Deterrence 2.0:
Deterring Violent Non-State Actors in Cyberspace

Workshop held
9-10 January 2008
in Arlington, VA

Prepared for
US Strategic Command Global Innovation and Strategy Center
(USSTRATCOM/GISC)

Prepared by
Strategic Multi-Layer Analysis Team
Edited by Carl Hunt
chunt@ida.org
and **Nancy Chesser**
Nancy.Chesser@js.pentagon.mil

UNCLASSIFIED

TABLE OF CONTENTS

Foreword

By James Fallows, Atlantic Monthly Magazine[1]

The simplest point to make about the essays that follow is the most important: they are worth reading.

The papers collected here offer a wide variety of perspectives, from different professional backgrounds, disciplines, and points of view. They complement each other – agreeing on some points, usefully disagreeing on others. They combine history, theory, sociology, and well-informed technical discussion – plus in some cases pure and lively opinion. Together they do a good job of answering the question originally posed: about the effects of new technology and new dispersions of destructive power on the theory and practice of deterrence.

I could end my comments there and simply say, Read on. But let me make one other point about the value of the exercise that led to this volume. (For the record, I took no part in the conference that led to these papers and am reacting, on a volunteer basis, to what I have read here.)

The details of conflict and combat are always changing: new adversaries, new technologies, new spheres of contention, new vulnerabilities, new avenues of defense and attack. But the fundamentals of conflict and combat are always the same. They involve recognizing and responding to the changed reality faster than an adversary can; using the new opportunities for attack and response; creating the bonds of trust, understanding, and shared values that let one's own forces and allies cooperate spontaneously, while eroding those bonds on the other side.

At any given moment, strategic advantage will go to the side that best understands how the possibilities of the moment match the longer-term interests it wants to defend – that is, the side that can best match what is changing to what is constant. The conference that led to these papers should be understood as an attempt to work out that match.

A number the papers emphasize what of today's new tools of communication have changed from the last time we defined deterrence—the Cold War. There are new means of recruitment, of propaganda and motivation, of exploiting vulnerabilities, yet also of providing resilience. But while the technology and business worlds have often assumed that "everything" has changed because of computers, Moore's Law, and the Internet, and that we are in a one-way shift from past to future, many of the papers here emphasize what has not changed.

The process of deterrence is different from what it was during the Cold War, but some of its underlying principles still apply. Idealism, openness, and other elements of "soft power" have always been part of America's strategy for undermining adversaries and preventing attacks. They remain part of that strategy – and have taken on new importance and must be exercised through new technological means. Resilience, in the sense of preparing to rebound from attacks

[1] Editors Note: The Foreword to this report was provided by Mr. James Fallows, National Correspondent for The Atlantic Monthly Magazine. Mr. Fallows was unable to attend the workshop and provided this Foreword based on a review of the report and personal interaction with some of the writers. He was not compensated for this work in any way.

that cannot be deterred, is also a long-standing part of national doctrine. (The Internet itself, after all, grew out of an effort to design a network that could withstand even nuclear attack.) But as some authors emphasize, resilience may be relatively more important now, when the nation cannot assume that it will be able to deter or prevent every conceivable terrorist attack.

For several years after the 9/11 attacks, many press and political commentators spoke as if the new diffusion of destructive power around the world, and the communications technologies that had been part of that diffusion, had placed the United States in a permanently more vulnerable and even fearful mode. The papers in this volume show that there is serious reason for concern, re-thinking, and vigorous new strategies – but not for defeatism or fear.

Dateline: March, 2008
James Fallows
Beijing, PRC

Preface

By Captain Todd Veazie USN

The chapters before you were born from the examination of two fundamental questions regarding the nature and theory of deterrence in the 21st century. First we had to consider what had changed since our victory in the Cold War (the experience from which most of our current doctrine is derived); and, armed with that understanding, consider how the United States might execute deterrence strategy in this new era. Our study revealed elemental shifts in the state of play that required more than "tweaking" on the margins of our thinking. Our observations compelled us to challenge the epistemological underpinnings of traditional nation-state deterrence models. What can be held at risk as we seek to deter the violent metastasis of ideas propagated over the Internet? How can we prevail in a global marketplace of ideas without compromising our own sacred values? The enclosed pages contain comments, insights and recommendations that transcend any thinking about deterrence that has ever gone before those of us in uniform. As evidenced by the sage words of James Fallows in the Foreword to this report, the ideas contained within are "worth reading." The Deterrence of Violent Non-State Actor Workshop during the period of 9-10 January 2008 was a special event that was both compelling and timely.

So what has changed? Of course, the answer is rather obvious yet curiously underrepresented in the recent deterrence scholarship. Humanity is undergoing a transformation from the Industrial Age characterized by machinery, factories, urbanization and measured change where resources, production and optimization were the source of wealth and power, to an Information Age, defined by knowledge and networks, interconnectedness, globalization, adaptability, agility, innovation and rapid change. New rules sets are emerging that cannot be predicted and with them come opportunities, creativity and societal dislocations that often breed violence and instability.

Like Damocles' sword, this global interconnectivity both strengthens us and moderates us at the same time. We are strengthened because we are better connected to others than ever before and thus capable of spreading the seeds of liberty and opportunity to populations that yearn for it and where the lack of it is still being justified. We are moderated by this interconnectivity because others can more easily exploit the seams and turn our freedoms against us to infect with vitriolic propaganda that violently radicalizes populations across this interconnected web.

It is the matter of moderation of our strength that brought together the remarkable group of thinkers whose words are reflected within this report. We are concerned here with the problem of deterring violent non-state actors from doing harm to our nation and to our allies. The questions of extending freedom through access while mitigating the misuse of that freedom to harm us were the dominant questions we took up in this workshop. This report captures the intellectual power and dynamic interactions that took place during these two days and must be read by today's and tomorrow's decision-makers. These thoughts will inform the planning and execution of deterrence principles for years to come.

During the workshop, our intrepid editor and valued contributor coined the phrase *Deterrence 2.0* to reflect upon the way science of interconnectivity is changing our world. I believe this connotation was right on the money. The world has changed around us through globalization and the interconnected collectives we have empowered through our nation's greatness in innovation and economic prosperity. Not only must we foster this empowerment, but we must also protect it. The thoughts captured within this report demonstrate this need and offer ideas about how to do it.

The world has changed and both the process and effects of deterrence are changing. This report is a magnificent beginning to a necessary discourse about Deterrence 2.0 and even Diplomacy 2.0. This conversation must include all of the United States and its Allies. I am delighted to forward this report to you, the reader. May we understand and learn to exploit the insights and recommendations of the authors as we better understand the principles of deterring violent non-state actors in cyberspace. This report initiates that conversation.

Executive Summary

by Carl W. Hunt, Institute for Defense Analyses

This report captures the essence of a two-day workshop on Deterring Violent Non-State Actors in Cyberspace, held on 9-10 January in Arlington, VA. The workshop was undertaken in response to a request from USAF Lt Gen Robert Elder to address deterrence of violent non-state actors (VNSA) in cyberspace, as a follow-on to the recently completed Strategic Deterrence Strategic Multilayer Assessment (SMA) report.[2] Participants in this workshop ranged from active military to civilian, including contractors and academics with backgrounds in physics, political science, social science (including anthropology) and technology fields. The purpose of the workshop was to engage experts in a strategic multilayer assessment of deterrence options in the 21st century that recognized an interconnected global threat environment for dealing with VNSA.

It was a remarkable two days of spirited interaction among the participants, enhanced by a topic that was timely and challenging. The insights and conclusions put forth by the participants, while hardly unanimous in detail, were not divergent either. As the remainder of this report shows, the United States faces a much more level global playing field as it seeks to shape deterrence options today than it did in the Cold War and before. Deterrence 2.0, as it became known in the workshop, is not always about holding at risk what the adversary values, particularly when these values might be manifested in far less tangible media than nation-states, their populations and their societies.

The participants, particularly the non-military practitioners, advised that the US consider traditional deterrence only as a baseline from which planners and policy-makers diverge to build adaptive (and more cooperative) forms of relationships with potential adversaries. While Cold War deterrence is still viable, the participants concluded, it will likely be less effective in the Cyber Age. Resiliency of US Infrastructure will be of great importance however, a hold-over from the Cold War forms of deterrence—forcing an adversary to conclude that there is no meaningful return on investment in attacking the US still works.

This report contains both a breadth and a depth of insights about the Cyber Age and what this country will face as it seeks new forms of deterrence policy and ways to implement the DIME power construct. We encourage the reader to take advantage of this report and study the insights of political scientists, economists, social scientists and even natural philosophers to better understand how the future of the Cyber Age may unfold and how the US will likely fit into this new Age. Deterrence 2.0 joins Web 2.0, Science 2.0 and other new forms of connected discourse for raising the curtain on the next stages of human history. This report gives a front-row seat for the stage the US will occupy.

[2] See Chesser (2007) for a detailed description of the strategic multilayer assessment (SMA) program, and for background on the initial Strategic Deterrence report done as an SMA project.

1 Promoting and Protecting US Interests in the Cyber World: Violent (and non-Violent) Non-state Actors - Workshop Summary

by Carl W. Hunt, Institute for Defense Analyses

The World of Deterrence 2.0

Like *Web 2.0* and *Science 2.0*, "Deterrence 2.0," or deterrence in the Cyber Age, is as much an emerging phenomenon as it is a sought-after method for dealing with both state and non-state actors in an increasingly interconnected world.[3] All three next generation environments suggest worlds of interaction and dynamism that have never before been possible. Near-infinite interactions taking place over near-infinite connections leave those who seek to practice the deterrence of the Cold War world in a true quandary.

