Center buildings was a target of high impact, an event that shook the world. The shooting of several American soldiers outside Camp Doha in Kuwait was a low impact target, noteworthy, but in the large scheme of effecting a nation, a small event.

b. Target Stability

Target stability models the window of opportunity when the target is vulnerable to attack. The World Trade Center buildings were rock-solid stable targets; they were not moving. However, the gassing of thousands of spectators at the Super Bowl would constitute a low stability target, where the window of opportunity consisted of a matter of hours.

c. Target Draw

Target draw represents the overall relative value of a mission compared to other missions. Targets with higher draw create missions that are more desirable to participate in them because of the potential for fame, glory, and perceived reward in the afterlife. Target draw consisted of the product of impact and the base 2 logarithm of stability, as shown in Figure 7.

$$\boxed{Draw = Impact \bullet \log_2 Stability}$$

Figure 7. Target Draw.

The logarithm in the draw equation puts emphasis on the impact value so that given two targets, one with high impact and low stability and another with low impact and high stability, those two targets are not on the same scale, but instead the target with the high impact and low stability has a higher draw.

d. Mission Requirements

The draw of the mission seeds a random number generator for deriving the mission requirements in terms of operators, resources, and time. The seed for the operator requirement is the base 2 logarithm of the draw, which is plugged into a triangle probability distribution as the mean and the maximum. Figure 8 shows a triangle distribution's probability distribution function. The distribution is defined by a minimum, a, a maximum b, and a mean, c. The TNS typically used right triangles for the distributions as seen on the right side of Figure 8. For code development, the authors found it easier to use right triangles versus keeping track of some global maximum, b, as seen on the left, that always exceeded any given mean.

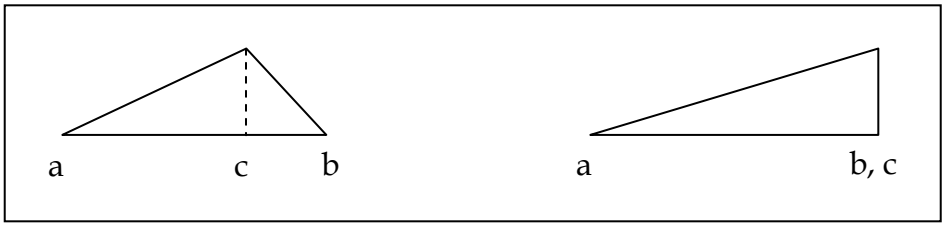


Figure 8. Triangle Distribution.

For the remainder of the resources, the mean and maximum were determined by the square root of the target's draw. These seeds produced

reasonable levels of required resources relative to other missions of higher and lower draw.

4. Roles

An Agent can take on one or more roles throughout its life cycle as mentioned above. These roles represent positions within the organization the agent takes on to further their own personal goals and those of the organization. Each role brings with it a set of associated goals that help define the behaviors the agents exhibit as described above in the variable goal apparatus. Figure 9 below shows the relationship between the roles, relationships, goals, and connectors in the TNS model. The arrows pointing to and from the connectors show the relationship between the stimulators and receptors. Stimulators have arrows pointing into the connector; receptors have arrows pointing from the connectors.

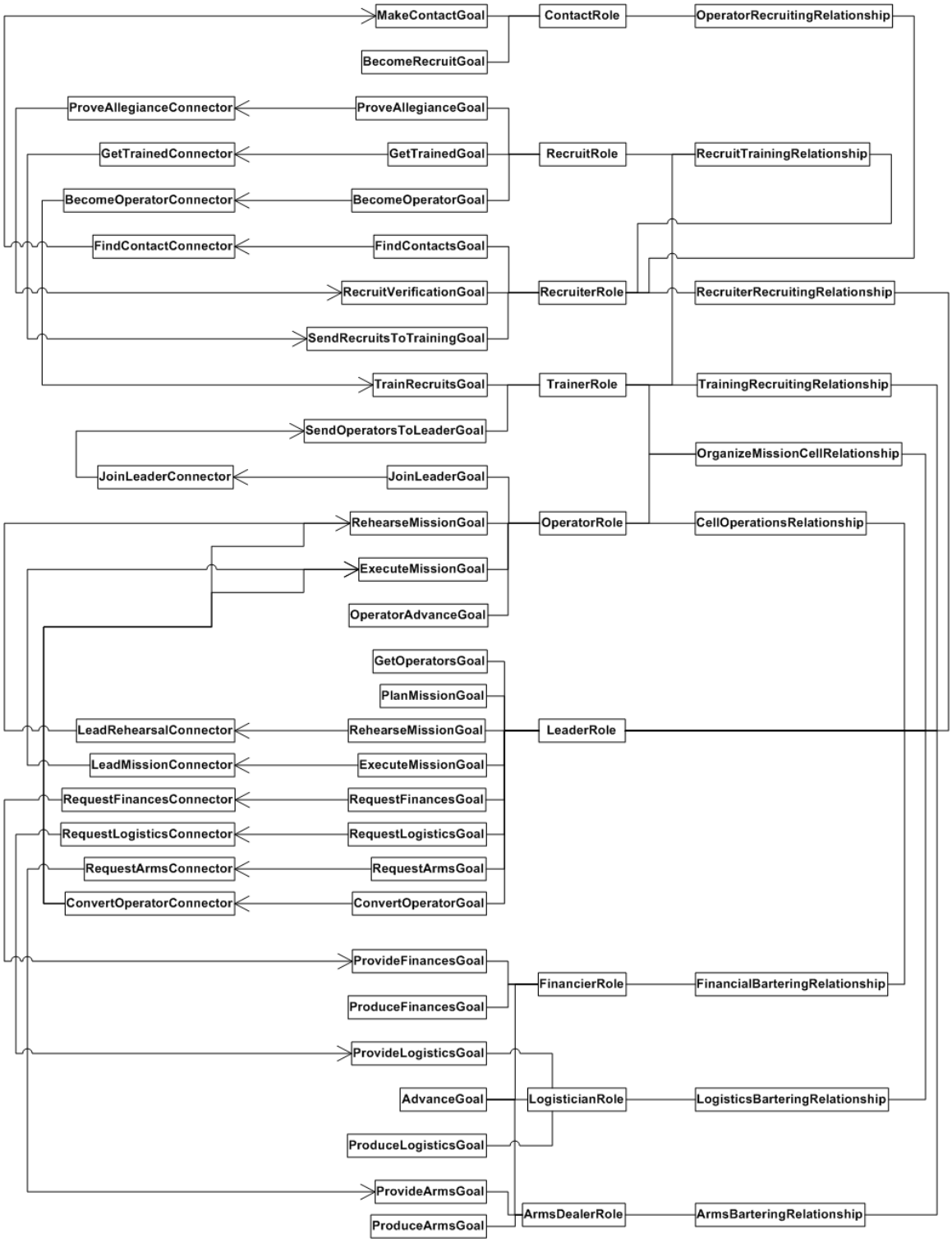


Figure 9. TNS Model.

a. Contact

The contact role represents those individual who are sought out by recruiters looking for potential supporters of the organizations cause. Contacts exist in the scenario for a particular period of time in which they may be contacted by a recruiter. At the time of contact, the contact decides whether or not to join the organization. If the contact does decide to join the organization, he will turn into a recruit.

b. Recruit

A recruit represents a greenhorn in the organization. Recruits join the organization with a given level of allegiance and if that level is not high enough for the recruiter, then the recruiter will take that recruit out on a mini-mission to let him prove his worth, possibly with other recruits. Once a recruit has been "proven," then the recruiter sends him off to a trainer to be turned into an operator.

c. Operator

Operators are the workhorses of the organization, providing the muscle and manpower to accomplish a leader's mission. Operators have the potential to advance up in the organization, either through a type of self-promotion or through a leader-directed promotion.

d. Recruiter

Recruiters represent locally influential and well-connected individuals who know where to look to find potentially lucrative contacts that might want to join the organization. Recruiters aren't typically experienced, as they don't participate in the day-to-day operations of the organization, but focus instead on pumping in new blood to the organization. Leaders seek recruiters out so that those leaders can meet their requirements for operators in a mission. Recruiters work with trainers to turn recruits into those operators.

e. Trainer

Trainers model those individuals in the organization who are good at what they do as far as the ins and outs of mission operations. As such, these trainers are ideal for passing that knowledge down to young recruits. Trainers are like career Non-Commissioned Officers (NCOs) in militaries today, people who've "been around the block" and are looking to share that wisdom with raw recruits. Trainers also sit at the top of one track of advancement for individuals in the organization. Those individuals who either do not become promoted by a leader to a specialist role and continue to gain experience and influence through carrying out missions, or become disavowed by the organization, convert into trainers and do not advance to any other role beyond the trainer.

f. Financier

The first of three specialist roles, the financier provides the ever-essential component for any operation, money. In the specialist roles, the agent's experience drives their ability to produce their particular resource and their influence controls how much resource; therefore specialists represent a range of individuals in this class. Financiers with a low experience and influence model individuals only capable of knocking over some convenience stores or conducting credit card fraud to grab a relatively small amount of money. Experienced and influential financiers on the hand are like bankers who know how to move large amounts of money discreetly, or oil sheiks who want to support the organization while at the same time appearing impartial, or individuals with "old money" that donate to the cause.

g. Logistician

The second of the specialist roles, the logistician provides the organization the ways and means necessary to carry out mission. Logisticians provide among other things, transportation such as vehicles and planes, obtain passports and the like, coordinate safe-houses, and setup communications such as obtaining encrypted satellite phones. Inexperienced logisticians probably

make fake passports out of their own house, hotwire cars for transportation, and buy cell phones from a local retailer, while their more experience brethren know whom to call to forge a visa, how to obtain stolen cars with fake license plates, and how to sanitize and fence stolen goods for the organization, while the really influential types have access to large-scale commercial and military transportation to include ocean-going vessels and might even own a transportation company or an import/export company, or maybe even work in a consulate or passport office (or at least know someone who does and is willing to help out).

h. Arms Dealer

The last of the specialists, arms dealers, provide the instruments of terror that mark the unconventional and often shocking methods these organizations employ. Bit player arms dealers might rob a gun store or make a fertilizer bomb from something they read off the Internet while real players in the arms market know how to obtain untraceable small arms, quality explosives, and possibly weapons of mass effects, such as "dirty" bombs or even quite possibly nuclear weapons, biological pathogens such as anthrax or small pox, or chemical toxins such as Sarin gas.

i. Leader

The leader role models the masterminds of some of the most despicable acts inflicted upon humankind. Leaders devise targets and lead the rehearsal and execution of missions. Leaders handle the gathering of resources from specialists to meet the target requirements and work with trainers and recruiters for their manpower requirements. The TNS allows leaders to grow from small-time thugs to the kingpins of large criminal and terrorist organizations. As each leader successfully completes a mission, he becomes more experienced and more influential, raising his stature in the organization over time, and therefore becoming capable of pulling off acts of terrorism that

reach the front pages of newspapers worldwide. For these leaders to accomplish all of these goals, they need to establish relationships.

5. Relationships

Relationships define the various associations the agents have with each other and frame the reasons for why they communicate with each other. Relationships allow for agents to accomplish goals that would not otherwise be accomplishable without the existence of relationships (Roddy, 2002, p. 38). Each role gives each agent a local set of skills they can bring to the organization, but one individual cannot do it all, so they have to collaborate with each other.

a. Managing Relationships

Each agent manages his own relationships through the `RelationshipManager` as mentioned above. Each turn the agent checks to determine which relationships it should belong in, create, or get out of. The functionality for determining if the conditions are met for forming a relationship in the TNS have been exported to the `RelationshipManager` vice in the individual `Relationship` objects since the requirements were the same for each `Relationship` object, that of maximum connectedness. This maximum connectedness facilitates the registering and de-registering of listeners for connectors. The rest of this section expounds upon each of the relationship types in the TNS.

b. Operator Recruiting

Contacts and recruiters participate in the operator recruiting relationship for the sole purpose of allowing recruiters the ability to entice those individuals in the population most likely to support the organization's cause.

c. Recruit Training

Once contacts join the organization and become recruits, they enter into a recruit training relationship with the recruiter who just recruited them. When the recruiter introduces the recruits to a trainer, they can also enter into a

relationship with the trainer as well so that they can receive training and become full-fledged operators.

d. Organizing a Mission Cell

Mission cell organization is handled by a three-way relationship between trainers, operators, and leaders. Once a recruit has become skilled enough according to a trainer, then he becomes and operator and looks to join a leader on a mission. Operators can either come in contact with a leader by being introduced to a leader via a trainer who knows one, or by asking around the organization for leaders who need operators and receiving a response from one of those leaders.

e. Cell Operations

Once an operator is in a cell, he participates in a cell operations relationship with that leader. This relationship facilitates the leader's ability to rehearse and execute his mission with the members of his cell. It also allows leaders to spot promote operators to specialists when the need arises.

f. Financial Bartering

The leader participates in five other binary relationships with members in the organization in order to accumulate the necessary resources and manpower for carrying out missions. The first of these relationships is the financial bartering relationship with financiers. This relationship allows the leader to request and receive money and other financial aid from the financier.

g. Logistics Bartering

The leader and logistician roles participate in the logistics bartering relationships for the sole purpose of exchanging logistical resources at the leader's request.

h. Arms Bartering

Leaders and arms dealers share the arms bartering relationship so that the leader can gather the necessary instruments of terror for the mission at hand.

i. Recruiter Recruiting

Leaders and recruiters share a relationship when leaders sense other recruiters in the environment that are not directly linked to the leader. This relationship models the fact that leaders seek out locally knowledgeable, influential, and willing individuals who can assist the leader in adding numbers to the organization's roster. Without operators in the organization, the organization cannot grow, so recruiters perform half of the critical role of feeding these individuals to the leaders.

j. Trainer Recruiting

Leaders and trainers join into a similar relationship as that between leaders and recruiters to fill the other half of the critical role of keeping the organization manned. This relationship allows leaders to seek out those individuals who can provide them with skilled people he needs to pull off missions.

6. Goals

All actions by agents are motivated towards goal. As mentioned above, each role carries with it certain goals that are also related to the relationships that that role type can join into. These goals also allow the agents to fulfill their part of a contract between the other members of the relationship for completing organizational goals.

a. Contact Goals

(1) Make Contact. Any contact that appears in the simulation starts off with this goal as the primary goal until they have been successfully contacted and recruited. This goal encodes the behavior of a contact being open for communication from a recruiter. Whether or not the contact actually joins the organization is another story; this goal simply facilitates that process. This goal also creates the behavior that the contact only gets one chance to join the organization. If the contact chooses not to join, then he will disappear from the simulation.