This new world of deterrence poised over globally interactive interconnectedness was the primary challenge faced by a remarkable group of experts from a variety of disciplines during a two-day workshop, held in Arlington, VA, 9-10 January 2008. The following report attempts to capture and synthesize the analyses and findings from the workshop. Their thoughts are synergized along with the thoughts of specially invited authors with varying backgrounds who contributed to both divergent but cogent perspectives.

The participants' initial conclusions, while not unanimous, were often piquant but rooted in common sense and grounded in the new disciplines of network and connection theory. In short, their insights were ultimately sensible and intuitive for those who have grown up within the networked world.[4] These insights should encourage and empower the United States "to combine the tools of intimidation with the tools of inspiration," as former Deputy Secretary of Defense John Hamre once put it. (Gates, 2008)

Workshop Overview

This two-day workshop, undertaken in response to a request from USAF Lt Gen Robert Elder, addressed deterrence of violent non-state actors (VNSA) in cyberspace. Participants ranged from active military to civilian, including contractors and academics with backgrounds in physics, political science, social science (including anthropology) and technology fields. The purpose of the workshop was to engage experts in a strategic multilayer assessment[5] of

[3] The connotations of Web 2.0 and Science 2.0 follow the popular press ideas about the imminent next generations of interconnected and collaborative World Wide Webs and "networked Science" (as science author Mitch Waldrop labels it). The idea behind a concept of "Deterrence 2.0," explained in detail throughout the report, also suggests that interaction, interconnectedness and collaboration may also apply to national policy concepts previously thought of as coercive, one-way, bilateral relationships. Such thinking may no longer be possible in the cyber world.

[4] In fact, several of the participants felt that the Workshop should have also had a contingent of 15-19 year olds who have been practicing virtual deterrence (and collaboration) techniques in online games for much of their young adult lives!

[5] See Chesser (2007) for a detailed description of the strategic multilayer assessment (SMA) program, and for background on the initial Strategic Deterrence report done as an SMA project.

deterrence options in the 21st century that recognized an interconnected global threat environment for dealing with VNSA.

After an initial deliberation about the main purpose of the workshop, the attendees began to debate their diverse positions on the two main questions of the workshop:

1) Is the US seeking to deter violent non-state actors from using the cyber world to recruit and plan attacks against the US and allies (including the ability to counter VNSA through offensive means)? Such an effort would seek to inhibit the formation of what Sageman calls a "Leaderless Jihad," (2008) or…

2) Is the US at least as interested in maintaining a maximally open cyber environment and using freedom of access as a novel form of deterrence-producing capability (perhaps an equally relevant way to counter the "Leaderless Jihad")?

While both thrusts may in the end be complementary, the answers to those questions shape the cyber environment as a deterrence medium, as they in fact shaped the debate throughout the workshop. Each approach requires a different starting point, and thus different strategies and resources, but potentially converges in ways only the cyber world can accommodate. As contributor James Fallows commented, "Any discussion of state- or non-state deterrence that doesn't dwell on the potential of eliminating threats through co-opting them, or winning supporters, is missing a huge opportunity" (Fallows, 2008). Mr. Fallows also wrote the Foreword to this report.

Essential Participant Findings

In considering the two main questions initially generated by the attendees, the workshop discussions centered around four closely linked findings:

1) Deterrence of VNSA in the cyber context involves a broad range of actions, including dissuasion, exerting influence, co-opting, and establishing positive relations. Deterrence can be both direct and indirect. Indirect, such as exerting influence, is a viable means of more effective deterrence in the cyber age; leveraging connectivity in ways never before considered empowers dynamic flows of information and virtual relationship-building. Sustainability, also an essential characteristic of deterrence, means that deterrence efforts may have lasting effects but yet require constant monitoring and adaptation. The networked world enhances these opportunities, often in what have been considered undirected, auto-catalytic ways.

2) If someone is violently bent or fundamentally fixated, they may not be deterrable. However, exerting influence, especially indirectly on their support population or the populations to which they appeal, may still be possible. Fault lines exist on the radical side that a new generation of "network warriors" can explore and exploit. As an example, "embourgeoisement" of the Middle East, as workshop attendee Mike Vlahos labeled it, is an important development; the middle class traditionally seeks stability. Instead of solely focusing on deterring enemies in conventional cold-way methodologies, more enlightened approaches might look for allies among prominent academics, NGOs, media personalities, and cultural/tribal brokers (those that typically compose the middle class of any nation).

Understanding the history, culture and perspectives of a potential ally or adversary takes time, but it makes influence feasible.

Network-savvy warriors and statesmen must also leverage and assist existing aid organizations. Providing NGOs with a communications infrastructure to better facilitate their efforts empowers them to be more connected to the people the US and our allies seek to influence (even through the most coercive forms of deterrence, when required). The promotion of an open cyber-based world is in fact a very meaningful deterrence strategy, according to several of the workshop members. While this may have originally seemed counter-intuitive to a large degree, free flow of information of all types helps people from diverse parts of the world discover for themselves the fruits of open and free exchange of knowledge. They must personally experience the freedom unrestricted flows of information provide to their families and societies and thus inculcate this process into their own way of life in ways that make the most sense for them. The US and West cannot force this discovery process, but can encourage and protect the ways in which it might happen.

3) The existing and emerging cyber-based world has created profound changes in communicating ideas and information. Wireless technology is being brought into remote areas, enabling telephone and Internet access, speeding up formation of relatively dispersed communities, and allowing airing of new ideas. In many parts of the world, this is happening even faster than it did in the West. Workshop attendee Thomas Barnett pointed out several times the impact of highly accelerated information within an increasingly interconnected world and the consequences that has for the emergence of new business, government and personal lifestyles. The interconnected life brought on by the Internet and World Wide Web makes it easier to create content, and to have that content accepted by a significant part of their community. Perhaps one of the most meaningful forms of deterrence at the US's disposal is to foster the growth and security of access to the interconnected world that Web 2.0 promises, a substantiation of point 2, above. In fact, another workshop participant, Tim Wu, Columbia Law School, discussed the US's obligations to maintain a "balanced approach" to cyber-based deterrence, similar to the US policy of "encouraging an open media and free press around the world." Dr. Wu summed up his thoughts as follows: "…it will be difficult for the United States to simultaneously criticize the Chinese regime's restrictive Internet practices if we begin to adopt many of them, even if the ends pursued are much different." These thoughts considered the role of China but could extend to any other entity, he said.

4) Finally, the roots of conventional, "Cold War" deterrence still apply. Several of the workshop attendees spoke about significantly hardening a manageable part of US infrastructure in ways that simply make it too costly for an adversary to attack. Resiliency is at the heart of this strategy (Barnett, Sub-Chapter 2.A, this report). If the US is able to recover more quickly than the adversary can mount the next attack or follow up from an initial success, the traditional notions of deterrence are likely to be most successful. In other words, the US, through its globally admired resiliency, obscures itself as a target simply because it makes no sense to obligate resources to attack if those resources offer such poor return on investment. The US must maintain its strength in the area of critical infrastructure and economic underpinnings and reduce the adversary's value proposition such that it costs too much for an adversary to attack. In this sense, the old forms of deterrence calculus,

assured return destruction (or equally effective, poor return on investment), probably still apply.

Preview of Subsequent Chapters and Authors' Contributions

Chapter 2, authored by Dr. Larry Kuznar, National Security Innovations, and Dr. Carl Hunt, Institute for Defense Analyses, examines the virtual global perspective of "Life in the Interconnected World." This chapter reviews some of the initial findings of the Strategic Deterrence SMA of 2007, and points towards the development of a meaningful typology that will inform all future efforts dedicated to better understanding of the threats the US will face in the coming years of the Cyber Age. It also attempts to explain globalization as it applies to the new forms of threats and opportunities the United States faces in the next few years and beyond.

Chapter 2 also manifests as sub-chapters original insights from three outstanding thinkers: Dr. Thomas P. M. Barnett, Enterra Solutions; Dr. Robert Axtell, George Mason University's Center for Social Complexity; and Mr. Ken Steinberg, Savant Protection. Dr. Barnett, a political scientist, provided several pages of interesting insights about resiliency and the role the US must play in the future of trade and connectivity; he concludes that the US must be humble in its approach to deterrence in the Cyber Age. Dr. Axtell, an economist and social science modeler, contributed to the workshop with unique insights on the responsibility of the country to shape the impact of deterrence in more modern and meaningful ways such that the entire world benefits, if possible. Finally, Mr. Steinberg offered a technical though accessible forecast of "Cyberism" and Innovation in the 21st Century, commenting on the role that technological innovation will have in deterring violent behavior in the Cyber Age.

Chapter 3, authored by Dr Allison Astorino-Courtois, National Security Innovations, and Matthew Borda, Creighton University, compares and contrasts deterrence at the conceptual level over the last century or so. This chapter goes to some length in defining deterrence terms and concepts that apply to both ages (the Cold War and the Cyber Age), but leans towards refining the concept of deterrence as it applies to the modern warrior. The chapter challenges traditional notions such as "rational actors" and seeks to define various types of conceptual "space" relative to the Cyber Age. The chapter seeks to clarify these terms and concepts in light of global connectivity and Deterrence 2.0.

Chapter 4, authored by Dr. Susan Numrich, Institute for Defense Analyses, looks at the apparent transcendent movement between the "real" and the cyber world. This chapter reveals significant insights on the consequences of global interconnectivity from a behavioral standpoint and the role that traditional and new forms of media have played in shaping these behaviors. Understanding the role of social networks is important, but this chapter explains how these networks form and how they influence new forms of organization and action. Chapter 4 explores and exposes the nexus between the world we thought we lived in and the cyber world that increasingly manifests the universe that actually transpires.

Chapter 5, authored by Dr. Robert Popp, National Security Innovations and several colleagues, offers a detailed and sometimes technical perspective of the social science modeling tools that hold promise for better understanding and predicting VNSA behavior – this chapter is the longest and most technical component of this report. Chapter 5 also examines at a top level the impact

of some 500 million web pages from what is known as the Dark Web, an area of the World Wide Web in which extremist/terrorist data is often posted and consumed. The authors conclude that there is very little difference in the level of sophistication of use of the Web when comparing the US and West and potential terrorist usages of the Web – it appears that the playing field is quite level. This chapter also reviews major features that social science tools offer for both comprehension of past and present events and the potential for predicting behaviors that might allow the US to "get left of boom." When understood in the context of the insights of writers such as Fallows, Barnett and Axtell, this final chapter offers new opportunities to understand the right mix of traditional deterrence and Deterrence 2.0 techniques that might better operationalize the sources of national power of the US and its allies, the world of the "CyberDIME."

References cited in all of these chapters are aggregated at the end of the report. A list of acronyms used is also provided.

The Challenge of Moving Ahead

Workshop participants raised a number of unresolved issues affecting future efforts in this area at the conclusion of the workshop, as well as in exchanges in the days following. Most of the key discussion questions and points raised during the workshop consisted of some form of the following five points. These questions and issues form the nucleus for the remainder of the report. Questions and Issues included:

1) How is the Internet used by all (US/Allied, Adversary, Others)? How do we influence (counter when necessary) adversary use of the Internet?

2) Given the variety and complexity of new threats, there is a lack of guidance as to what we must deter. More guidance regarding deterrence objectives is required from policy makers in the US Government if effective deterrence concepts and courses of action (COAs) are to be developed.

3) How do we practice deterrence in this new, interconnected world so that it remains a useful concept even if demonstrably different from Cold War deterrence?

4) What other concepts, in addition to deterrence, do we synergize to ensure that the US can sustain maximum global access to the Internet?

5) The process of globalization and development of the cyber domain are both complex and emergent. It is likely that anyone or any state that attempts to control or even to shape the interconnected domain globally will be frustrated.

Initial Conclusions:

This summary recaps two days of highly interactive dialogue and many pages of written material offered by the workshop participants (included where appropriate). Many of these comments and writings shape the following report and offer novel ideas about deterrence of non-state actors in the cyber age, as well as validating conventional notions about deterrence in any age.

Deterrence 2.0 is likely not something the US does by itself – globalization as part of the cyber age seems to change much of the unilateralism and bilateralism of the past. Deterrence 2.0 may not even be recognizable by practitioners of conventional deterrence and may be difficult to implement (or worse, to recognize when our adversaries use these techniques against the US or its allies). These new components of the Deterrence 2.0 arsenal are still worthy of consideration nonetheless.

The strongest recommendation of many of the Workshop panelists is to consider deterrence from at least an evolutionary standpoint where new political, cultural and societal landscape features have recently surfaced that may be more relevant (and noticeable) than they would have been in the past. Barnett's caution seems prudent that the US proceed humbly in crafting and executing new forms of deterrence policy and capability. Only in this way might the US "combine the tools of intimidation with the tools of inspiration," as former Deputy Secretary of Defense Hamre is quoted in Secretary Gates' speech.

The Strategic Multilayer Assessment team gratefully acknowledges the contributions of all of the workshop participants – their names are listed throughout this report. The challenge of shaping deterrence or any strategic DIME tool for use in the Cyber Age will continue to be subject to the same interactions described in this report. Such is the dilemma of deterrence of non-state actors in the dynamic, interconnected world that arrays itself before the United States. Welcome to the world of Deterrence 2.0!

2 Life in the Interconnected World: Globalizing Effects of the Cyber Domain and a Typology to Accommodate the Effects

by Lawrence A. Kuznar, National Security Innovations and Carl Hunt, Institute for Defense Analyses

This chapter provides an overview of globalization and its interlocking role with cyber technology. It also extends from the original SMA Strategic Deterrence report the important discussion of a much needed typology that accommodates globalized behavior in the cyber domain (Chesser, 2007). This chapter is based on discussions as part of the SMA workshop as well as other research on globalization and the emergence of a cyber domain.

The chapter begins with a brief characterization of the cyber domain. We then discuss the relevance of complexity and complex systems theory to these phenomena. Next, we address the challenges of deterrence in complex, globalizing cyber environments and consider thoughts proffered by Workshop attendees. The spread of the Internet and World Wide Web in the Arab world is reviewed as an example. Finally, we consider the beginnings of a taxonomy that enables us to understand VNSAs in a globally interconnected environment.

Key points include:

- Globalization is a historic process that will continue to connect all the world's people
- Traditional forms of deterrence may inform US interactions with other states and non-state actors, but these forms of deterrence will no longer be a dominant method for interacting with others
- The cyber domain includes a broad range of technologies that are spreading very rapidly, giving people unprecedented networking and communication abilities
- Globalization and the cyber domain are interconnected, dynamic, changing and genuinely complex
- Deterrence options in the 21st century require a broad range of approaches, including strategic communication and other forms of "upstream" activities for shaping the operational environment
- Complexity obviates control of the emerging cyber domain
- Deterrence activities should be aimed at monitoring and deflecting threats through indirect means
- Deterrence capabilities must be adaptive and flexible, since new and unforeseen threats are certain to emerge
- Third party and surrogate forms of deterrence may be more appropriate and effective, particularly in dealing with non-state actors
- Practitioners require clearer guidance from policy makers concerning what threats require attention

The Cyber Domain

The cyber domain includes much more than the Internet or the World Wide Web. It also encompasses satellite communications, audio and video broadcast, cellular communications, and

other new technologies people increasingly use to communicate. The US Air Force even considers certain weapons such as Directed Energy weapons to be part of the cyber domain. These technologies, particularly the high-speed interconnecting technologies, are not only new, but they are proliferating rapidly, spreading throughout the world even to replace more traditional means of communication (such as land-line telephones that are becoming less relevant in a wirelessly connected world). These new technologies provide people with unprecedented capabilities for social networking and communication. The growth in these new technologies has been mathematically exponential and is continually increasing, as any review of the history of the Internet demonstrates.

The initial Global Deterrence SMA and final report began to consider the consequences of massive interconnection, particularly as it applied to the sources of national power: the DIME.[6] To provide for an enhanced understanding of national power amplified (and diminished) in the cyber age, the authors of the Strategic Deterrence SMA report (Chesser, 2007) proposed a concept called the CyberDIME. The CyberDIME considered the sources of national power through the lens of a globally interconnected system of people, culture and commerce. The CyberDIME and the related discussions of DIME actions as part of deterrence was one of the first and most cohesive reports on deterrence in the cyber domain. This report ultimately informed the development of the Deterrence 2.0 workshop and discussions upon which this current report is based.

Globalization

Globalization is a complex process by which the world's people are increasingly connected to one another through economic transactions, communications and media. This process has many ramifications, including the rapid spread of ideas and technologies, challenges to traditional and local ways of life, and shifts in political power. Some of the more obvious effects of globalization have included the rise of service (as opposed to manufacturing) industries in the West, the growth of multi-national corporations, the exportation of manufacturing to Third world countries, the spread of Western culture to all reaches of the globe, and the exposure of the world's peoples to many different cultures and ways of life. These shifts from the atomic world to the digital world, as many contemporary authors claim, are all empowered by an interconnected globe, linking small groups and individuals to large international businesses and governments to enhance commerce and communications (Anderson 2003a).

Workshop panelist Thomas P.M. Barnett suggested one stage-setter for this report in his sub-chapter addendum to this chapter: *Because of the rising complexity of SOA[7]-enabled global business platforms that bind our economy with those of states featuring less robust legal and security rule sets, we are necessarily made more vulnerable to the nefarious ambitions of violent non-state actors.* Barnett's characterization of global business processes as SOA (Service

[6] The DIME is an acronym for Diplomacy, Information, Military and Economic forms of national power. This has been lately augmented by a new model known as DIMEFIL, in which Financial, Intelligence and Law Enforcement forms of power are also now considered. See Chesser, 2007 for further discussion.
[7] SOA: Service Oriented Architectures, as currently being deployed in the DoD Global Information Grid by the Defense Information Systems Agency.

Oriented Architectures) was an interesting way to define the nature of the increasingly strong interrelationships forming among state, non-state and even individual actors.[8]

Barnett also cautioned against placing too much emphasis on non-state actor roles in disrupting US-global relationships, a caution not universally accepted among all participants. *As such, to the extent that violent non-state actors succeed in their efforts, they provide a clarifying function that focuses public and private sector attention to existing vulnerabilities. However, if we unreasonably elevate the importance of such violent non-state actors, we're likely to damage our own capacity for day-to-day resilience rather than expand it—the iatrogenic effect.* The notion of a clarifying function, post-VNSA "success" prompted a good deal of discussion on the importance of preparation and preemption versus resilience to attack, and how global institutions were important in absorbing the effects of VNSA attacks.