(2) Become a Recruit. This goal models the contact's official passage from being just a contact to actually getting his foot in the door as a recruit.

b. Recruit Goals

(1) Prove Allegiance. The recruit training relationship defines a threshold that a recruit's allegiance value must exceed before they can proceed onto training. This goal represents the recruit's desire to become initiated into the organization, to prove their worth so they can move on to being an operator.

(2) Get Trained. Once a recruit has been initiated or is trustworthy enough not to need initiation, the recruit needs to meet a trainer so that he can gain some base-level experience before joining a cell and participating in missions. This goal creates the behavior of a recruiter introducing the recruit to a trainer for that purpose.

(3) Become an Operator. This goal creates the behavior of the recruiter training with the trainer to become an operator. When the trainer has deemed the recruit has had enough training, the recruit becomes an operator.

c. Operator Goals

(1) Join a Leader on a Mission. The first priority of an operator is to get into a cell. This goal creates the behavior of an operator looking for that opportunity. The operator can either go through the trainer or ask around the organization to accomplish this goal.

(2) Rehearse a Mission. Once an operator has received a target as part of joining a leader in a cell on a mission and the leader has decided the mission needs to be rehearsed, this goal allows the operator to exhibit the behavior of the agent secluding himself with the rest of his cell to practice the upcoming mission.

(3) Execute a Mission. Once the leader has decided that mission is ready to be executed, this goal gives the operator the behavior of

participating in the mission for a period of time as specified by the leader's requirements.

(4) Advance to a Trainer. If the agent becomes bored or disavowed because he has not participated in a mission for a given length of time, this goal gives him the behavior to possibly advance to the trainer role.

d. Recruiter Goals

(1) Find Contacts. One of the primary behaviors a recruit exhibits is that of find new contacts for the organization. This goal gives the recruiter that ability by having him attempt to contact and woo any contacts he can find.

(2) Verify Recruits' Allegiance. Another function the recruiter performs is initiating new recruits, testing them to see if they are willing and ready to commit to the organization. This goal provides recruiters with the behavior to increase the allegiance of new recruits before he sends them off to become trained.

(3) Send Recruits to Training. The last duty a recruiter performs is to put recruits in contact with a trainer so that they may go off to a training camp and train up to become operators. This goal gives the recruiter the behavior of either introducing recruits to a known trainer, or putting out his feelers throughout the organization to find a trainer willing to take the new recruits. When sending the recruits to a known trainer, the recruiter exhibits the behavior of passing the recruits to the most influential trainer the recruiter knows at the time, helping to induce the rich-get-richer phenomenon in the system.

e. Trainer Goals

(1) Train Recruits. This behavior interacts with the recruit behavior of becoming an operator to produce operators for the organization. This goal allows the trainer to continue training a recruit until that recruit's experience has exceeded the threshold needed to become an operator.

(2) Send Operators to Leaders. This goal interacts with the operator goal of joining a leader on a mission to introduce willing operators to leaders through the organize mission cell relationship. The behavior of this goal allows the trainer to introduce the operator directly if he knows a leader, but if he does not, he can query those he knows in the organization to find one for him.

f. Specialist Goals

The three specialists, arms dealer, financier, and logistician all have the exact same goals since they are all resource providers. The only difference between the three roles is the type of resource they provide.

(1) Provide a Resource. This goal encodes the behavior that the specialist has a cache of resources either at hand or on call that he has standing by for a leader to request. Another behavior created by this goal is that a specialist has a minimum amount below which he will not provide the resource and instead return to restocking that resource. In evaluating this goal, the specialist examines if a leader requested resources during the last turn via messaging (described below). If so, then an additional weight is given to this goal, described below as well.

(2) Produce a Resource. With this goal, the specialist exhibits the behavior that he will produce resources until he exceeds his capacity to acquire the resource. The agent's influence value determines how much of a resource an agent can stockpile. The idea with this design decision was that more influential specialists would have access to greater levels of resources as described above. In evaluating this goal, the specialist checks if providing a resource was the active goal the turn before and if the agent did not provide a resource, then an additional weight is given to this goal so that the specialist has a chance to go back to producing resources and not become stuck on providing resources.

(3) Advance to a Leader. Specialists also have a behavior that allows them to advance to a leader under certain conditions. The first condition occurs if a specialist has become bored through continually providing a resource without anyone requesting that resource, he will go off and promote himself to a leader and start his own cell. The other condition of this behavior occurs if the specialist becomes disavowed from the organization by losing his connections to the main network system, in which the specialist advances himself to a leader and starts a splinter cell.

g. Leader Goals

(1) Plan a Mission. The primary behavior a leader exhibits is that he creates targets and organizes missions. This goal allows the behavior that a leader can seclude himself away to plan the mission for short period of time, during which the leader does not perform any other tasks, nor is he as likely to interact with the rest of the organization during that period.

(2) Get Operators for a Mission. This goal gives leaders the behavior of seeking out the source of operators for missions: recruiters and trainers. If the leader detects any recruiters or trainers he will try to contact them, much the same way recruiters introduce themselves to contacts. If the leader does not know either one of these types of agents, then he will post a request to those he knows to find these agents so that he can get the agents he needs.

(3) Request Resources. Next to acquiring manpower, the other key behavior a leader needs to accomplish missions is to acquire the financial, logistical, and arms resources necessary to carry out the mission. This goal allows the leader to exhibit one of two behaviors in accomplish this part of putting together a mission. If the leader knows a specialist directly, then he attempts to contact the specialist and request the resource from him. However, the specialist may not be available, but instead off creating more resources, so then the leader uses his other behavior to put out a request to the organization

requesting the resource. While these requests are out, the leader's impatience begins to grow, at which time the leader reveals his behavior to convert operators in his mission to the needed specialist role.

(4) Convert an Operator to a Specialist. This goal allows the leader to turn to the most influential operator in his mission and promote him to a specialist role. The operator ceases to exist in that role, removing himself from the mission as an operator and takes on the responsibilities of creating the resources for the job he was promoted to. When the operator leaves the mission, the leader will need to find a replacement for him, so the get operators for a mission behavior eventually re-emerges so that the leader can fill that vacancy.

(5) Lead Mission Rehearsal. The lead mission rehearsal goal gives the leader the behavior that once the preponderance of the resources for the mission have been obtained, all the necessary people have been recruited, and the leader knows a trainer who can setup the necessary training facilities for him, the leader can take his cell and run them through the mission for the required period of time. Once the rehearsal finishes, the leader can return to gathering any remaining resources before launching off into the mission.

(6) Lead Mission Execution. This last behavior available to the leader lets him and/or his operators conduct the mission. Once the mission finishes, each of the members of the mission gain possibly gain experience and influence, with the leader receiving a majority of the experience and influence, furthering the rich-get-richer phenomenon. This goal also provides the members of the mission the behavior of resetting their goals, thus allowing them to participate in the next available mission and the leader can plan a new mission.

7. Communication Model

The TNS uses two methods of communication between the agents so that they may collaborate with each other and accomplish group as well as personal

goals. As mentioned above this thesis incorporates John Hiles' biological metaphor and concept of connectors to bring agents together, allowing them to take actions particular to the connection. The thesis also uses the notion of a broadcast e-mail-like system for sending requests throughout the network.

a. Connectors

Connectors are used as a communication mechanism between agents that know each other, or between other agents one particular agent detects, such as between recruiters and contacts. Connectors are implemented in the TNS using the listener model in Java. The individual `Relationship` objects handle the responsibility for setting up and tearing down the listener mechanics. The stimulator connectors are handled through physical instantiations of `Connector` objects that change a state variable to indicate whether they are extended or retracted. For the receptor connectors, their extended or retracted state is created using an if-then selection structure that only takes action if the type of connector that was extended is of a particular type, so like the biological metaphor, only the right proteins can attach to right receptors on the cellular surface (Hiles et. al., 2002 and Osborn, 2002, p. 55).

b. Messaging Model

The messaging model in the TNS allows agents to communicate with agents they are not directly linked to in the network, which is critical given that the connector communication paradigm only works within the confines of directly linked agents and in the use of the sensory model. In the messaging model, messages are placed in an outbox, evaluated to whether or not they should be sent to a particular person, delivered, placed in other agents' inboxes, and then when an agent checks his inbox, he evaluates whether or not those messages should be answered. Each message includes the originator (so that the person who answers it knows who sent it), the intended target, stated in terms of the role that should answer the message, the type of ticket to execute when the

message is answered, and an identifier for the type of message as shown in Figure 10.

Message = {Originator, Target Role, Ticket Type, Type Identifier}

Figure 10. Components of a Message.

This communication does include three important optimizations that prevent the complete explosion in the number of messages being passed through the network, while leaving one optimization for future work. The first optimization prevents agents from forwarding a message back to the sender. So, if agent A sends a message to agent B, agent B will not re-send the message back to agent A, or "ping-pong" as shown in Figure 11.

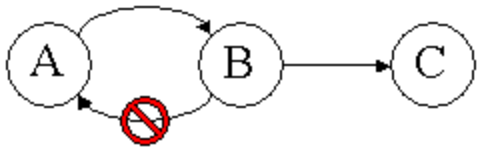


Figure 11. Preventing "Ping-Pong" Messages.

The second optimization kills loops in the messaging system. If agent A sends to agent B who sends to agent C and agent C knows agent A, agent C won't send the message to agent A because it would create a loop in the messaging process as shown in Figure 12.

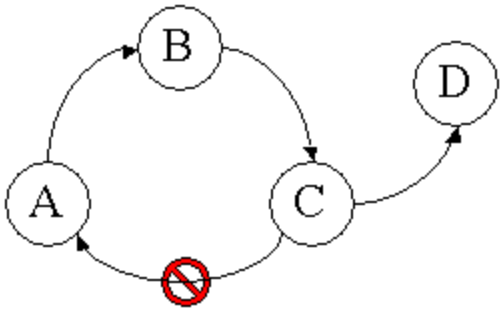


Figure 12. Preventing Message Loops.

To accomplish these optimizations, messages keep track of the forward chain for the message with a collection of agent pairs that identify the sender and the receiver. So when agent A sends to agent B who sends to agent C, the message chain becomes an ordered set of pairs, looking like {{A, B}, {B, C}} as shown in Figure 13.

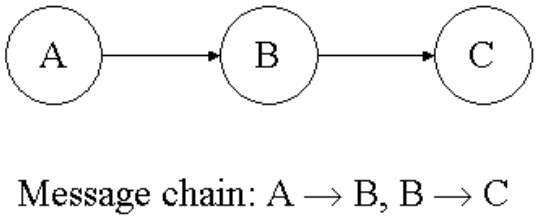


Figure 13. Message Chain Between a Set of Agents.

The third optimization prevented multiple messages from being sent for the same type of request, just from different agents. If recruits A, B, & C also needed to get trained and recruiter D did not know a trainer, then without this optimization, recruiter D would send one message for each of the recruits, creating an exponential explosion in the number of messages. However, agents keep track of the types of messages they send with a fully qualified name that includes the Java class name, the type of the intended recipient, and the identifier of the originator as shown in Figure 14.

ClassName.TargetRole.Originator Ex. FindPersonMessage.TrainerRole.TA9

Figure 14. Fully Qualified Names of Messages.

Agents only send out one message for each fully qualified named message in the agent's outbox.

The one optimization the author's left for future work was to only send messages directly down paths within the network to known targets, thus reducing message traffic significantly and improving the overall performance of the system. If agent A is connected to agents B, C, and D, C is connected to agent E, and agent A wants to send a message to E, the current model would send the message to B, C, and D, and the message would still arrive in E's inbox, but the other agent's would still forward the message even though they did not need to. The optimization would be to examine the agent's mental map, determine the necessary path for the message to reach the target, and create a message chain that ensured the message only followed the specified path. The bold arrows in Figure 15 demonstrate this optimization.

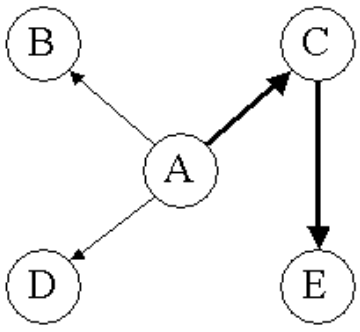


Figure 15. Message Optimization.

Before a message is sent or before it is answered, it is evaluated on the basis of benefit versus risk before being sent or answered. The ideas with

benefit greater than risk, or as the authors have abbreviated it, B > R, was that the benefit of sending or answering a message had to outweigh the risk of answering the message and possibly being observed by the enemy.

c. Benefits

Benefits model the various reasons why a terrorist agent sends, forwards, or responds to a message.

(1) Organizational. An agent's allegiance defines the organizational benefit. This benefit models the behavior that in general, the more committed an agent is to the organization the more likely the agent will act on the message.

(2) Personal. The personal benefit models the fact that people are generally somewhat selfish in nature and that they are more likely to serve their own needs before those of others and therefore will send their own messages.

(3) Influence. The influence benefit models the fact that who sent the message matters. If an influential arms dealer receives a message from some low level operator looking for a leader so that he may join a mission, the arms dealer will be less likely to pass the message than if the sender of the message was an influential leader such as Osama bin Laden looking for operators to join his latest mission.

(4) Goal Completion. The goal completion benefit reflects the fact that if responding to the message would bring the agent closer to completing a goal, then the agent is more likely to answer that message.

(5) Mission Draw. The mission draw benefit models the fact that if a leader needs a resource for an important mission that an agent might be more inclined to respond to that request than if the mission some small scale operation.

d. Risks

Risks model the reasons a terrorist agent refuses to send, forward, or answer a message.

(1) Familiarity. The familiarity risks models the fact that people are more likely to communicate with people they know than complete strangers. This risk allows agents to build a rapport with each other over time so that their familiarity risk is eventually driven down to zero and two agents become more likely to communicate with each other because of the relationship they have developed.

(2) Separation. The separation risk models that people are more likely to do some task for someone within their own circle of friends or known associates. If a person asks someone else to do something for his sister's friend's husband's cousin, that person is probably pretty unlikely to perform that task because of the amount of separation. However, for a person's immediate friends and maybe their friends the amount of separation probably is reasonable.

(3) Goal Synchronization. This risk models the fact that in planning, preparing, and carrying out missions, agents progress along a story line template of particular stages, and that like any traditional story during certain stages some events make sense to happen and in some stages others do not. During the climax of a story, it would not make sense to introduce entirely new main characters to the story. Likewise, as an agent progresses along the story line of the life cycle of a mission, it makes sense for an agent to process or participate in certain types of communications and ignore others. While Mohammed Atta is in Boston about to board a plane destined for the north World Trade Center building and he gets a call from an associate looking for Mohammed to introduce a friend to a well-connected arms dealer, Mohammed wouldn't take the call because he's in the middle of an important mission in which he knows he's going to die for the glory of his cause. The message type

identifier is used in evaluating the goal synchronization risk against a table created by the authors to model this behavior.