The Challenges of VNSA and Cyberspace: Complexity

Complex systems are systems with many parts that interact in nonlinear ways to produce higher order phenomena that have properties of their own. Complex systems often exhibit bottom-up unintended development, which may be created by the interactions of their many constituent elements. These systems exhibit emergence, an often unexpected generation of higher-order phenomena in which the whole is greater than the sum of its parts (Holland 1998:225). Interactions are often nonlinear, which means that a given input can have disproportionate effects on the system's behavior depending on feedbacks that amplify or decrease the input's influence (Epstein and Axtell 1996:154).

Globalization as Complex

Globalization takes place on so many fronts and in so many ways and involves so many people that understanding its causes and tracking its directions has proven challenging. It is best, as Robert Axtell noted in this workshop, to regard it as a genuinely complex phenomenon that will defy traditional methods of analysis and prediction.

Cyber Domain as Complex

The growth of the Cyber domain in the context of globalization likewise has been rapid, unpredictable and emergent, giving new cyber technologies an awe-inspiring if not frightening quality. Recursive processes (e.g. population growth rates under carrying capacity) can cross thresholds over which they fluctuate wildly (Gleick 1987). Traditional communication was face-to-face (typically, one-to-one). In the past century, broadcast (one-to-many) developed. Cyber

[8] In terms of defining deterrence of VNSA in cyberspace, Barnett offered the following: *My definition of deterrence in the 21st century has little to do with moving as far to the left of "boom" as possible. As globalization reformats traditional societies, the root causes of violent non-state actors will be exacerbated in the short and medium run but ultimately mitigated over the long haul by the extension of rule sets accompanying those expanding networks. Confusing friction (the social anger caused by the reformatting process) with the force (globalization's penetration of traditional societies) is deeply unhelpful, because conflating the two dynamics muddies causality: the more successful globalization is, the sharper the local resistance to its advance.* Barnett makes a case for looking at the current world of threats offered by VNSA as "frontier integration," a time we must live through as the Internet and globalization manifest their collective role in shaping history. See Barnett's sub-chapter which follows.

technologies allow for massive many-to-many forms of communications that occur near instantaneously across the globe. It is likely that some of the complexities of the emergent cyber domain are due to these new capacities. A recurrent theme in the workshop was that unpredictability in the cyber domain is neither bad nor mystical. It is a process that is ongoing and that can potentially be understood.

Complexity theory as a branch of mathematics provides the means for analyzing and understanding the cyber domain. The elements of complex systems can be understood through engineering analysis of its infrastructure and social analysis of people's behavior with cyber technology; these observable elements can be modeled in agent-based simulations to gain insight into how and why cyber technologies spread and what their likely effects on other social phenomena may be. Simple explanations and clear predictions about the cyber domain will not likely be forthcoming, but understanding the range of possible effects is. Another issue identified in the course of the workshop is that the cyber domain is both a manifestation of globalization (it would not be possible without globalization) and a facilitator (cyber connectedness clearly contributed to the globalization process). The cyber domain provides a self-reinforcing feedback loop that amplifies interconnectivity.

Deterrence in a Complex Environment

The complexity of the cyber domain presents several challenges to deterrence, including identifying threats, the scope of deterrence and feasible effects.

The cyber domain is vast and multi-faceted. Consequently, potential threats one may wish to deter are many and to some extent unknown. This presents an unprecedented challenge to deterrence, especially when contrasted with Cold War objectives of deterring Soviet nuclear aggression. The next section, on possible cyber-based typologies, coupled with Chapters 3 and 5, outline the range of potential threats. These threats can be divided into two categories: threats in and to the cyber domain, and use of the cyber domain in a threatening manner.

Consequently, deterrence objectives can range from deterring certain uses of the cyber domain (e.g. for recruiting, passing information, attacking the cyber domain) to deterring attacks outside of the cyber domain, which may involve use of the cyber domain (surveillance, strategic communication, etc.). An important theme that emerged from the workshop was the need for policy makers to provide better guidance to operators in terms of what activities require deterrence. The knowledge of academic and government experts is vast and the talents of operators are formidable, but they require focus on the behaviors the USG wishes to deter.

Deterrence in the cold war was not only focused on a particular threat (nuclear war) from a particular enemy (the Soviet Union), but it was also based on a decision calculus that involved identifying what an adversary valued and holding it at risk so that an adversary would find greater value in avoiding actions we wished to deter (Zagare 2004). Given the range of adversaries and their differences in strategic calculus, such a straightforward approach to deterrence is no longer feasible (Bodnar 2003).

Deterrence now appears to lie on a continuum from traditional threats on an adversary's values to influence operations aimed at denying adversaries support to shaping the battlespace so that

potential adversaries do not become threatening (Chesser 2007; USSTRATCOM 2006). This follows the idea of a Deterrence 2.0 presented in the opening summary of the report. Not only does such a range of possible activities present challenges for operations, but organizational coordination across military specialties (deterrence, information operations, PSYOPS, civil affairs) and agencies (DoD, Dept. State, others) will be necessary.

However, if the desire is to avoid reactive responses to crises, then it will be necessary to work proactively upstream of problems before they materialize. The concept of deterrence will have to be broadened and new working relationships will have to be forged to accomplish these new missions. We see this as consistent with former doctrinal approaches to preparing the battle-space (Joint Chiefs of Staff 2000) and newer concepts of preparing the operational environment (for example, Joint Intelligence Preparation of the Operational Environment, JIPOE).

Given that the cyber domain is a complex phenomenon in the context of a complex globalization process, and given that potential threats are ill-defined and to some degree unanticipated, it is fair to ask, "What feasible deterrence effects can one expect?" Globalization as a process and the spread of the cyber domain are complex, bottom-up processes. Therefore, they are probably largely out of any direct control (see Sub-Chapter 2B, by Robert Axtell). In fact, Axtell noted that VNSA as they are currently defined in this study "represent simply the latest stage in the development of a long line of technologically-enabled combatants with interests opposed to the system of states in which the actors find themselves."[9]

Axtell also noted that "as global-reach of low-cost production brings high performance computing and fast Internet connections to great numbers of households around the world there is increasing confrontation of globalization's urgencies with traditional cultural systems." Such a clash aggravates both complexity and the likelihood of continued use of the Internet by VNSA to further their causes.

However, to the extent that their complexity is realized and appropriate analyses are employed, more effective means of dealing with specific problems can be designed. A useful analogy would be trans-oceanic sailing – success is defined not by controlling the ocean but by its successful navigation. We anticipate that successful deterrence in the cyber domain will involve strategic communication focused on specific, timely issues designed to influence audiences and potential adversaries; all of these elements, the issues, audiences and actors are likely to change. As such, deterrence in the cyber domain will have to be sustainable (maintained through time) and adaptive (ready to change focus to address a new threat and prepared to employ new methods).

It is even possible that the US will expand the Deterrence 2.0 continuum to include building out and protecting cyberspace as part of its goal of staying "to the left of boom!" The United States is uniquely qualified in history to accomplish such an effect. Contributor James Fallows recounted from interviews of French, German, British and Danish officials in recent years when he asked them why America had less to worry about the dangers of home-grown terrorism.

[9] Axtell further notes that the "cyber-domain and global economic integration lead to status disparities, and knowledge of such disparities, and this fuels anti-global movements." This potentially fuels the fight of both disruptive forces and the use of the Internet and globalization to further the causes of VNSA.

"America has absorbed most of its Muslim immigrants. It had been open to them. It had assimilated them. They didn't feel estranged from American opportunity and the whole of the American idea. We could not possibly pay enough to provide the deterrence that the openness of our society does." (Fallows, 2008)

Despite the multiplicity of threats, expansion of the deterrence concept and varieties of effects, workshop panelists and participants did focus on several issues and guidelines for cyber deterrence in the 21st Century.

Guidelines

Panelists discussed several substantive issues likely to be timely and useful for informing current cyber deterrence. These issues concern the transference of traditional communication to the cyber world, the juxtaposition of local and global issues, constraints on individual information processing, and future forces and untapped resources for cyber deterrence.

Panelists noted that in many ways, people use cyber technology to continue and even extend traditional means of communication; this is apparent as families use email and singles use online dating services to conduct the age-old business of respectively taking care of family and finding mates. Related to this continuity with traditional life is the fact that themes in cyberspace often are decidedly local – people discuss personal and political issues of the day that concern them in their corner of the world. For this reason, demography (e.g., young males with frustrated ambitions often flock to the Web to find direction and like-minded friends) and economics continue to be root drivers of Internet use and themes (Atran 2006; Conway 2007; Gruen 2007). However, the anonymity and globalism of the cyber domain also provides unprecedented contact with people from around the world. This has led to the proliferation of universalist themes, such as global jihad or White supremacy, on the Internet (or even globalization in a more positive vein).

With so much information available in the cyber domain, issues of bounded rationality are more relevant than ever in analyzing how information is perceived and processed by users. Given the constraints on cognition, people will be forced to filter much information and decide and act upon only a small portion of it. Furthermore, with attention divided between traditional communication (which always goes on), cell phones, pod casts, and multiple email accounts, the time people have to deliberate on options is likewise more constrained than ever. Therefore analyses of decision making behavior in the cyber domain need to move away from traditional rational choice paradigms and their assumptions of complete information. In the highly interconnected cyber world we face, complexity almost guarantees that decisions will be made under conditions of incomplete information.