(4) Status. The status risk models the fact that the terrorist agents have a certain stature within the organization and that their time is valuable. Therefore, if an influential logistician receives a request from some second-rate leader looking for some fake passports, he is probably going to turn him down because the leader is beneath him, but if he receives a call from Pablo Escobar looking for the same thing, he's probably going to accommodate him. To place the status risk on par with mission draw for the purpose of processing the "get resource" message as described below, this risk is based on the product of the specialist's influence and experience.

e. Inbox

Each agent has an inbox that other agent's can place messages in. At the start of any agent's turn, that agent will process the messages in his inbox. The agent first checks the target role to see if it matches one of his roles. If it does not, then he places the message in his outbox to be forwarded on. If the agent has a role that matches the target role, then the agent evaluates the benefits and risks of answering the message. If the benefits exceed the risks, then the agent takes the action specified in the message's content, which is in the form of a ticket. The last action an agent takes in answering a message is to look at the message's forwarding chain and if any of the agents or links between them are missing from the agent's mental map he adds those nodes and links. As each message is examined it is removed from the agent's inbox.

f. Outbox

Each agent also has an outbox for sending messages to other agents. At the end of an agent's turn, the agent will process the messages in his outbox. The agent keeps track of the messages he has processed by their fully qualified name, so he does not send more than one message of any given fully qualified name. If the agent hasn't send a message of a given type, then he first

checks to see if he is the originator or if he is forwarding the message. Next, he evaluates the benefits and risks of sending or forwarding the message. If the benefits exceed the risks, then he creates a new message forwarding chain if he originated the message, or adds a new element to the chain if he is forwarding the message. The agent then puts the message in the recipient's inbox and lastly annotates how many times the agent has communicated with the recipient. This annotation is used in determining how familiar an agent is with another agent when evaluating the familiarity risk.

g. Messages

Messages provide agents with the ability to find people within the organization, seek out resource providers, and get in touch with leaders who need operators for their missions.

(1) Find a Person. This type of message provides an agent the capability to find an agent with a particular role if the agent does not know one directly. This message allows the originator to create a direct link to an agent with the desired role.

(2) Get a Resource. This message allows a leader to seek out resource providers if he does not know any, or to try to persuade a known specialist that isn't responding to the leader's attempt to use a connector to reach the specialist because the specialist is off producing a resource.

(3) Seek out a Leader. Operators use this message to find leaders who need manpower for their mission. Operators use this type of message when the trainer they just trained with does not know a leader directly.

8. Tickets

As mentioned above, tickets encapsulate procedural knowledge for the agents. A unique adaptation of tickets in the TNS, tickets inherit from a class in a discreet event simulation package called Simkit, described below, that allows them to be placed on an event list and therefore scheduled to occur on future turns. The only ticket that currently uses this scheme is the leader's "plan a

mission" ticket. The authors discussed using this for resource production, but that implementation has been left for future work.

a. Contact Tickets

(1) Make Contact. When a recruiter recruits a contact, the contact creates a permanent connector to the recruiter, or a link in the network, and the recruiter does the same with the contact. They both also add each the other person to their mental maps. The contact then marks the make contact goal complete.

(2) Become a Recruit. The next step that a contact takes is to change roles to a recruit and mark the "become a recruit goal" complete.

b. Recruit Tickets

(1) Prove Allegiance. The recruit uses this ticket to extend a connector the recruiter can hear so that the recruit can be initiated.

(2) Get Trained. Like the prove allegiance ticket, the recruit uses this ticket to extend a connector for the recruiter so the recruit can get in touch with a trainer.

(3) Become an Operator. The connector in this ticket is heard by a trainer, who then trains the operator for the turn.

c. Operator Tickets

(1) Join a Leader on a Mission. If the operator knows at least one leader, he first picks out the leaders that need operators on their missions and then he looks at the draw value for their missions. The operator joins the leader with the highest draw mission, receiving the leader's target and resetting a "stuck counter" that determines how bored an operator is (and how close to advancing to a trainer) and how impatient a leader is for finding recruiters and trainers. If the operator does not know a leader directly, he will extend a connector the trainer can hear and he will put a seek leader message in his outbox unless a trainer hears his connector and therefore connects with the operator. If the trainer does connect with the operator, the trainer will interrupt

this ticket, thus preventing the message from being placed in the outbox. The reason for this modeling decision was to work with how connectors and the listener model operate. The way the model operates is that the extender of a stimulator connector does not know if a receptor connector made a connection unless the agent on the receptor end changes some state variable in the agent on the stimulator end. Therefore, for the ease of encoding the desired behavior, it was easier to simply put a frame in the ticket to put a message in the outbox in the case that the connector was not heard and the ticket therefore not interrupted.

(2) Rehearse a Mission. This ticket increases a counter for the number of turns the operator has rehearsed a mission. If the counter reaches the required number of turns then the rehearse mission goal is marked complete.

(3) Execute a Mission. Like the "rehearse a mission" ticket, this ticket increases a counter for the number of turns the operator has executed a mission. When the counter reaches the required number of turns, then the mission execution goal is marked complete, the operator receives experience and influence from the mission, all of his goals are reset, and his current target is cleared out so he can join a new mission.

(4) Advance to a Trainer. This ticket removes the operator from a mission if he is in one and then changes the operator's role to that of a trainer on one caveat. The operator will only become a trainer if the system can handle having another trainer. The ratio between the number of operators in the system and the number of trainers in the system is computed and if that ratio exceeds a particular value then the operator can become a trainer. The idea behind this modeling decision was to prevent the system from becoming saturated with trainers.

d. Recruiter Tickets

(1) Find Contacts. With this ticket the recruiter extends a connector that sensed contacts could hear and then make a decision whether or not to join the organization.

(2) Verify Recruits' Allegiance. This ticket gives the recruiter the ability to increase the allegiance value of recruits until they reach a threshold at which time the recruits are eligible to get trained.

(3) Send Recruits to Training. In this ticket the recruiter checks to see if he knows any trainers directly. If he does, he looks the each trainer's influence and sends the recruits to the trainer with the highest influence, supporting the rich-get-richer phenomenon. The recruit and the trainer each create a link to each other and add the other person to their mental maps. The recruiter then receives either experience or influence for each recruit he sends to a trainer. If the recruiter does not know a trainer directly, then he sends out a find person message looking for a trainer role.

e. Trainer Tickets

(1) Train Recruits. This ticket works like the recruiter's "verify recruits' allegiance" ticket in that the trainer gives each recruit he is training a point of experience. If the recruit's experience exceeds a threshold, then the trainer turns the recruit into an operator.

(2) Send Operators to Leaders. This ticket works like a blend between the recruiter's "send recruits to training" ticket and the operator's "join leader on a mission" ticket. The trainer checks to see if he knows any leaders directly. If he does, he finds the leaders who need operators for their missions. Next he finds the leader with the highest draw mission and introduces the operator to the leader. The operator receives the leader's target and resets his "stuck" or bored counter and the leader's "stuck" counter for finding operators. The trainer then receives a point of experience or influence for each operator he

sends to a leader. If the trainer doesn't know any leaders at all or any leaders that need operators, he sends out a find person message looking for a leader role.

f. Specialist Tickets

The tickets for each of the specialists are the same except for the type of resources they provide or produce.

(1) Provide a Resource. When a specialist hears a connector from a leader requesting a resource, the specialist looks at his current level of resource before trying to provide the resource. The specialist provides resources to the leader up to either the amount requested by the leader or the amount the specialist has on hand, which ever is smaller. The specialist then receives either a point of experience or influence for every point of resource that was exchanged. The specialist then sets a Boolean latch that indicates that the specialist provided resources during the turn. This latch is used in the evaluation of the produce a resource goal as described above.

(2) Produce a Resource. This ticket allows the specialist to increase his stockpile of resources. The specialist's stockpile is increased by a random amount based on a right triangle distribution as shown in Figure 8 above, using the specialist's experience as the maximum and mean value.

(3) Advance to a Leader. This ticket allows a specialist to potentially advance to a leader role. If the specialist is not directly connected to a leader (which means most likely the specialist has become disconnected from the network, or disavowed), then the specialist changes to a leader. If the specialist is still connected to a leader, then a similar check occurs as was described for operators advancing to trainers. If the ratio of operators to leaders in the system exceeds a certain threshold, then the specialist will advance to a leader. Again, the reason for this modeling decision was to avoid saturating the system with leaders, who would subsequently require operators and operators are a scarcer resource than those the specialists provide, as will be discussed further below.

g. Leader Tickets

(1) Get Operators for a Mission. This ticket increments one of two "stuck" counters the leader has. The "stuck" counters allow goals to bubble up to the highest weighted goal over time, thus allowing the goal to become active. The stuck counter for getting operators was created to help the "get operators" goal bubble up to the top so that a leader would take action to find the source of operators: recruiters and trainers. This ticket works in concert with the find recruiters and find trainers tickets.

(2) Find Recruiters. This ticket works similarly to the "join a leader on a mission" ticket. If the leader does not know a recruiter, then the leader extends a connector that sensed recruiters can hear and puts a find person message for a recruiter role in the outbox unless a recruiter hears the connector and interrupts the ticket. The purpose of this ticket is to put the leader in contact with the source of new recruits in the organization.

(3) Find Trainers. This ticket works exactly like the "find recruiters" ticket, except that it is designed for connecting to trainers.

(4) Plan a Mission. This ticket creates a new target and a new mission for the leader. This ticket is unique in that it is scheduled via a discrete event simulation mechanism discussed below so that the ticket actually takes place some number of turns later and the leader "blocks" on the plan mission goal, much the same way network sockets block until they connect, until the leader creates a target and mission. The purpose for this design decision was to allow operators attached to a leader that just completed a mission the ability to become mobile and potentially migrate to another leader. If the leader did not take more than one turn to create a target and mission, the leader would always have the same operators in his missions and other leaders in the system might starve on the need for operators. By allowing operators to migrate between leaders, the system as a whole can progress further on accomplishing missions.

When the leader finishes planning a mission the "plan a mission" goal is marked complete.

(5) Request Resources. The tickets for requesting resources (the leader has one for each type of resource the specialists provide) increments the leader's stuck counter for requesting resources. If the leader does not have all the operators needed for a mission, the stuck counter for getting operators is incremented as well. The reason for incrementing the counter for getting operators is if the leader is just starting out and his goal for getting operators has a low weight, but the leader does not know any specialists, he'll never satisfy his request resource goals and the leader will remain stuck on those goals. Therefore, by incrementing the counter for getting operators allows the leader to find a source of operators and the leader can promote operators to specialists, therefore the leader can grow a network. The other counter is used to model the leader's impatience with waiting for a specialist to provide a resource or for the leader to get in touch with a specialist that has a needed resource. This counter is used to weight the "convert an operator to a specialist" goal, which in turn allows the leader to turn an operator into the needed specialist and the leader can progress along on the mission, albeit at probably a slower rate since the newly converted specialist will likely been unskilled. This type of ticket is also interruptible. The leader extends a connector specific to the type of resource requested and if a corresponding specialist hears the connector, then the ticket is interrupted, preventing the get resource message from being placed in the leader's outbox.

(6) Convert an Operator to a Specialist. This ticket allows the leader to convert his most experienced operator into a specialist to satisfy an outstanding resource requirement. The leader finds the most experienced operator and then extends a connector that the operator can hear, resulting in the operator changing roles to the desired specialist. The ticket also resets the stuck counter for requesting a resource.

(7) Lead Mission Rehearsal. This ticket simply extends a connector that operators in the mission can hear, which causes the operators to execute their "rehearse mission" ticket described above. The leader also performs similar actions as the operators.

(8) Lead Mission Execution. This ticket works like the "lead mission rehearsal" ticket, except that it is used for executing missions.

h. Messaging Tickets

(1) Find a Person. When this ticket is executed, the recipient and the originator create links to each other, they update their mental maps with the message chain as described above, and lastly they update the history value for each of the pairs represented by the message chain. Adjusting the amount the pairs receive affects the look of the network topology. The less the chain is rewarded, the easier relationships eventually degrade and fall apart, resulting in a more plausible looking scale-free network.

(2) Get a Resource. When this ticket is executed, the recipient of the message and the originator of the message create links to each other, update their mental maps based on the message chain, and the history values of the message pairs in the message chain are updated. This ticket also sets a resource requested latch for the specialist, which is used in evaluating the provide resources goal as mentioned above. This ticket also calculates the weighting applied to the specialist's provide resource goal.

(3) Seek out a Leader. Just like the other message tickets, the recipient and the originator create links to each other, update their mental maps based on the message chain, and update the histories of the agent pairs in the message chain. The operator receives the target from the leader, then the leader's stuck counter for getting operators is reset and lastly the operator's stuck counter (for changing to a trainer) is reset as well.

9. Connectors

a. Find Contacts

Recruiters extend this connector so that contacts can connect with it and make a decision to join the organization or turn the offer down.

b. Prove Allegiance

Recruits extend this connector that recruiters can connect with so that recruits can get initiated and become eligible for training.

c. Get Trained

Recruits extend this connector that recruiters can connect with so that the recruiter can introduce recruits to a trainer.

d. Become an Operator

Recruits extend this connector that trainers can connect with and provide training to the recruits.

e. Join a Leader on a Mission

Operators extend this connector that trainers can connect with so that the trainer can introduce the operator to a leader.

f. Request a Resource

Leaders extend these types of connectors that specialists can connect with to provide the leader with needed resources for conducting a mission.

g. Lead Mission Rehearsal

Leaders extend this connector that the operators in their mission can connect with and increment their rehearsal counters, indicating progress in mission rehearsal.

h. Lead Mission Execution

Leaders extend this connector that the operators in their mission can connect with and increment their execute counters, indicating progress in mission execution.

i. Convert an Operator to a Specialist

Leaders extend this connector that operators in their mission can connect with (they always have a receptor connector for this stimulator extended once they are in a mission) so that the leader can promote them to a specialist role.

j. Find a Recruiter

Leaders extend this connector like the connectors that recruiters use to find contacts, but leaders use this connector to find recruiters so that they can obtain a source of operators for their missions.

k. Find a Trainer

Leaders extend this connector just like the "find a recruiter" connector, except this one is used to find trainers.

10. Actions

a. Extend a Connector

This action simply extends a connector and then subsequently retracts it. If agent connects with the connector, then tickets fire for both of the agents before the connector is retracted.

b. Make a Double Link

In this action an agent takes the other agent in the connection and adds the other agent to his mental map; the process occurs for both agents. The agents are added to a container of directly linked agents and to a container of known agents. The mental map creates an agent pair for the two agents if one did not already exist.

c. Mark a Goal Complete

This action does simply as its title suggests.

d. Change Roles

This action removes the agent from the relationships associated with the current role, removes the role from the agent's collection of roles, creates

the new `Role` object and adds the role to the agent's collection of roles. The agent loses the goals associated with the old role and gains the new goals associated with the new role.

e. Recruit Verification

This action adds a point to the recruit's allegiance value. If the recruit's allegiance value then exceeds a threshold set by the recruit training relationship, then the recruit's "prove allegiance" goal is marked complete.

f. Reward an Action

This action iterates a number of times equal to a scalar value, as mentioned above in the tickets that use this action, and awards one experience point or one influence point on an equal basis during each iteration. When that part of the action is finished, the agent is awarded allegiance on a triangle distribution with a minimum of –1, a maximum of 1, and a mid-point of 0.5. The reason for the modeling decision to use this distribution for allegiance was that a terrorist agent can gain influence or experience based the event that they just participated in, whether it be sending an operator to a leader, exchanging resources, or finishing a mission, but the agent either has a good experience, a bad experience, or a neutral experience. The authors weighted the distribution so that agents had a lower chance of having a bad experience and a higher chance of having a neutral experience, so that an agent's commitment to the organization slowly increased over time. A feature the authors left for future work was to remove an agent from the organization when the allegiance value dropped below a certain threshold.

g. Put a Message in the Outbox

This action creates a new message using Java's reflection capabilities and then places the object in the agent's outbox.

h. Train Recruits

This action works much like the recruit verification action, except it adds a point to the recruit's experience value. When the value exceeds a

threshold set by the recruit training relationship, the recruit changes roles to an operator.

i. Receive a Target from Leader

This action adds the operator to the leader's mission and the operator receives information about the target.

j. Interrupt Another Ticket

This action simply causes another ticket to stop executing by setting a Boolean flag in the target ticket.

k. Rehearse a Mission

This action increments a mission rehearsal counter. If the counter exceeds the required number of rehearsal turns for the target, then the mission rehearsal goal is marked complete.

l. Execute a Mission

This action increments a mission execution counter. If the counter exceeds the required number of execution turns for the target, then the agents in the mission receive experience and influence. The amount of reward points available to the agents in the mission is the draw value of the mission. The leader always receives the largest share of the reward, with a minimum of 25%. The rest of the operators in the mission receive a reward proportional to their influence plus experience compared to the sum of influence and experience from each of the operators in the mission. Therefore, more influential and experienced operators receive more influence and experience than their less experienced and influential brethren, furthering the rich-get-richer phenomenon. The reward value becomes the scalar used in the reward action described above. Lastly, this action marks the mission execution goal complete.

m. Mission Cleanup

This action removes the mission rehearsal and mission execute tickets from both the operators and the leader and replaces them with new ones since they were modified when the mission was completed by the "execute a

mission" action above. The action then resets all of the goals for the operators and the leader and lastly clears out the target information for the operators and clears out the mission and target information for the leader.

n. Remove Self from a Mission

This action removes the operator from the mission, creating a vacancy that the leader now has to fill. The operator's goals are all reset except for the advance goal and the target information is cleared out for the operator.

o. Produce a Mission

This action creates a target and then creates a mission, associating the target with the mission.

p. Increment a Stuck Counter

This action simply increases the stuck counter for the agent.

q. Reset a Stuck Counter

This action simply resets the stuck counter for the agent.

r. Increment a Get Operators Stuck Counter

This action increments a separate stuck counter the leader role uses as described above.

s. Reset a Get Operators Stuck Counter

This action resets the separate stuck counter the leader uses as described above.

t. Produce a Resource

This action produces a random number of resource points using a right triangle distribution with the maximum and mean set to the same value as the specialist's experience value.

u. Resource Exchange

This action increments the resource level collected for the leader's mission and decrements the resource level the specialist has on hand as described above. This action also rewards the specialist using a scalar equal to the number of resource points exchanged.

v. Set a Latch for Requesting a Resource

This action simply sets a Boolean latch for the specialist indicating that a leader requested a resource from the specialist via a message as described above.

w. Set a Latch for Providing a Resource

This action simply sets a Boolean latch for the specialist indicating that the specialist did provide resources during the turn.

x. Increment a Provide Resource Goal Weighting

This action creates a weight value to be added to the specialist's "provide a resource" goal if the specialist processes a "get resource" message. The amount of the additional weight is the difference between the draw of the leader's mission and the status risk of the specialist. If a leader and a specialist on nearly on par with each other in terms of influence and experience, this value should be small, reflecting the relative influential power agents have with each other when dealing with missions and resources.

y. Update Mental Map from a Message Chain

This action takes a message's forwarding chain and updates the mental maps of the originator and the recipient by adding nodes and links from the chain that are absent in the respective agents' mental maps.

E. SIMULATION DESCRIPTION

1. Overview

The Terrorist Network Simulation (TNS) demonstrates that a Multi-Agent System build around the descriptions of the interactions between the various roles in a plausible terrorist organization does indeed form a scale-free network without direct intervention or top-down control. The authors wanted to describe the life cycle of terrorist agents and the organization as it plans, prepares, and carries out terrorist missions. Therefore, the authors decided to create a turn-based simulation, where each agent senses other agents, determines which agents to form relationships with, what goal to perform, and what messages to

process. The turn-based structure of the simulation allows the organization to evolve temporally while preserving certain mechanics that make the simulation possible.

2. Turn Structure

To preserve the idea of preferential attachment and the rich-get-richer phenomenon, at the beginning of each turn the agents are sorted into a list in decreasing order of influence. This sorting allows the most influential agents to always take their turn before the less influential ones. Next, the history values for each of the agent pairs in the simulation are decremented to create the aging relationship behavior in the model. The next part of the turn constitutes the main section where agents take their individual turns. Each agent first processes his inbox, and then he checks for sensed contacts. He adds those agents he senses to those he is directly connected to as his sensed environment and uses that sensed environment as necessary for evaluating his goals, which comes next. After evaluating his goals, he takes the highest weighted goal and executes whatever ticket is associated with that goal. Some tickets are not executed until the agent connects to another agent's connector, so some goals do not have tickets that necessarily execute during the agent's turn, but get executed on another agent's turn when a connection is made. The last part of each agent's turn is to process his outbox. Once all the agents have taken their turns, the simulation checks for any relationships that should be terminated because their history dropped past a minimum threshold. The last part of the turn is to remove any contacts that have not been contacted for a set number of turns or have been contacted, but decided not to join the organization. The turn structure is summarized below in Figure 16.

1. Sort the agent list
2. Decrement agent pair history values
3. Agent turns
    a. Process inbox
    b. Sense/detect agents
    c. Check relationships
    d. Evaluate goals
    e. Execute active goal
    f. Process outbox
4. Check for aging relationships
5. Remove contacts that did not join

Figure 16. TNS Turn Structure.

3. Discreet-Event Simulation Elements

The authors wanted to introduce contacts into the simulation using a plausible arrival process, so they turned to the discreet event simulation (DES) package Simkit, primarily developed by Dr. Arnie Buss of the MOVES Institute at NPS. Once the basic integration of the Simkit libraries was made with the TNS, recruiters were added to arrive into the simulation, a timing thread was included to enhance the graphical rendering, and tickets were extended such that they could be scheduled as well.

a. Simkit

Simkit provides the developer with powerful tools to create discreet event simulations ranging from the trivial to complex. A DES is controlled via an event list and an event list consists of events that have been schedule to occur at a particular time in the simulation. No simulation time passes during an event, just between events. The earliest scheduled event currently on the event list becomes the next event executed. Events can have a priority, so if two events have the same time scheduled on the event list, the higher priority event occurs first (Buss, 2001, p. 1). The TNS schedules turn events to occur one (1) unit of simulation time apart. Each turn event schedules a

new turn event to occur one (1) unit later. Due to the turn-based nature of the TNS, all events on the event list are integer time steps.

In the TNS, Simkit controls two arrival processes, one for contacts and one for recruiters. An arrival process is a scheduling process by which the times between the arrivals of new events are independent and identically distributed (IID) random variables. IID random variables come from the same probability distribution (Law and Kelton, 2000, pp. 12-13). The TNS uses a Poisson arrival process because is the most common type of arrival process (Law and Kelton, 2000, p. 389). The Poisson arrival process uses an exponential probability distribution for the interarrival times, or the times between the arrivals of new entities into the simulation. Contacts arrive into the simulation at a much higher frequency than recruiters. Even so, the authors found that contacts become the scarcest resource for the leaders in putting together their missions since an arrival process controls the generation of new contacts. The specialists can generate numerous points of a given resource in a particular turn while contacts continue to arrive less frequently into the simulation. As such, the random number seed for determine a mission's operator requirements is typically much smaller than that of the other resource requirements because of this disparity between the production capabilities of the two resources. Examining the resource production model for further refinement has been left for future work, although the authors did consider using an inventory model combined with the ability to schedule tickets that produce resources for future turns.

b. Discreet Event Graph

Discreet event graphs are used to visually represent a discreet event simulation. Event graphs depict how events from one from the other, how events are scheduled, and what the times are between events. Event graphs also show the significant state variables used in the simulation related to events.

Event graphs show event listeners if any are present in the simulation. The event graph for the TNS is shown below in Figure 17.

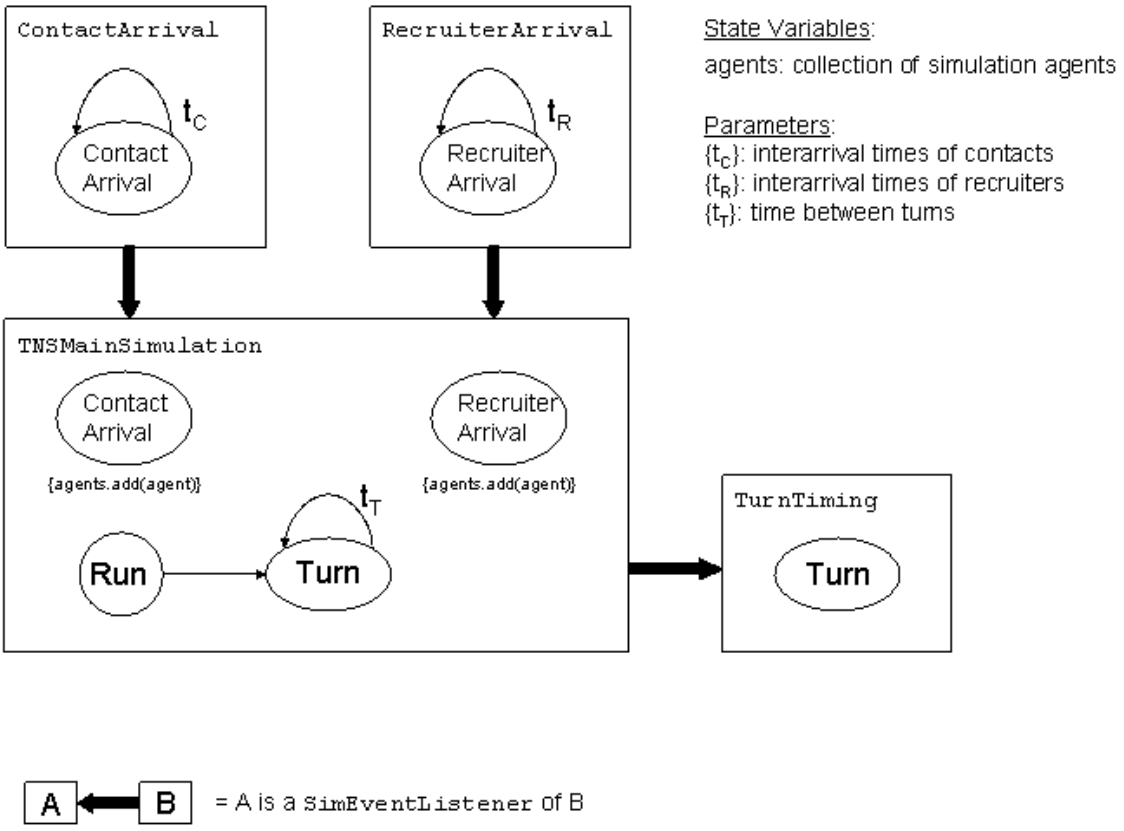


Figure 17. TNS Event Graph.

c. Listener Models

As seen above in Figure 17 the TNS event graph incorporates several event listeners. These event listeners work much the same as the connector listeners. In the scheme of the event model, when a contact or recruiter arrival event occurs, the main simulation hears that event through the listener model. Subsequently, the main simulation invokes methods that create the new `TerroristAgent` objects and add them to the simulation's collection of agents.

d. Timing

Whenever a turn event happens in the main simulation, a helper class hears that event an invokes a `sleep()` method on a `Thread` object. This timing event slows down the graphical rendering of the network so that users can see the network evolve at a reasonable speed.

4. Graphics

The authors decided to adapt an open source project designed to display and manipulate graphs (a superset of networks) vice trying to write their own. This decision saved countless hours of work, leaving the authors the ability to concentrate on the simulation itself. The graphics used in the project were not without some issues however as mentioned below. The package used by the authors was TouchGraph.

a. TouchGraph

The TouchGraph package of classes was designed by Alex Shapiro and can be found at the TouchGraph website, www.touchgraph.com, under the Development section, http://touchgraph.sourceforge.net/index.html. TouchGraph was designed with interactive graph and network exploration by the user in mind, but the package's graph rendering capabilities were more than adequate for use in the TNS even though the TNS was not designed with user interaction in mind. The TNS uses TouchGraph version 1.21. Figure 18 below shows what a basic TouchGraph application looks like.