Finally, new forces are likely to play a profound role in shaping the future cyber domain, and new sources of expertise will be necessary for dealing with it. China contains a quarter of the world's population and is rapidly modernizing. Concomitant with their development is increasing integration with the cyber domain by Chinese citizens, despite Chinese governmental efforts to control access. Future interests, trends and economic developments in China and elsewhere (e.g., India) are therefore likely to have a profound influence on the future of the cyber domain.

Attendees to the workshop noted that middle-aged analysts and operators are unlikely to possess the cutting edge expertise on what is happening in the cyber domain or more important, what approaches may be useful for deterrence in this emerging world. However, our military (and even the US State and Justice Departments) already has many "Generation Y" young adults who were socialized with cyber domain savvy, and they and their civilian counterparts need to be more a part of discussions of deterrence in the cyber domain.

Example: The Cyber domain in the Arab World

The adoption of the Internet in the Muslim world has occurred in three phases: Phase 1, 1980s – Initial use by "technological adepts", which included computer engineers, technicians, students and other professionals of the Muslim Diaspora in Western societies; Phase 2, 1990s – Activists engage the Internet for debate on religious texts, both fundamentalist and moderate; and Phase 3, Late 1990s – Engagement of both official religious spokespersons and audiences through blogs, etc., (Anderson 1997a, 2003a, 2007). Conway (2007) adds to this a fourth, post-911 Phase spearheaded by radical Islamic fundamentalists.

Anderson's work is important because he identifies who the majority of Muslim users of the Internet are and what issues bring them to the net. In short, most users of the Internet are middle class professionals and students who seek the Internet for advice on being Muslim in a modern world. This includes many Muslims living in Western societies where they do not have a local Islamic community with which to interface, and what he terms the "internal diaspora" of Muslim professionals within Muslim societies who have few peers with which to interface (Anderson 2007). Anderson (2007) also stresses the complex alliances and networks that have been forged as Muslims have adopted and supported the Internet in uniquely non-Western ways. These alliances include governments (which are becoming less important), business and religious entrepreneurs, and a class of mobile elites with a global perspective.

As participants in the workshop noted, the primary users of the Internet continue to be middle-class folk with middle-class concerns that tend not to be radical, although they may be conservative. On the whole they will be receptive to messages that reinforce their conservative goals of maintaining the well-being of their lives and families in a manner consistent with the values they hold. This is an opportunity for positive strategic communications, provided that they are sensitive to the culture-specific and non-violent goals of much of the Muslim world.

This brief history of the Internet in the Arab world illustrates the complex nature of cyber domain adoption and the dynamic relations between key players. Consequently, the cyber domain in the Arab Muslim world, threats that may emerge from it, and deterrence measures will necessarily be fluid and changing.

Extending the Typology of Deterrence with Cyber Actors and Cyber Threats

Identifying who may use the cyber domain, what drives their motives, and how they go about using it requires collecting the right kind of information. This task is challenging for the cyber domain for several reasons. First, the military and intelligence communities do not typically collect information relevant to the broad range of technological, social and cultural variables related to non-state actors. Second, the complexity of the cyber domain, those that use it and

why, challenges any straightforward attempt to "get one's arms" around the problem. Third, the cyber domain has emerged so recently that there is no canon of literature that adequately defines it. As part of this and other SMA efforts, we have developed a general social typology that at least guides analysts toward asking the right questions. A few examples of the diverse approaches to understanding cyber terrorism will illustrate how multifaceted this problem is. The typology below illustrates how key variables identified by cyber terrorism researchers can be identified.

Non-state political activists have learned to use the Internet adroitly for a variety of purposes (Arquilla, et al. 1999; Lesser 1999). Conway characterizes terrorist use of the Internet in the following 4 ways (Conway 2004:276):

- Use – simple use of communication and recruitment
- Misuse – use of Internet to disrupt websites or infrastructure
- Offensive Use – use of Internet to cause damage or theft
- Cyberterrorism – actual assault on the Internet that results in violence or severe economic damage.[10]

Maura Conway and Madeleine Gruen provide analyses of Internet use by terrorist organizations (see also CTC 2006 for a catalogue of images and their meanings used by terrorist organizations). Conway (2007b) describes bin Laden's use of websites like Al-Neda and Al-Ansar to disseminate speeches by bin Laden, analyses of conflicts in Iraq and Afghanistan, Islamic scholar's commentaries, and assessments of how al Qaeda's goals would benefit the community of Muslims. She also notes al-Zarqawi's (al Qaeda Iraq) effective use of the Internet to advertise his deeds and spread fear, actually enabling him to reduce the size of his attacks and drive away foreign contractors necessary for the rebuilding of Iraq. Conway (2004; 2007b) also notes Hezbollah's use of a website associated with al Manar TV in Lebanon for propaganda and strategic communication during the Israeli invasion of 2006. Conway also provides thoughtful discussions of the challenges of regulating the Internet (Conway 2007a) and cautions against blowing the threat of cyberterrorism out of proportion (Conway 2008).

Madeleine Gruen (2004; 2006) provides detailed descriptions of how Islamist organizations (Hezbollah, Hizb ut-Tahrir) adroitly use popular music, online games and blogs to attract bored or disaffected young Muslim males. Hizb ut-Tahrir has actually subtly infiltrated blogs of hip/hop Muslim groups to shift the discussion toward radical Islamist themes. Hezbollah launched an online computer game, "Special Force," which depicts operations against Israeli troops and target practice on Ariel Sharon.

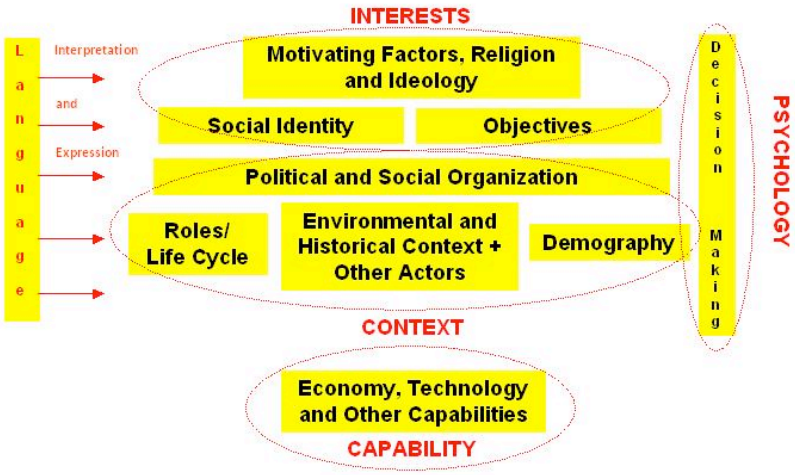
This next leads us to ask: Who is attracted to radical Internet sites? Scott Atran and Jessica Stern provide insights from their investigations of terrorist Internet use and found that disaffected and culturally disoriented young males in diaspora communities gravitated toward the Internet where they could be radicalized (Atran 2006; Atran and Stern 2005). This profile fits within the broad patterns Anderson describes.

[10] NOTES: In Chapter 3, author Allison Astorino-Courtious also discusses a different way of looking at the problem that includes classification by Actors and classification by threats.

Probably the most detailed description of terrorist recruitment and use of the Internet is from the New York Police Department study of 11 terrorist plots (Silber and Bhatt 2007). The Internet was especially important in the Toronto 18 Case (2006) and the London bombers (2005), where members variously discovered radical Salafist Jihadism, met future collaborators, and reinforced their radical views. The most vulnerable individuals were young Muslim males or recent converts who were disaffected, had experienced a life crisis and were searching for meaning in their lives. In line with other studies, young males in diaspora communities were especially vulnerable. The report concludes that the Internet can be a driver of radicalization by providing young, disaffected males with access to radical ideologies, by facilitating the meeting and networking with like-minded individuals, as a means for studying and immersing oneself in radical views, and finally as a source of information for planning attacks (Silber and Bhatt 2007: p8-9).

Svetlana Peshkova (2002) studied the role of Hib ut-Tahrir'org in Uzbekistan. Like Conway and Gruen, she provides a description of how the organization uses the Internet to spread its religious and political message. She also provides a characterization of the recipients, noting that recipients of Hizb ut-Tahrir's messages are likely to be better off economically, and have high linguistic and technical competence thereby biasing the audience and the nature of discussions that take place (Peshkova 2002:19). This leads to sometimes surprising debates in e-Forums that argue the relationship of Sunni Islam to other religions, engage debates internal to Islam, and sometimes even question the political agenda of Hizb ut-Tahrir (Peshkova 2002:21-22). She closes by noting that much more study of actual use of radical sites on the Internet is necessary to elucidate who uses, why, and what connections emerge between them.

The broad variety of radical Internet users, issues, demographics, and forms of Internet interaction make the typological characterization of the complexity of non-state actors (violent or not) within cyberspace is critical. It is vitally important that relevant information on a broad range of issues is appropriately considered, and a typological approach can facilitate this end. The below diagram depicts a basic socio-cultural typology that was first introduced in an earlier discussion of typologies as they referred to deterrence (Chesser, 2007).