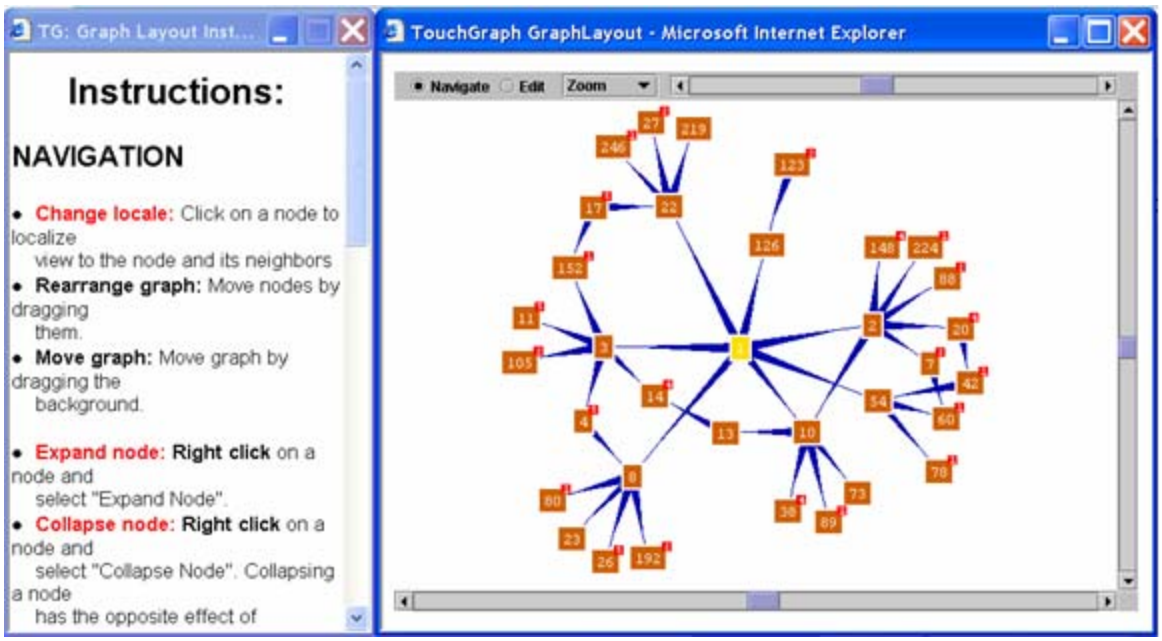


Figure 18. Basic TouchGraph Application.

b. Adaptations to TouchGraph

The authors used the TouchGraph display in two places in the simulation. The main simulation window uses a descendent of a TouchGraph `GLPanel`. The authors wrote their own constructors, and overwrote the `initialize()`, `createGraph()`, `addUIs()`, and `buildPanel()` methods to fit their needs for the simulation. TouchGraph interaction is controlled through user interface (UI) classes. The authors created their own UI class, `GLExplicitUI` (named after the network's explicit map, or ground truth), following the pattern the TouchGraph designers used for their `GLEditUI`. The `GLExplicitUI` class included code to launch agent "brain lids," which are graphical displays that provide information about a particular agent. "Brain lids" are explained further below. An example of the resulting main simulation panel is shown below in Figure 19.

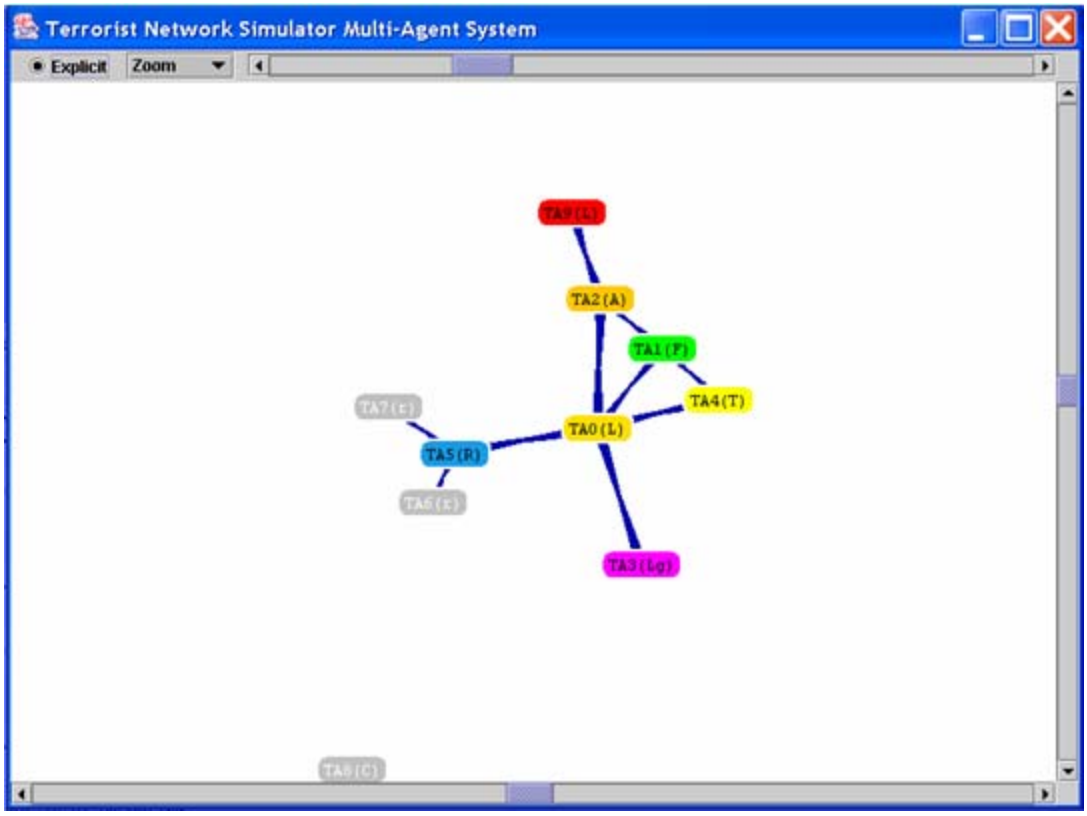


Figure 19. Example Main Simulation Panel.

Figure 19 above shows the various types of agents in the simulation and how they are graphically represented. Each agent role is assigned a color and a symbol to aid in picking out the agents in the network, particularly when the network grows rather large. Role colors and symbols are shown in Table 1 below.

Role	Symbol	Color
Contact	C	Light grey
Recruit	r	Grey
Operator	O	Dark grey
Recruiter	R	Blue
Trainer	T	Yellow
Arms Dealer	A	Orange
Logistician	Lg	Magenta
Financier	F	Green
Leader	L	Red
Multiple Role agent	As for each role	Cyan

Table 1. Agent Role Colors and Symbols.

The UI class provides several controls for viewing the network: zoom, rotate, locality, and drag. Zoom and rotate functions are self-explanatory. The user can grab either a node or the screen itself to drag the network around for better viewing. Once a node is selected by a single left mouse click, the locality control allows the user to see those agents that are a specified degree of separation from the selected agent. The slider bar on the top of the display controls the degrees of separation. Figure 20 below shows what the graph looks like when the locality control is dialed down to a value of one. The little red squares in the upper right portion of the nodes contain a number indicating the number of links or edges connected to that node but are hidden from view.

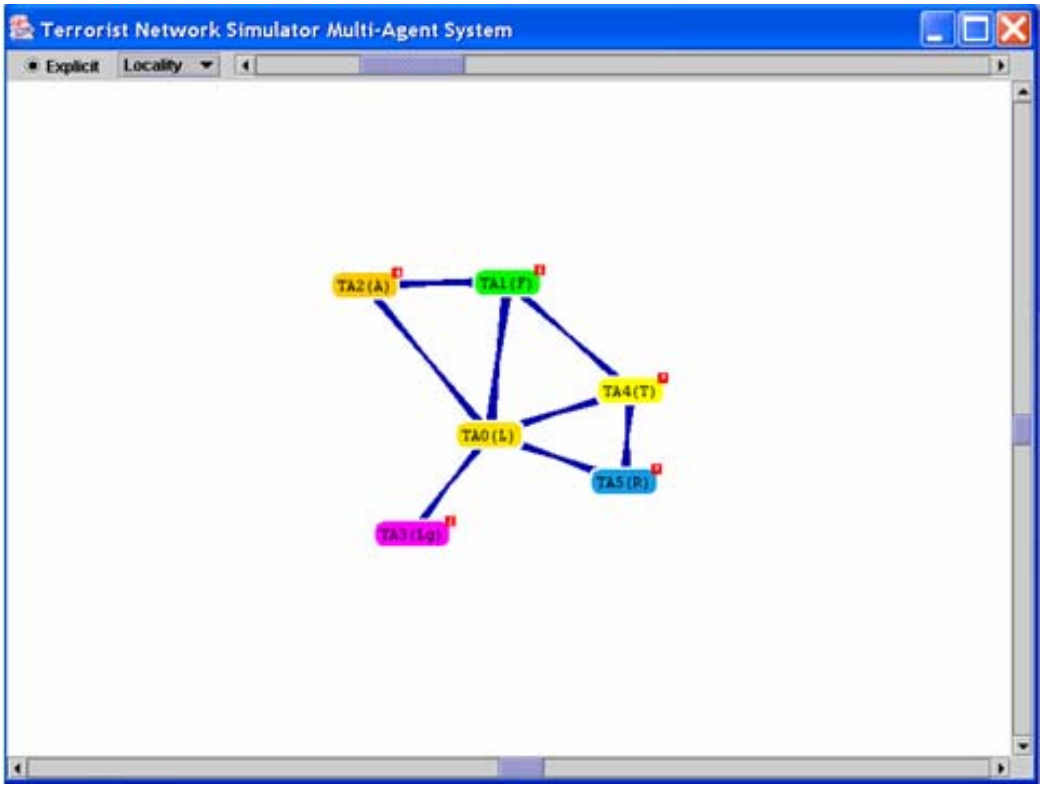


Figure 20. Locality Control.

In the TNS, when two agents form a link between each other, two edges are created, one in each direction, hence the difference in the look of the links in the TNS from the normal TouchGraph links as shown in Figure 20 above. When new agents appear in the simulation, when they disappear from the simulation, and when links are created and destroyed, the simulation dynamically draws the changes. These changes are made possible through the listener models employed in the TNS.

c. Listener Models

The TNS graphics packages use listeners for changes in nodes, links, and agent state. The explicit map drawing panel, `TNSPanel`, listens to each agent in the simulation for changes in links to the explicit map. When new agents are added to the simulation or when agents are removed from the simulation (currently only contacts who are not contacted or do not join the organization are removed), the `TNSPanel` is notified of the changes. In the agent

"brain lids" state change listeners are used to update both graphics and tabular data as will be explained further below.

d. Agent "Brain Lids"

An agent "brain lid" provides the user the ability to peek inside an agent to see the agent's roles, goals, personality, and mental map. Some roles have specialized panels that provide additional information particular to those roles. An agent "brain lid" for a leader role is shown below in Figure 21.

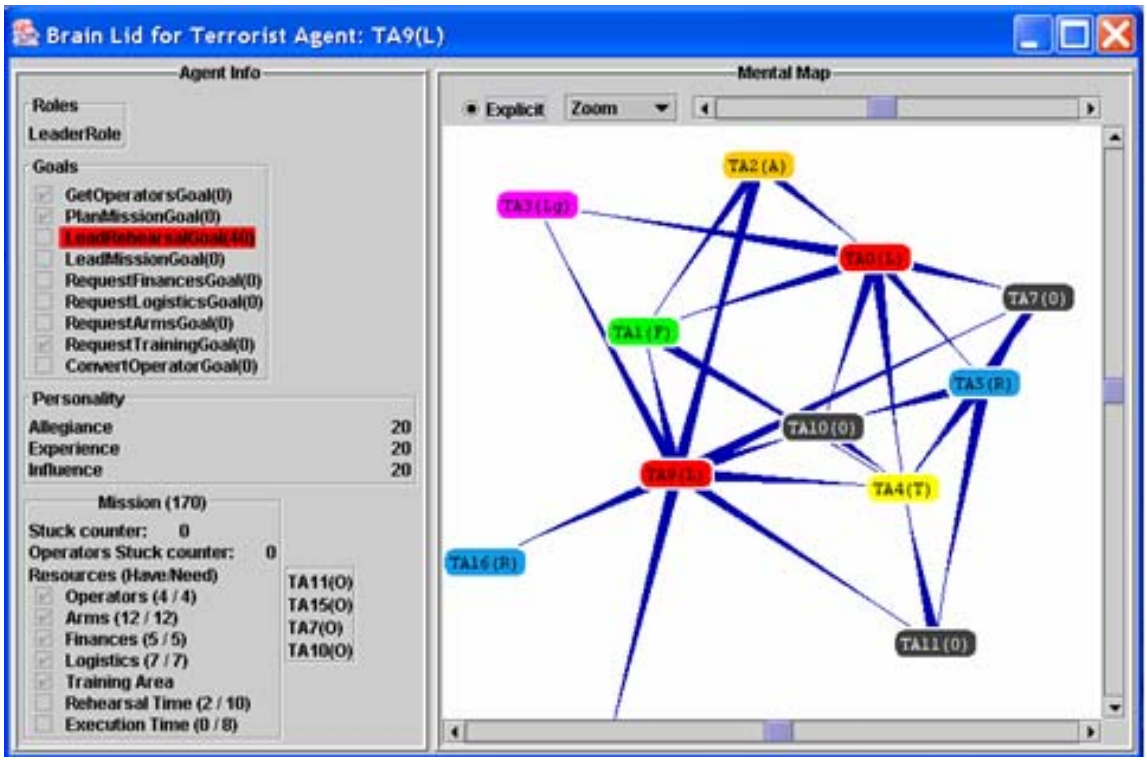


Figure 21. "Brain Lid" for a Leader Role.

On the left side of the "brain lid" is the agent's information and on the right side the mental map. In the goals section of the agent info the goal weight for each goal is shown in parenthesis to the right of each goal and the active goal is highlighted in red. Completed goals are marked with a check to the left of the goal. The "brain lid" shown in Figure 21 above shows a panel for the leader's mission at the bottom of the agent information. The number to the

right of the word "mission" in the border title is the target's draw. The status of the leader's stuck counters are displayed and then the mission requirements are shown next with how much the leader has followed by how much the leader needs. Operators that have joined the mission are shown to the right of the mission information panel.

The mental map on the right side of the "brain lid" shows the agent's worldview of the network. Only those agents the agent knows directly or knows about indirectly through messaging are displayed on the mental map. Links in the mental map are unidirectional, which highlight the indirect links in the agent's mental map, those links between agents only known about, but not directly linked to. The mental map-drawing panel has link and node change listeners like its parent, `TNSPanel`. The "brain lid" itself listens to changes in the agent's state so that the "brain lid" can dynamically update the agent's information. This capability makes it easy for a user to follow a leader's mission and watch the progression on the "brain lid" and the explicit map. A brain lid for a specialist is shown below in Figure 22.

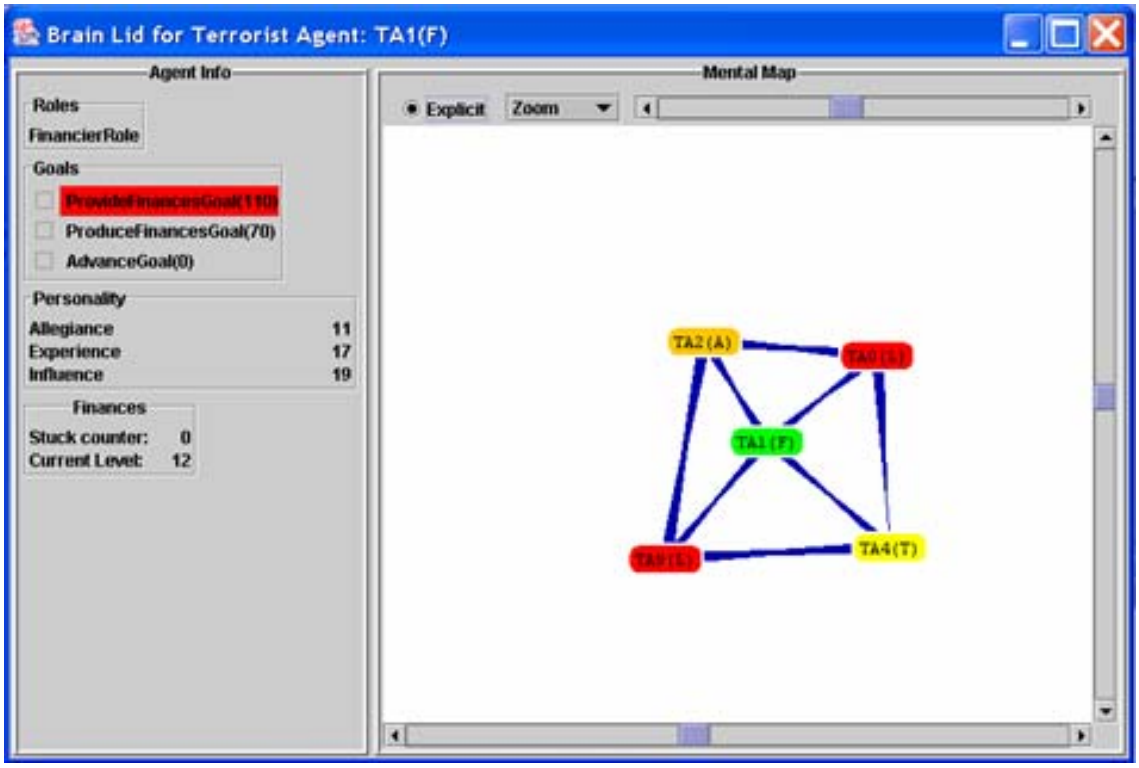


Figure 22. "Brain Lid" for a Specialist.

Specialists have a panel that shows the current level of their resource and the status of their stuck counter. The "brain lid" for an operator in a mission is shown below in Figure 23.

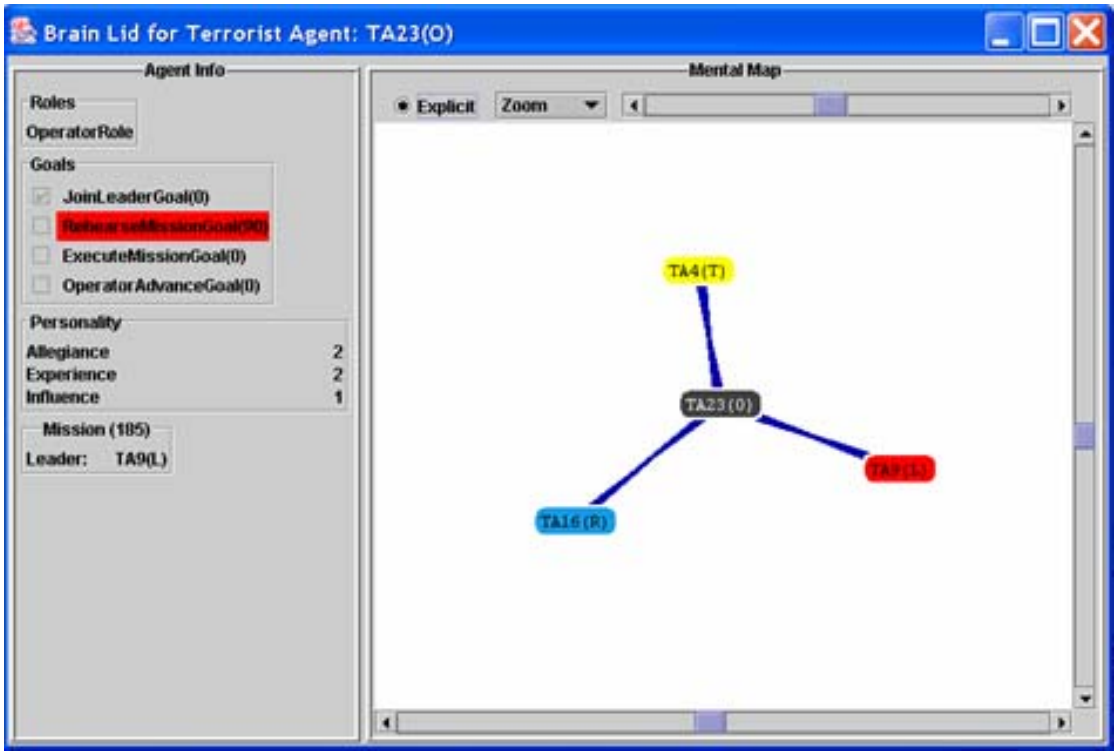


Figure 23. Operator "Brain Lid".

The operator "brain lid" shows the mission the operator is part of by displaying the draw of the mission's target and the leader who is leading the mission.

e. Graphics Issues

The graphics displaying capabilities of TouchGraph worked the majority of the time. Occasionally though the drawing panels of the explicit and/or cognitive maps would blank out without explanation. When the number of debugging statements was reduced the frequency of graphics panel crashes appeared to be less frequent. TouchGraph has some minor issues with the drawing of links when the locality number is low such that links are draw without their associated nodes on the other end. Also, sometimes a similar problem arose when a contact seemed to be contacted and a link was drawn from the recruiter to the contact, but only the link and not the node were drawn.

Since TouchGraph is still developing into a mature product, the authors are confidant these issues will be resolved in future versions of the software.

5. Emergent Behavior

After running the simulation for several hundred turns, the emergent network clearly forms a scale-free, hub-and-spoke looking network. Figure 24 below shows the network after one run of 350 turns. The run that created this network started with one leader, one trainer, and one recruiter.

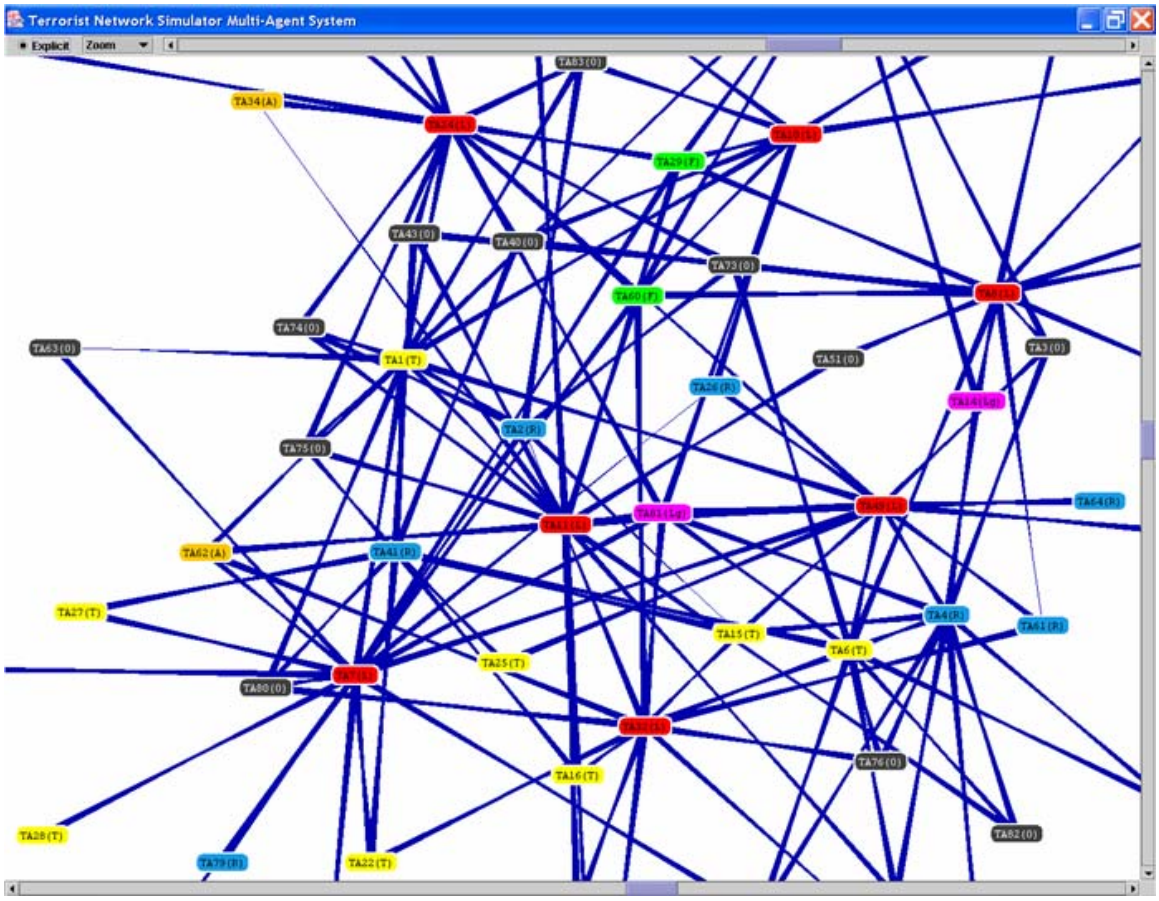


Figure 24. Emergent Network Behavior.

Figure 24 clearly shows the leaders (in red) as the most connected agents in the simulation, followed by some of the trainers (in yellow) and recruiters (in blue). The leaders have formed their own cells, creating a hub and spoke look to

the agents attached to the leaders. Figure 25 below shows the first leader in the system, TA0, and all the agents within one degree of separation from that leader.

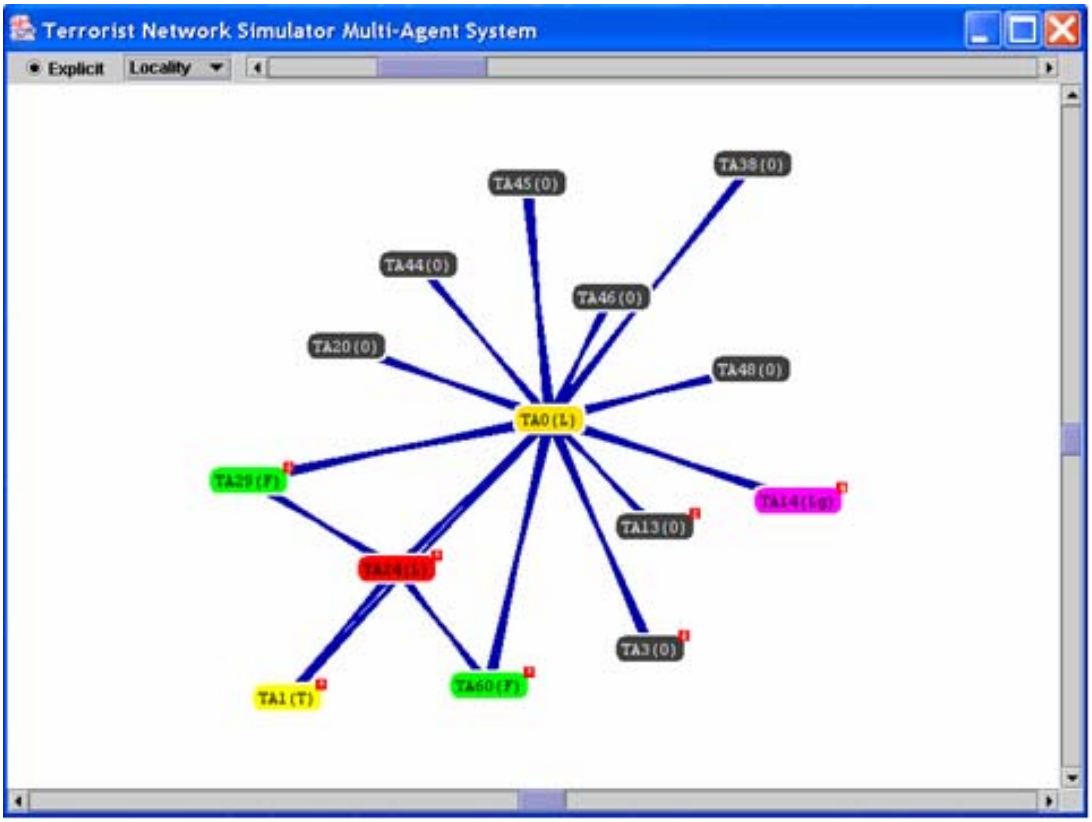


Figure 25. Leader's Circle of Followers.

The leader definitely has a small band of followers and the leader is connected to a logistician and two financiers, but no arms dealer. The leader is also connected to the original trainer, TA1. The other leaders in the network have very similar looking networks. To show how well connected the original trainer is, see Figure 26 below.