In the main, the purpose of a typology in the current work is to provide a generalizable organization structure for military and intelligence analysts and planners to characterize socio-

cultural systems. These systems could include a military organization, a terrorist organization, a tribal society or a nation state.[11]

The following brief descriptions of the typological factors apply to the model above. The first broad category above addresses ***Interests***.

- *Motivating Factors – Ideological*: One source of motivation for VNSAs is the realm of their ideals, some of which may be very abstract (e.g. a Manichean belief in a struggle between good and evil), and others may be more concrete (e.g. the moral superiority of Sharia, or democracy). Ideological motivating factors can include principles of leadership, political values (democracy, autocracy, communism), legal principles, military doctrine, religious dogma. These factors also include basic existential and moral beliefs, such as good versus evil, the afterlife, moral principles such as honesty (also the "Golden Rule"), beliefs about proper place in the social or natural world, cosmology. This is the symbolic realm of an actor's cognitive environment that provides aspirations – how they look at the world. It is useful to separate it into codified (i.e. military doctrine, church dogma, charters, legal codes) and uncodified (social norms, senses of right vs. wrong, morality) norms. Codified motivating factors also include rituals and other scripted performances used to express motivating factors.

- *Social Identity*: This includes the constellation of factors brought together for self-identification or labeling by outsiders; these factors may include history, appearance, language, political objectives/ideology, geographic location, and any other element of the typology. The key here is that self-described identity may provide objectives and/or constrain actors to behave in certain ways. Identities in the cyber domain can be especially fluid and overlapping as actors can take on multiple, and at times radically different, identities.

- *Objectives*: This includes concrete goals that actors wish to achieve; often motivated by or justified by motivating factors (establish a Caliphate to establish Sharia law), identity (extract revenge for historical slights against one's group), or even organizational structure (think of bureaucratic decision making and organizational culture).

People's motives do not exist in a vacuum and understanding motives, behaviors, and even capabilities requires understanding the world from which these emerge. Therefore, the second broad category includes ***Context***:

- *Environmental and Historical Context + Other Actors:* These categories may be thought of as external factors that influence a system under study. Environmental factors include

[11] By definition, "typologies are a product of deductive research. The researcher conceptualizes the types that are relevant to the research. These types form the cells of the classification scheme and each cell is labeled (named). The researcher then identifies cases that possess the characteristics deemed essential to fit the cells. The great advantage of typologies is their ability to simplify complex concepts by classifying objects according to a few, often two, criteria at a time." (Lambert, 2006) Typologies often specify artificial or contrived classifications whereas a taxonomy, often confused with a typology, looks to generate natural classifications. In the case of a VNSA in cyberspace, typologies are likely the best we can do at this time.

climate, terrain, natural resources, arable land/pastures, water, security situation, or political/economic position in world. Also, people's views of the world and especially political motives have a history that should not be ignored. This historical context conditions who an actor is likely to perceive as friend or foe, the key events used by actors to evoke emotional responses, and the actor's justification for grievance. The US Military Academy Combating Terrorism Center's 2006 publication on Jihadist imagery is an excellent example of how historical themes are woven throughout the symbols used by Islamist terrorists. And equally importantly, all actors, whether individuals or groups, behave in relation to others. Other Actors: e.g., "No society is an Island" describe relations with and influences from other societies that are key factors influencing variables within a society. Influences range from political interference (Iran in Lebanon) to refugee populations (Darfur refugees in Chad, Iraqis in Jordan), to immigrants (Turks in Germany), to economic (Western capital intrusion into Third world societies, globalization), to cultural (spread of Western values and behaviors through globalization, spread of global Salafist Jihadism).

- *Demographics:* "How people reproduce." These factors include age/sex structure, age at marriage, availability of mates, marriage types (monogamy, polygamy); sexual behaviors and mate choice were added since these vary by culture; all of these are very important, and have an impact on demographic trends. As noted in the examples of terrorist use of the cyber domain, young unmarried males tend to be the prime targets for recruitment for Salafists, including through the Internet. Understanding the demographic characteristics of these populations can lead to insights as to why they are attracted to such movements, and possibly ways to deflect their interest in violence.

- *Roles/Life Cycle:* "Functions and positions people play in groups." Social context (includes other categories) influences roles. Since a person's social roles typically change throughout life, they are included here. Effective operation in a culture requires knowing how roles change throughout the life cycle. As well documented in the NYPD study of radicalization, violent Jihadist movements require individuals to fulfill certain key roles, such as organizational leader, religious sanctioner, and of course various forms of foot soldiers. Understanding the functioning of a VNSA requires an understanding of the roles necessary in such groups.

- *Organizational Structure/Social Organization:* "How are people in a society organized?" This is a large category that contains many variables not normally considered by intelligence analysts. Understanding the different social organizations that influence an individual or group is the key for identifying decision units and constituencies, and for identifying enabling or constraining factors. For instance, harm done to one's family in a society organized by kin groups both motivates an individual in that group to take revenge, and provides clan or tribal resources for mobilizing that individual. One workshop participant made the point that much of what occurs in the cyber domain is a transference of traditional social relations to a new medium. Because so many organizations impact actors' lives in so many ways, it is important to include norms of behavior, habits, traditions, doctrines, rituals, practices, and it includes: kinship (bilateral, patrilineal, matrilineal descent, kinship terminology; this influences how families are organized - often key primary alliances); sodalities: non-kin based social

organization, county clubs, Rotary, etc.; political parties, religious organizations and military organizations.

People exist in meaningful social structures and draw motives from a variety of sources, including history, demography, identity, and values. However, assessing whether or not an actor is able to realize objectives requires assessment of ***Capabilities***.

- *Production/Technology:* "What people do for a living" jobs, productive activities (farming, horticulture, herding) plus technologies that people use (tools, weapons, implements) are indicators of capability. Anderson's (2007) research is an excellent example of how technical skills of engineers, and their Western incomes were fundamental in initiating and spreading cyber technology throughout the Muslim world.

- *Settlement/transportation/communications:* "Where people live and how they get around/communicate," types and availability of housing, rural vs. urban settlement, road systems, communications are also indicators of capability. Clearly, the infrastructure required for cyber communications, electronic grids, cell towers, satellite systems, and cable systems is key to understanding an actor's capability for using the cyber world.

- *Economic System:* "How production/exchange is organized at the social level." Such a breakout includes markets, barter systems, social division of labor, industrial sectors, distribution of wealth and inequality. Once again, Anderson's research on the spread of the Internet in the Muslim world illustrates how the global market for engineering skills caused migration of Muslims to developed countries where they acquired technical skills necessary to spread the Internet in their home countries. Afterward, complex alliances formed between governments, financial institutions and industries to finance the creation of a cyber infrastructure for the Muslim world.

A fourth broad category above addresses ***Psychology***.

- *Decision Making:* This sub-category of psychology is particularly important when considering the cyber domain, and includes risk sensitivity, emotion, cognitive style, decision modes (typology), and neuroscience. Its influences range from neurological functioning to more social influences (emotional attachment to symbols). As we noted earlier, the immense amount of information available in the cyber world requires filtering; the manner in which people attend to messages in the cyber world and the ways they process those messages will require attention if appropriate models of how a motivated and capable actor decides to act.

Also included in the model above is a broad category called ***Language***. Symbolic communication is fundamental to nearly every aspect of human life and permeates all elements of the typology. Language includes not only traditional linguistic concepts such as knowledge of particular language/dialect used, grammar, lexicon, and phonetics, but also the socially appropriate use of language/dialect(s) in different social contexts.

Chapter Summary

This chapter seeks to lay the social and top-level technical considerations for life in the global, interconnected world. The three sub-chapters that follow this one (Barnett, Axtell and Steinberg) represent divergent but no less reasonable perspectives on the potential successes of the US government in dealing with VNSA use of cyberspace, as well as a likely technological future viewpoint. Barnett advises that the US work hard to foster the development of the Internet for all, be resilient in the face of attacks and not try to own the problem cautioning that it may take a non-state actor to deal with a non-state actor. In support of this final point, workshop panelist John Robb cautioned that, "deterrence within the small group context is best accomplished by working like a participant in the system and not an owner." (Robb, 2008) Axtell describes the co-evolutionary effects that seem to be taking place among all of the players in the Age of Cyberspace, also cautioning against the US taking too much ownership and thus control of the potential solution space.

It should also be clear that a meaningful typology to help the US and its allies understand the complex environment is more critically needed than ever thought possible when the Strategic Deterrence SMA began almost a year ago. The broad typology under development is an attempt to expand approaches to understanding and deterring VNSA. The thoughts captured in this chapter and sub-chapters, as well as succeeding chapters all seem to point to the need to understand Deterrence 2.0 as having only a few parallels to Cold War deterrence. The parallels (and convergences) that do exist, however, seem to show that when it is possible to find something of the adversary's to place at risk, old fashioned deterrence might still work (if that's the way the US wishes to play the game in the Information Age).

2.A Deterrence in the 21st Century

by Thomas P. M. Barnett, Enterra Solutions

The definition of deterrence in the 21st century

I like to leave Cold War analogies back in the 20th century, because they all tend to speak toward the preservation of the international status quo instead of managing a dynamic process such as we face today with globalization. Our problem with globalization isn't that it's geographically stuck and needs defending, but rather that it's spreading at a rate that we can't easily manage in terms of handling all of the new threats suddenly inside the "tent" that—until recently—included a mere one-tenth or so of the global population—namely, the West.

Because threats can come from all angles in a service-oriented architecture (SOA) world, and because our definitions of crisis/war today are much "lower" than in previous ages (e.g., anything with a loss of life, anything that triggers business or network discontinuity, anything with significant environmental impact, anything with significant property loss), trying to define universes of non-state actors with nefarious ambitions becomes a hugely ambitious affair. Likewise, limiting your perspective to just non-state actors with violent intentions misses too much of these actors' ambitions to steer the course of human events by creating unacceptably high returns on investment (i.e., their attempted or successful one-time action triggering an exponentially more expensive lasting response from us).

Or as I like to joke, be grateful Richard Reid didn't shove that bomb up his rear-end instead of just sticking it in his shoe . . ..

Because of the rising complexity of SOA-enabled global business platforms that bind our economy with those of states featuring less robust legal and security rule sets, we are necessarily made more vulnerable to the nefarious ambitions of violent non-state actors. However, as a practical reality, those ambitions, to the rather limited extent they are realized on a daily basis, rarely rise above the "white noise" of snafus and discontinuities created unintentionally or intentionally by nonviolent non-state actors throughout these ever-expanding global networks (a.k.a., "stupid" people operating what David Isenberg calls "stupid networks").

As such, to the extent that violent non-state actors succeed in their efforts, they provide a clarifying function that focuses public and private sector attention to existing vulnerabilities. However, if we unreasonably elevate the importance of such violent non-state actors, we're likely to damage our own capacity for day-to-day resilience rather than expand it—the iatrogenic effect.

My definition of deterrence in the 21st century has little to do with moving as far to the left of "boom" as possible. As globalization reformats traditional societies, the root causes of violent non-state actors will be exacerbated in the short and medium run but ultimately mitigated over the long haul by the extension of rule sets accompanying those expanding networks. Confusing friction (the social anger caused by the reformatting process) with the force (globalization's

penetration of traditional societies) is deeply unhelpful, because conflating the two dynamics muddies causality: the more successful globalization is, the sharper the local resistance to its advance.

As such, I believe it is necessary to accept the notion that the threats from violent and non-violent non-state actors (both intentional and unintentional) will rise in coming years, and rather than attempt to go significantly "left of boom" to deal with root causes (a task better left to friendly non-state actors), I think the national security community should focus on protecting its own networks and working hand-in-glove with the private sector to do the same, with its definition of deterrence being, *Anything you (the enemy) can throw at me, I can counter faster and better*.

In short, rather than threatening reciprocal and proportional punishment (amazingly hard to achieve), it's better to dramatically reduce the attacking actor's perceived benefits—to wit, proving them illusory and meaningless. So as much as the media derides President Bush's "shopping mall" strategy, living well is the best revenge and the best deterrent display.

I argue, as does my company (Enterra Solutions), that the dynamic management of rule sets (e.g., compliance, security, performance metrics, systems integration) is the best path forward for creating resiliency in the face of an unlimited pool of potential threats, not going upstream to deal with motivations per se, a job better left to friendly non-state actors in the private sector.

Recognizing the national security community's biases on this subject

There are a number of unfortunately pervasive biases inside the national security community that fuel unrealistic ambition for "left of boom" solutions to violent non-state actors.

First, there is the assumption that new technologies are persistently transcendent: wiping out the previous paradigm and "changing everything." Americans love to make a fetish out of technology, especially within our military. Instead of seeing them as tools and recognizing we've gone through similar mechanism breakthroughs in the past (e.g., it's still called "wire fraud," so phishing isn't exactly new), we tend to be the ones who ascribe almost magical capacities to new technologies, whereas it's our less advanced brethren around the planet who more readily focus in on the most practical applications--despite our usual condescension on the subject.

Second, there is the totally unsupported assumption that all new technologies favor our enemies overwhelmingly in comparison to ourselves, leaving them to serve as the fountainhead of real innovation while we're allegedly always in a defensive, reactive crouch (I know, it sounds almost too stupid to write).

While it is true that criminals and other informal economy types tend to exploit new communications technologies faster than business or the general population (i.e., the first *anything* usually involves pornography), there is no lasting or pervasive advantage that accrues to nefarious non-state actors over time, as history demonstrates decade after decade. The "Wild West" only stays wild for so long.

Third, all new technology creates "chaos" and thus is uncontrollable, in turn establishing the long-term permanent advantage of nefarious non-state actors, who—again--become the main source of innovation within these domains over time (the super-populated world of Dr. Evils).

In obvious contrast to this notion is a fourth bias that says all new technologies favor those seeking systematic control over others—the Orwellian perspective. Oddly enough, it's the merging of these two diametrically-opposed ideas within the national security community that fuels the most ambition to go as far "left of boom" as possible: if we don't control the non-state actors as soon as possible, all will be reduced to complete chaos, or—worse—the terrorists will soon be controlling our brains with the same evil technologies.

The reality, of course, is that each new wave of technological advance creates more freedom for individuals, not less, and more systematic capacity for self-governance and resilience, not less. Still, these worst-case biases within the national security community are quite pervasive, speaking to that cohort's innate tendency to focus on dangers instead of opportunities.

Thank God for the private sector.

Finally, there is the sad tendency among Americans to view all global history and global grievances as stemming from past and present American action ("We alone created this monster that never would have arisen without our complicity!"). We believe we run the world and cause all relevant world history. We believe Washington runs America and the Defense Department is the only truly capable change agent inside the USG, ergo, the Defense Department can be used to change the world, using the Trojan horse of "interagency."

If that sounds like the neocon worldview that served us so badly in postwar Iraq, then you're paying attention.

Again, the argument I offer through Enterra Solutions is that the national security community should view the spread of networks through globalization's advance as an opportunity--not a danger. The more our networks extend, the greater the transparency for our intelligence community, the more the private sector becomes the pervasive and less resisted agent of rule-set enforcement, and the more resilient communities can become—both in the advanced and less-advanced portions of the global economy.

Competition is nothing. Co-optation and co-evolution are everything. In the private sector IT industry, everyone is simultaneously a client, a distributor, a supplier, a competitor, and an ally.

The need to view the current phase of globalization as a period of frontier integration

Understanding that we're in a period of vast frontier integration ensures that we'll pursue more suitable responses to violent non-state actors and to non-state actors in general.

The relatively rapid extension of globalization from its narrow, Western-based roots (North America, Western Europe, industrialized Asia) to its current, near-global embrace is the most important historical fact of our age. Jump back to the early 1980s and you'll find a mere tenth of the human population connected deeply by markets and security regimes that had moved past zero-sum definitions of defense. But race ahead to 2008, only a quarter-century later, and we

now face a global economy that deeply connects as much as three-quarters of the global population.

Depending on how you count, this is roughly a five to ten-fold increase in the absolute number of people reasonably considered to be relatively deeply embedded in the globalization process, with all the mass violence in the system being ghettoized—to no one's surprise—in those regions of the world that are poorly or only thinly connected (such as through the export of commodities alone) to the global economy—or what I call the "Non-integrating Gap" that extends from the Caribbean Rim of Latin America through much of Africa to southwest, central and southeast Asia.

The challenge we face now is how to rapidly extend the West's long-established security rule sets across this far more expansive geographic swath of the world—i.e., the emerging markets of Asia and Latin America and the former Soviet Union.

A good historical comparison here is the challenge faced by the United States in the period immediately preceding and following the Civil War. Having watched it's territory roughly quadruple in the first half of the 19th century, America was forced to engage in massive frontier integration and infrastructural build-out. Not surprisingly, this was a seemingly chaotic affair dominated by all sorts of "uncontrollable" non-state actors, both good and bad.

In this process of frontier integration, we faced a choice: focus on preventing bad things from happening, or accept that a certain amount of bad things were going to happen and focus instead on spreading the networks of security, transportation, and legal rules. America chose to focus on the latter, accepting a certain level of risk, and mitigating that risk with a security approach that was selectively agile (various campaigns against various local bad actors) but systematically ponderous (the slow but steady extension of forts and then settlements and then towns and then admitted states, plus the progressive elimination of off-grid areas). Our greatest asset in this process was the individual resilience of the friendly non-state actors involved—the pioneers and settlers and early-adopting companies that drove economic activity. As they carved out nodes and eventually networks of control, their efforts were legally recognized through property rights (e.g., the Homestead Act promulgated by Lincoln). Until then, it really was *Deadwood*-like.

And if you want to see the modern version of that show, go visit China today.

I bring up this historical example because of the ethos and perspective it presents. Yes, we want to make all necessary efforts to hunt down the bad guys and prevent their nefarious acts, but overall our focus remains on the extension of governance—rules. So we should be generous to any and all "homesteaders" in this process, recognizing that their positive example is more likely to "drain the swamp" or reduce the pool of potentially negative non-state actors than edicts from above, or a posse that swoops in from outside, or fantastic attempts to apply motivational therapy to those who've already gone over to the dark side (*No, Osama, **I** am your father!*).

Understanding globalization's division of labor in settling frontiers both real and virtual

You need to visualize globalization's historic advance as a series of successful replications.

The original globalization structures of the modern world began in Europe with the rise of nation states in the 17th century, followed by an unprecedented infrastructural build-out that linked those states and economies in profoundly synergistic ways, facilitating the original Industrial Revolution there. That globalization structure was then replicated via Europe's colonial extensions: somewhat successfully to south Asia, less so to Africa, "thinly" to South America, late and with deliberate shallowness to the Middle East.