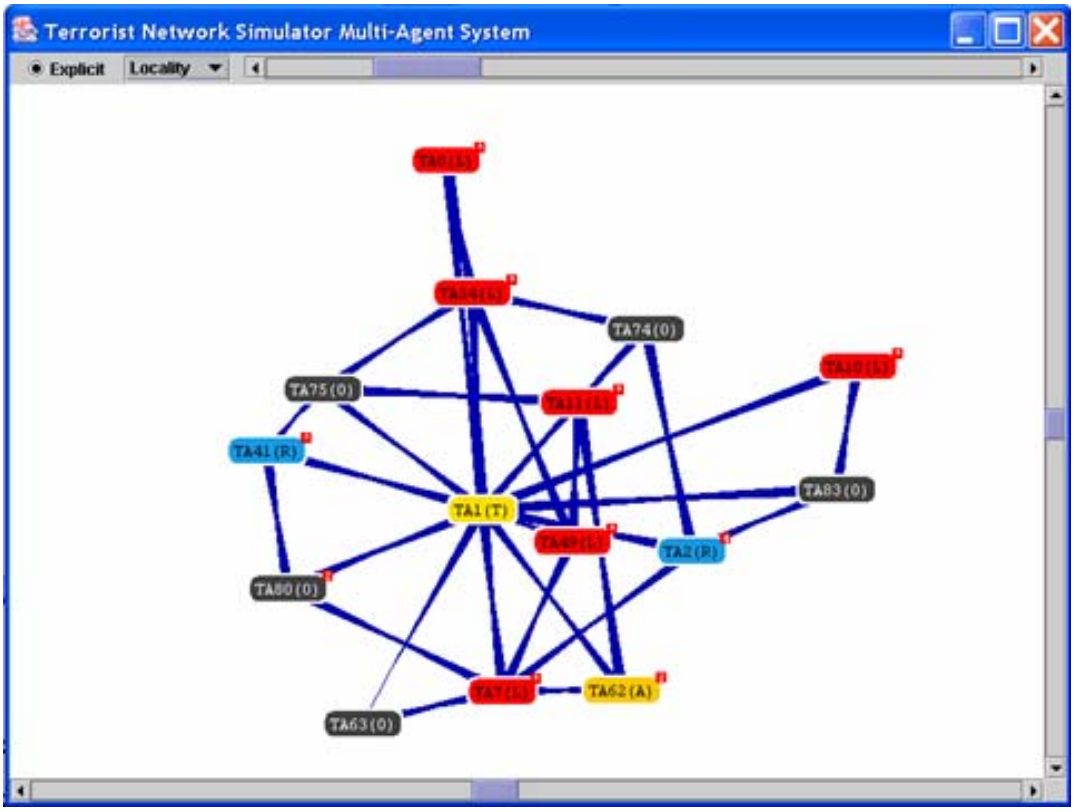


Figure 26. Original Trainer's Closest Associates.

The original trainer knows six out of seven of the leaders that emerged in this network, showing that the rich do get richer as the trainer continues to pass on operators to the leaders as the trainer of choice. Interestingly, the higher the operator to leader ratio, the more connected the original trainer becomes as those extra operators not in a mission stay attached to that trainer. As more leaders enter the system, the operators move on to cells, eventually losing contact with the trainer and the trainer begins to look less like the most connected agent in the system, but still a hub nonetheless. The world of the original recruiter is not as well populated as seen in Figure 27 below.

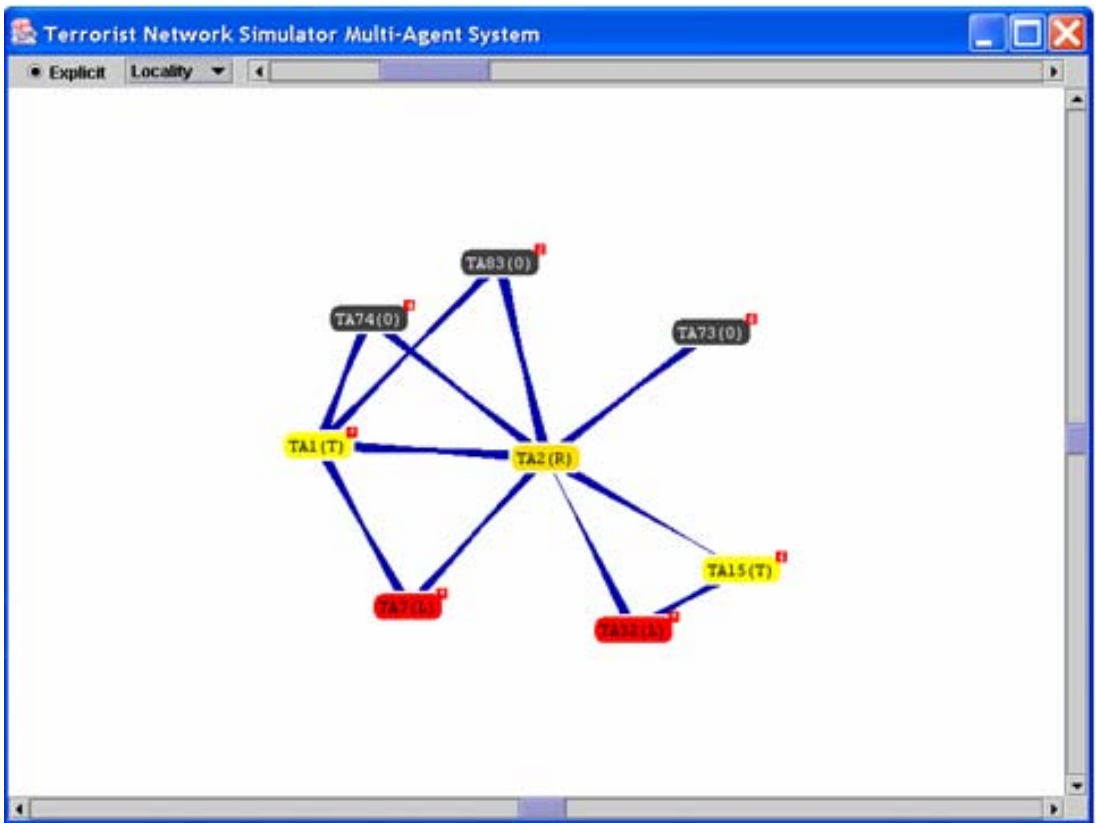


Figure 27. Original Recruiter's Closest Associates.

The recruiter is a minor hub, one connected to two trainers (including the original) and two leaders. Since recruiters are removed from the process of providing operators to leaders by one extra step as compared to the trainers, they are less well connected within the organization. The recruiters remain locally influential, gathering recruits, but not real involved in the rest of the organization as was the expected behavior. Lastly, the specialists' inner circle remains the leaders they interact with to provide resources as evidenced by the financier's network in Figure 28 below.

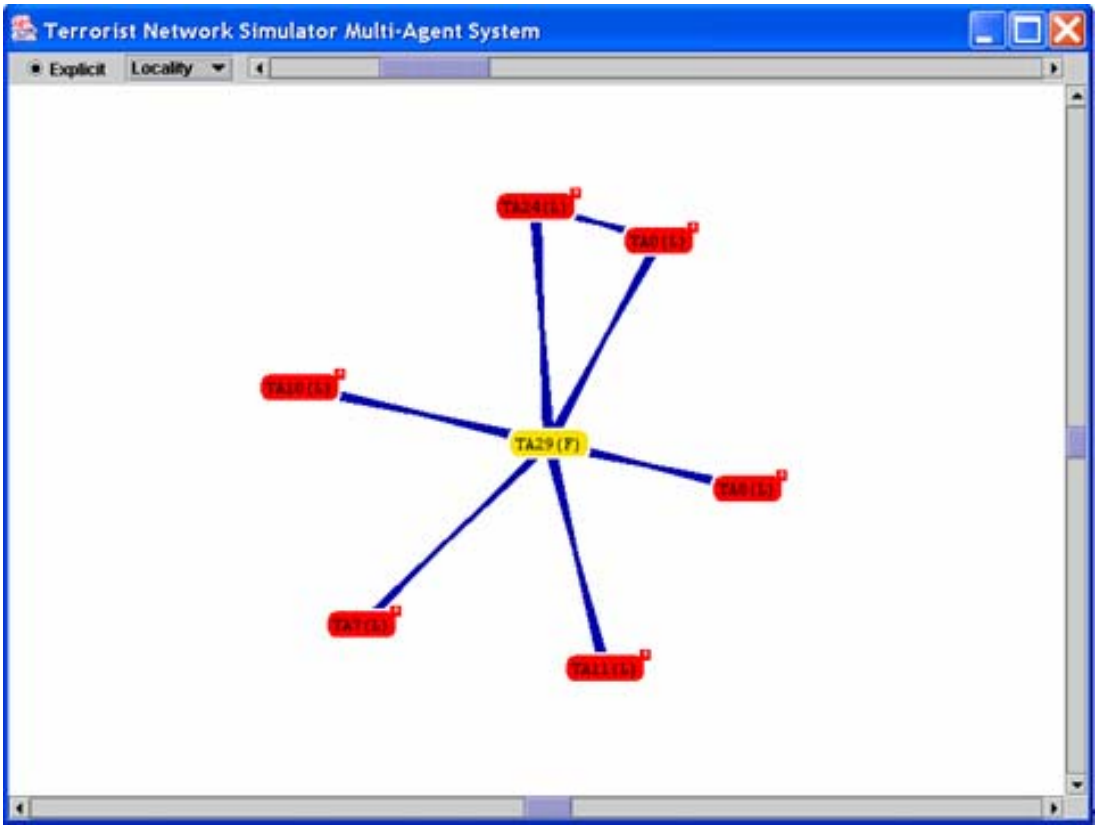


Figure 28. Financier's Inner Circle.

The financier knows six out of seven leaders in the system and no one else, as is the expected behavior since they only move in the highest circles once they become influential. As a whole the system produces reasonable and plausible scale-free networks based on the low level interactions of the agents, which were defined based on their expected associations and activities with each other.

6. Future Work and Optimizations

The authors had several other elements they wished to implement in the TNS, but were left for future work. Most importantly, the authors' had intended to implement the four Stimulus Based Discovery tactics with a Blue agent that "learned" about the terrorist network from intercepted communications and observed connectors. Blue's probability to detect a communication or connector would be based on many factors including the terrorist agents experience,

familiarity with the recipient and network penetration. For example, a very experienced financier simulates a wealthy individual sympathetic to the terror cause or an organizer that operates among sympathetic elites. Whereas a low-experience financier simulates operators that conduct credit card fraud and armed robbery to gather resources. In this example, Blue's probability to detect credit card fraud and armed robbery is significantly higher than an experienced financier that provides resources only through established trust relationships. Blue's variable probability of detection would needs to be implemented across all interactions. This probability scheme would form the basis for Blue's capability to construct his own mental map of the terrorist network. From this map, Blue would also need a decision system to create different stimuli and to target and/or engage hubs when discovered. With these components in place the authors intended to conduct a series of experiments that collected quantitative data such as a network suppression score measured by the number of mission points that were successfully executed, and other network health metrics referenced in social networking literature. Furthermore, the authors felt that qualitative data would be available on the emergent behavior of the network when subjected to attack.

Additionally, the authors had intended to configure the simulation from XML files so that the dozens of parameters controlling agent interaction could be changed without re-compiling the simulation's source code. This step is critical to running a large sample of different networks that validate the scale-free topology under a wide array of input variables. Another feature the authors had on their list was the ability to "grow" an organization for a period of time and then store the state variables of the organization with a capability to recall them later. This allows experimentation on "mature" networks. For example, these mature networks would then be used in several experiments with different targeting strategies to show how the same network responded to different forms of stimulus and attack.

Directed messaging, already mentioned above, would cut down on the number of messages being created and processed in the system and therefore improve the performance of the system.

Another optimization that would improves performance deals the authors' adaptation of RELATE in `RelationshipManager`. When an agent was checking to see if another agent should be added to an existing relationship and that proposed agent was not maximally connected in any the first agent's relationships, a new one was created. As an optimization, instead of just simply creating a new relationship, the algorithm could check the proposed agent's relationships to see if the first agent was maximally connected in the second agent's relationships, thus possibly cutting down on the number of `Relationship` objects created. Additionally, the TNS does not have any code to eliminate duplicate relationships. The authors found this problem occurred when a third member of a three-way relationship left the relationship that the remaining two stayed in the relationship. When the remaining two were involved in several three-way relationships where the third member was different in each one, but the other two remained the same, the remaining two would end up with several `Relationship` objects with the same membership, thus wasting memory.

Lastly, the TNS was designed so that agents could have multiple roles, each having multiple goals. As such, the code used Java `Iterators` and `Enumerations` extensively for iterating through the various `Vectors`. In these iterations, new objects were created and subsequently destroyed during each loop, creating additional work and overhead for the object creation and destruction. To optimize these iterations, one object reference should be created outside of the loop and then it should be assigned the reference for each object in the `Vector`, thus saving processing time and memory.

V. CONCLUSIONS AND FUTURE WORK

Two structural characteristics of conflict in the Information Age are apparent now in the pioneering days of this new era. First, the Information Age empowers individuals to act alone or in small groups with great strategic impact. This elevates the unpredictable nature of a deranged individual or secret sect to strategic significance and brings with it high uncertainty about who opponents will be and where they will strike. As such, it becomes futile to create exhaustive plans to account for all avenues of attack. The second characteristic obvious now is that the U.S. military has broken the historic link tying range with accuracy. American Sailors, Marines, Soldiers an Airmen must no longer get close to get accurate. The challenge for attacking networks of empowered individuals devolves to finding valid targets for the application of that firepower that leads to network suppression.

The first step in finding such targets requires a revised strategic framework for evaluating networked adversaries. However, the Joint Professional Military Education given to most military officers has become formulaic and is not well suited to adversaries that defy categorization in industrial terms. Additionally, the Joint Campaign Planning Process is not aligned to fight adversaries that cannot be mapped before hostilities commence. This is a disturbing shortfall in the capability to fight networks that demands a new concept for a new kind of fight. This new concept should allow for broad application of principles, but provide clear discriminates of who and what to engage.

Unfortunately, most attempts to locate and discriminate network threats are reliant on passive systems to "put the pieces together" and "see where it leads." Such defensive tools are evidenced by ongoing efforts to increase surveillance, build large databases and information management systems, and

the organizational redesign of numerous law enforcement agencies. These tools and new bureaucracies are worthwhile, but lack key components of a **military strategy** to defeat network threats. Because the aforementioned steps rely heavily on unintended mistakes by an adversary in order to gain detection they are inherently defensive. If an adversary is cunning and avoids detection there are few tools in place that force mistakes. Consider how easily major league baseball players would hit homeruns if they did not have to hit against pitchers that force mistakes. Therefore, while defensive measures are critically important to securing America from emergent threats they do not form a complete solution set.

Fortunately, discoveries in new areas of science provide tools that allow for military attack against elusive networks. Albert-László Barabási and a group of researchers at the University of Notre Dame have recently brought to light the mathematics and science on one of nature's most naturally occurring phenomena: networks. The importance of this discovery is amplified by the fact that natural human social activity forms networks, independent of any other organizational structures that those individuals may by a part of, and that those networks are scale-free. Since those networks are scale-free, they benefit from a natural robustness against random failures and attacks, yet at the same time, those same networks suffer from one highly crippling Achilles heel. The most connected nodes in a scale free system, called hubs, are susceptible to attacks which will break the network apart, and eviscerate its structural connectivity. If the hubs in a scale-free network can be found and a significant portion of them negatively affected in near simultaneity, then network functionality will halt, effectively shattering its operation.

The issue then for military intelligence and targeting is to find those hubs. To take the offensive against networks the authors have proposed a strategy to find hubs in concealed networks. This strategy called "Stimulus Based

Discovery" aims to accelerate learning against a denied system, thus leading to targeting information faster than standoff observation.

The case studies in Stimulus Based Discovery demonstrate the four tactics for stimulating networks to reveal their topology. The tactics presented are explicit nodal stimulus, explicit link stimulus, cognitive nodal distortion, and cognitive link distortion. In each case, stimulating the adversary network accelerated the revelation of network components that would have otherwise remained hidden, been learned with much less fidelity, or taken much longer to discover. Exploiting the naturally occurring social network between human nodes attained the success achieved in each case. The theory and case studies in Stimulus Based Discovery suggest three findings about attacking networks.

- All complex human systems form scale-free networks.
- Scale-free networks are quite robust against failure and random attack but crumble when network hubs are successfully debilitated.
- Stimulus Based Discovery leads quickly to hub identification and network mapping thereby accelerating network collapse.

Since social networks were at the center of stimulus efforts, then a model of social human behavior in a networked organization could be built as a laboratory for applying the authors' proposed targeting strategy. Using a natural parallel for complex human interaction, a Multi-Agent System (MAS), the authors created a model of human interaction within a hypothetical terrorist organization. The design focused on interactions and collaboration between terrorists, represented as software agents, and framed by the relationships that terrorist archetypes could plausibly have with each other. Each agent takes on one or more of these archetypes, or roles, in the organization, and each role brings with it associated goals that drive the agents' actions.

The MAS, dubbed the Terrorist Network Simulation (TNS), was founded on the design principles of Jacques Ferber and extended agent concepts forged at the Naval Postgraduate School's MOVES Institute by John Hiles.

Implementations of Hiles' ideas such as Brian Osborn's Story Engine and Kim Roddy and Mike Dickson's RELATE architecture provided a solid foundation for TNS. The authors' work modified the RELATE architecture to create a model of terrorist agents existing in the iterative and evolving story of recruiting, training, planning, preparing, and carrying out terrorist missions against targets of their design. The simulation design incorporates two models of communication, the first of which, connectors, is based on Hiles' cellular protein metaphor, for entities to connect with each other and take certain actions upon making contact. The other communication model is a broadcast e-mail-like system that allows agents to reach other agents across the network. TNS also uses the concept of tickets and frames extensively to give the agents procedural knowledge that they use in accomplishing their goals.

Most importantly, TNS validates the formation of scale-free networks as a conceptual tool for attacking terror networks. There is no high-level control structure to govern the connections in TNS. However, by implementing growth and preferential attachment in low level interactions the macro behavior of scale-free systems is self-organizing. The authors' simulation clearly shows the formation of a scale-free network topology, developed over time without any global control. Given the fact that the simulation creates a scale-free terrorist network based on human nature, the authors conclude that the model can and should be used for future experiments to refine the four theoretical tactics for Stimulus Based Discovery. Furthermore, the authors' adaptations of RELATE, the message communication system, and the authors' implementation of connectors, frames, and tickets provide an outstanding structure for building a wide variety of other network simulations.

Lastly, the authors left some areas for future work. Most importantly, the authors did not implement the four stimulus tactics in the TNS model. This work is important to refine Stimulus Based Discovery and to provide both

quantitative and qualitative analysis on network behavior under attack. Additionally, the model should be configured to import a runtime configuration that does not require recompiling the source code. This would allow a large sample of different networks that validate the scale-free topology under a wide array of input variables. Also, the ability to "grow" an organization for a period of time and then store the state variables allows experimentation on "mature" networks. For example, these mature networks would then be used in several experiments with different targeting strategies to show how the same network responded to different forms of stimulus and attack.

In conclusion, Stimulus Based Discovery converts American firepower superiority into information advantage over networks. Despite the overuse of the word *network* in discussion of "Network-Centric", "FORCEnet", "Netwar", "Navy Marine Corps Intranet", and dozens of other permutations it is the authors' observation that most of the *network* concepts discussed in the armed forces tend to focus on how our military can benefit from the power of information and networking. Rather than join this important debate, Stimulus Based Discovery begins a new thread examining how networks already exist in our current and future adversaries, and adversary networks already contain inherent vulnerabilities that can be exploited to achieve network collapse. Observant readers may have already considered the extension of this inherent vulnerability that American networks and our current fascination with building more networks unduly expose U.S. forces to Stimulus Based Discovery and hub attack. Therefore, a final potential for future work is an analysis of American networks that seeks to mitigate our exposure to similar tactics.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, James, *The Next World War*, Simon & Schuster, New York, 1998.

Arquilla, John and Ronfeldt, David, *In Athena's Camp*, p. 10, Rand 1997.

Arquilla, John and Ronfeldt, David, *Networks and Networks,* p. 1, Rand, Santa Monica, California, 2001.

Baker, Wayne E. and Faulkner, Robert R., 1993, "The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry," American Sociological Review, Volume 58, Number 6 (December), pp. 837-860

Barabási, Albert-László, Linked: The New Science of Networks, (Cambridge, MA: Perseus Publishing, 2002), p. 220.

Beeler, M. *et al*. Item 96 in Beeler, M., Gosper, R. W., and Schroeppel, R. Hakem, Cambridge, MA: MIT Artificial Intelligence Laboratory, Memo AIM-239, p. 35, February 1972.

Blitzer, Charles, *Age of Kings,* p. 42, Time Incorporated, New York, 1967.

Bowden, Mark, *Killing Pablo I,* New York, Atlantic Monthly Press, 2001.

Bush, George, "Address to a Joint Session of Congress and the American People," 20 September 2001, Accessed at [http://www.whitehouse.gov/news/releases/2001/09/print/20010920-8.html], on 23 March 2003.

Carley, Kathleen, "Inhibiting Adaptation" Unpublished Research Paper for the Advanced Adaptive Command and Control Project, Aptima Corp.

Carr, Caleb, *The Lessons of Terror*, p. 9, Random House, New York, 2002.

Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Campaign Planning*, p. I-3, January 2002.

Clark, Wesley, *Modern War.* Public Affairs, 2001.

Clausewitz, Carl Von, Translated by Paret, Peter, *On War*, p. 120, Princeton University Press, 1984.

Cohen, Eliot A., "A Revolution in Warfare", Foreign Affairs, Vol. 75, No. 2, March/April 1996.

Cordesman, Anthony and Hashim, Ahmed, *Iraq: Sanctions and Beyond,* Boulder, CO, Westview Press, 1997.

DARPA, "Defense Advanced Research Projects Agency's Information Awareness Office and Total Information Awareness Project," Accessed at [http://www.darpa.mil/iao/tiasystems.thm], on 21 March 2003.

Devore, Jay L., *Probability and Statistics*, p. 166, Duxbury Pub., Pacific Grove, California, 2000.

Douhet, Giulio, *The Command of the Air,* trans. Dino Ferrari (1942; New iImprint, Washington, D.C.: Office of the Air Force History, 1983), p. 57.

Edwards, Greg and Morrison, Mark, "Click that Clicker," *The Roanoke Times*, 4 June 1994.

Erickson, Bonnie H., "Secret Societies and Social Structure," *Social Forces*, Vol. 60, No. 1 (September), pp. 188-210.

Essay on Man, Ep. II, pp. 303-4.

Fauconnier, G. and Turner, M., *The Way We Think: Conceptual Blending and the Mind's Hidden Complexities*, Basic Books, New York, New York, 2002.

Ferber, J., *Multi-Agent System, An Introduction to Distributed Artificial Intelligence,* Addison-Wesley Publishers, 1999.

Friedman, Thomas, *The Lexus and the Olive Tree*, p. 403, Farrar Straus and Giroux, 2000.

Gallucci, Robert L., "U.S. Nonproliferation Policy: Lessens Learned from Our Experience with Iraq and North Korea," *Pulling Back From the Nuclear Brink: Reducing and Countering Nuclear Threats*, Ed Barry R. Schneider and William L. Dowdy, London, Portland, Oregon, Frank Cass, 1998.

Global Security.Org, "Operation Eldorado Canyon" Accessed at [http://www.globalsecurity.org/military/ops/el_dorado_canyon.htm], on 23 March 2003.

"Harpoon Fact Sheet, Accessed at [http://www.strikenet.js.mil/pao/Fctshtupdtes12oct/slide4.jpg], on 19 December 2002.

Hiles, J. E., "*Integrated Asymmetric Goal Organization IAGO: A Multiagent Model of Conceptual Blending,*" Unpublished White Paper, Naval Postgraduate School, Monterey, California, 2003.

Hiles, J. E. and Lewis, T., "*Project IAGO: Research into Cognitive Modeling of Terrorist Behaviors,*" Conceptual Modeling and Simulation Notes, Naval Postgraduate School, Monterey, California, 2002.

Hiles, J. E., Osborn, B. A., VanPutte, M., Lewis, T. G. and Zyda, M., "*Story Engine: Dynamic Story Production Using Software Agents that Discover Plans,*", Unpublished Technical Paper, Naval Postgraduate School, Monterey, California, 2002.

Hobbes, Thomas, *Leviathon*, p. 82, Basil Blackwell, Oxford, 1960.

Ilachinksi, A., *Irreducible Semi-Autonomous Adaptive Combat (ISAAC): An Artificial-Life Approach to Land Warfare*, Center for Naval Analysis Research Memorandum CRM 97-61.10 August, 1997, Center for Naval Analysis, Alexandria, Virginia, 1997.

Krebs, Valdis, "Uncloaking Terrorist Networks," *First Monday*, Accessed at [http://firstmonday.org/issues/issue7_4/krebs/index.html], on 20 March 2003.

Krulak, Charles, Quoted by Arthur Brill, "A Defining Moment in Marine Corps History," *Sea Power*, p. 11, November 1998.

Loeb, Vernon, Washington Post, 07 May 2001, p. A02.

Lowenthal, Mark M., *Intelligence: From Secrets to Policy*, p. 63, CQPress, Washington, 2000.

McCarthy, Rory, "Dangerous Game of State Sponsored Terror that Threatens Nuclear Conflict," *The Guardian*, 25 May 2002.

McClure, Stuart et al., *Hacking Exposed, Third Edition,* p. XX, McGraw Hill, New York, 2001.

McKenzie, Donald, *Inventing Accuracy*, MIT Press, Cambridge MA, 2000.

Myer, Josh. "U.S. Agents Race to Follow Up on Electronic Data Seized in Radi," *The Mercury News,* 03 March 2003, Accessed at [http://www.bayarea.com/mld/mercurynews/news/5303755.htm], on 21 March 2003.

Osborn, B. A., *An Agent-Based Architecture for Generating Interactive Stories*, Dissertation, The MOVES Institute, Naval Postgraduate School, Monterey, California, 2002.

Owens, Bill, *Lifting the Fog of War,* Johns Hopkins University Press, 2001.

Parker, Geoffrey, The Thirty Years War, Routledge and Kegan Paul, London, 1984.

Public Broadcasting Service, "Vietnam Online, "[http://www.pbs.org/wgbh/amex/vietnam/trenches/mylai.html].

Ritter, Scott, *Endgame,* New York, Simon & Schuster, 1999.

Roddy, K. A. and Dickson, M. R., *Modeling Human and Organizational Behavior Using a Relation-Centric Multi-Agent System Design Paradigm*, Master's Thesis, The MOVES Institute, Naval Postgraduate School, Monterey, California, 2000.

Russell, Stuart and Norvig, Peter, Artificial Intelligence: A Modern Approach, (Upper Saddle River, New Jersey: Prentice Hall, 1995), p. 139.

Ryan, Cornelius, *The Longest Day*, Simon and Schuster, New York, 1959.

Schwartz, John, "Year After 9/11, Cyberspace Door Is Still Ajar," *New York Times*, 09 September 2002.

Second Treatis, Para 94, p. 90.

Shelby, Richard C., "Excerpts from September 11 and the Imperative of Reform in the U.S. Intelligence Community," 10 December 2002, Accessed at [http://www.darpa.mil/iao/tiasystems.thm], on 21 March 2003.

Sullivan, Bob, "Is a Larger Net Attack on the Way?" MSNBC Online, 28 October, 2002, Accessed at [http://www.msnbc.com/news/827209.asp?cp1=1], on 21 March 2003.

Sun Tzu, *The Art of War,* Chapter 10.

"The Next Big Blue Thing," Newsweek, p. 83, 13 December 1999.

Treaty of Westphalia, Accessed 13 January 2002 at [http://www.tufts.edu/departments/fletcher/multi/texts/historical/westphalia.txt].

United Nations Charter, Chapter 1 Article 2.

United States, Goldwater-Nichols Department of Defense Reorganization Act of 1986, Washington, DC: GPO, 1986, Title IV, Public Law 99-433.

"United States Tomahawk Cruise Missile Program," Accessed at [http://www.strikenet.js.mil/pao/tomhis.doc], on 18 December 2002.

Waltz, Kenneth, *Theory of International Politics*, p. 6, McGraw Hill, New York, 1979.

Weigley, Russell, *The American Way of War*, p. 313, Indiana University Press. Bloomington, Indiana, 1977.

Wilde, Oscar, Quoted by Jon Winokur, *The Portable Curmudgeon*, New Books Inc., 2002.

Williams, Phil, "The Dark Side of Global Civil Society: The Role and Impact of Transnational Criminal Organizations as a Threat to International Security", *International Security Management and the United Nations,* Ed Alagappa, Muthiah and Inoguchi, Takashi, United Nations University Press, Tokay, 1999.

Wolf, John B., *Toward a European Balance of Power 1620-1715*, p. 190, Rand McNally, Chicago, Illinois, 1970.

Wooldrigde, M., *An Introduction to MultiAgent Systems*, John Wiley & Sons Ltd, West Sussex, England, 2002.

Worden, John.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Mr. John Hiles
   Research Professor
   MOVES Institute
   Naval Postgraduate School
   Monterey, California

4. Dr. Rudy Darken
   Chairman, MOVES Academic Committee
   MOVES Institute
   Naval Postgraduate School
   Monterey, California

5. Dr. Dan Moran
   Department of National Security Affairs
   Naval Postgraduate School
   Monterey, California

6. MOVES Institute Reference Library
   Attn: Dr. Michael Zyda
   Chairman, MOVES Institute
   Naval Postgraduate School
   Monterey, California

7. Dr. Arnold Buss
   MOVES Institute
   Naval Postgraduate School
   Monterey, California

8. Dr. Jon Czarnecki
   Naval War College, Monterey Program
   Naval Postgraduate School
   Monterey, California

9. Gordon Nakagawa
Department of Operations Research
Naval Postgraduate School
Monterey, California