The only place where the globalization model truly flourished was in North America and especially in the United States, which subsequently emerged, thanks more to the second Industrial Revolution, as an alternative source code for globalization—different from Europe's colonial brand.

Following the self-destruction of Europe's empires in the two World Wars spanning the first half of the 20th century, American-style globalization found successful replication—along with adaptation to local values—in East Asia (e.g., Japan, South Korea, the other "tigers," then China, India and increasingly Pakistan—despite its political unrest).

As we look to the future of globalization's successful penetration into, and integration of, the remaining off-grid locations (e.g., the Middle East, Africa, Central Asia—all sources of violent non-state actors galore) will be driven largely through the efforts of Asians—not Westerners.

The logic here is relatively simple: those "last in" the global economy serve as its most natural near-term purveyors. India and China, for example, are the countries driving the current commodity boom, given their relatively recent income elevation and productive growth. Their models of development are likewise far more appropriate to the regions in question, far more so than the more resource-intensive models pursued previously by Europe and North America.

So when we approximate the cyber sphere with the globalization process, and speak about each in the vein of frontiers to be integrated through the progressive extension of rules and governance structures (to include resistance to that rule-set spread—both violent and nonviolent), it should come as no surprise that the rising, "invasive species" in both realms are those cultures who've most recently and aggressively embraced globalization. They have the surfeit of bodies and ambition and needs and necessitated creativity.

For an America considering the cumulative challenges of postwar and post-conflict and post-disaster responses in these less integrated, "gapped" regions, it's only natural that it eventually come to the conclusion that it's future best allies in this frontier-integrating process are those cultures currently engaged in such activity at home, where domestic frontiers consist primarily of a vast sea of rural poor (a rough equivalent of my Gap strategic construct), for these countries are closest, in historical terms, to this challenge.

In contrast, Europe and Japan are far beyond their colonizing periods, and America's days of frontier integration are—by some measures—anywhere from 70 to over 100 years past (our last big internal nation-building efforts involved the taming of the West and the "New Deal" response to the Great Depression). In our scaling of the industrial production ladder, we've largely priced ourselves out of this activity, both economically and demographically speaking.

So when we speak of trying to tame or marginalize violent non-state actors, whether it's in worlds virtual or real, it's important that we remember that the cultures likely to lead this process will not be Western, but Eastern, and that Asian values will likely flavor this advance of rule sets more than Western values will.

How does this play out in the cyberspace? The West favors both unlimited connectivity and unlimited content flows. The East does not, favoring the former but not the latter, hence the extensive use of censoring and firewall technologies in many of the states there. When we consider the fears of Westoxification (read, pornography) that drive many violent non-state actors in Gap regions, this compromise seems inevitable in the cyber world—at least for some period of time.

Accepting the reality that as connectivity spreads, so too will "irrationality"

There is the general assumption that familiarity breeds trust and that connectivity—especially trade connectivity--breeds peace. Over the long haul, this is clearly the case in international affairs. But in the short-term, especially under conditions of rapid ramping up of said connectivity, the usual reaction from all sides is heightened nationalism. Moreover, when there is heightened connectivity between societies of different levels of modernity, we tend to see a rise in religious sentiment in the less advanced society as individuals there reach for religion as a way to maintain collective cultural identities that are perceived as being put at risk through the exposure to outside, foreign influences (the essence of the globalization process).

The only advanced society given to increased bouts of religiosity when opening up to the outside world is the United States, belying its status as cultural source code for today's globalization.

Having said that, globalization's rapid advance around the planet, when combined with the individual-empowering communication technologies of the Information Revolution, means that the early 21st century is likely to be far more religious than the latter half of the 20th century. It will also feature more "clashes" of civilizations and more youthful rebellion (the Gap regions are naturally skewed toward the youth), along with more nationalism. All these coping skills will be applied to the universal task of retaining identity in a seemingly homogenizing world, the end result being that localization barely beats out globalization in most matters of cultural content.

In the cyber world, this dynamic speaks to the Balkanization scenario, which, to some, signals a "chaotic fragmentation" that subverts the Internet's promise of creating a global culture or village. But to others, this dynamic merely signals that the Internet will largely conform to real world cultural contours—at least in the foreseeable future. It also signals that the resulting cyber sphere will more likely resemble the sloppy, cultural mash-up that is the United States than any clearly demarcated civilizations—again recognizing the rising Asian quotient to that global mix.

So think more "Blade Runner" than "Mayberry RFD," but keep in mind the globalization of Hip Hop.

Dealing with non-state actors isn't about diminishing demand but meeting it

Part of the unreasonable ambition of the national security community with regard to moving as far "left of boom" as possible on violent non-state actors stems from the belief that, even if root

causes cannot be addressed through the cyber realm, effective therapy can somehow be administered through "strategic communications" and information operations in general. Two varieties are found: 1) the Oprah-like, "if they only knew us better they'd like us more" approach; and 2) we'll-disinformation-them-to-death approach. Neither is very realistic given the tendency of believers of all stripes to self-select their cyber sources of news and information. In other words, pissed-off individuals look for rationalizations on the web, not conversions.

Underlying these approaches is the notion that if demand can be turned off, then the pool of potential violent non-state actors can be reduced to those already lost to an aggressive stance—in effect, the at-risk population is depopulated.

The problem with this mindset, besides the aforementioned self-selection tendency, is that it seeks to reduce the demands of targeted individuals instead of simply meeting them—e.g., promoting secularism over religiosity when the former denies the search for reinforcing cultural identity and the latter enables it. Until, for example, it becomes clear to an individual that their religious identity can be maintained under the new conditions of heightened connectivity with the outside world, any communications pushing the desirability of religious freedom comes off as a non-too-subtle assault on existing local tradition—as in, "let my version of non-/religion enter into your culture and compete with yours--or else!"

To truly reduce the pool of potentially violent non-state actors is to meet their demands for identity protecting cultural "tariffs," not reducing them. If we expect these traditional cultures to let globalization in, then such generational trade-offs are inevitable. In the end, only the locals can ostracize violent non-state actors.

Only non-state actors can tame non-state actors

Let me end with two pleas.

First, let me argue that whatever you write should assume a relatively humble tone regarding the utility of driving too far "left of boom." Now, when it comes to the question of trying to find bombers before they are armed with bombs, I'm not saying you don't use the cyber sphere for all it's worth. I'm just saying that the national security community shouldn't entertain fantastic ambitions to win "hearts and minds" through the cyber realm. Simply put, Americans don't trust our own government, so I really don't see why we'd expect foreigners to, especially those already given to disliking us.

Second, realize that the best change agents when it comes to flipping non-state actors (potential or realized) are other non-state actors, especially when it comes to young people and even more so for this current generation raised under conditions of hyper- and/or radically ramping connectivity. In general, young people respond to peer pressure better than authority figures, and authenticity here cannot be spoofed.

2.B Life in the Interconnected World: Globalizing Effects of the Cyber Domain

by Rob Axtell, George Mason University and the Santa Fe Institute

I have been asked to provide a short 'think piece' on this topic, so I shall attempt to take your thinking in some new directions while, due to space constraints, avoiding any pretense of comprehensively treating all facets of the problem.

Let me start by saying that I do not like the sub-title of this workshop—"Promoting and Protecting US Interests in the Cyber World." I would be happier if it were less 'normative' and more 'positive,' in the conventional sense of these terms in the social sciences—'normative' meaning 'what should be done' while 'positive' asks 'how does it work.' Too often policy is put in place to solve real problems before the actual connections between the policy levers and the problem space are sufficiently well understood to promise success. I fear this may be the case for our subject, for the 'cyber domain' is sufficiently powerful and 'plastic' that its most pernicious use by actors antithetical to the West are surely yet to come, and it is almost certainly true that policy prescriptions we might author today will primarily treat symptoms instead of the problems themselves.

Violent non-state actors are certainly not a new phenomenon. Violence against the state by loosely organized antagonists has roiled every empire since the dawn of history. The boundary of the Roman Empire, for instance, was essentially determined as the distance at which the Empire's reach was matched by one or another 'barbarian' group, of which there were probably thousands over the better part of a millennium, all engaged in more or less violent action against the Romans and their minions. These groups varied greatly in their organizational forms, some being proto-states whose names we know from history, while surely the vast majority were more loosely knit, temporary coalitions of tribes, many of which, when not fighting the Romans, would have been competitors for resources, land and so on. In the same vein, consider pirates in the 17th and 18th Centuries. Operating on the fringes of competing European empires, these (largely European) non-state actors were incredibly violent, plundering and pillaging all manner of treasure being expropriated to old Europe, often with shocking violence (Pennell, 2001). These actors were eventually neutralized by the 19th Century, but not until states grew in size to effectively rule all the seas with large navies (although some pirate activity of this type remains in the least developed parts of the world even today). In the American Civil War, it is well-known that groups with only loose connections to either the Union or Confederacy fought very violent, irregular campaigns, often against civilians. Much like current non-state actors, it was often difficult to distinguish those pursuing the pro- or anti-slavery cause from those who were simply common criminals and outlaws. William Quantrill was one such leader, whose violence is legendary (e.g., Lawrence Kansas massacre of women and children) and whose connections to the Confederacy were at least tenuous. Several members of his band went on to infamous bandit careers (e.g., the James-Younger gang).

Most violent non-state actors have appeared on the fringes of civilization, often taking advantage of the technologies that had been harnessed by the state to extend its control. In the case of

Rome, the great Roman technologies of road and bridge building, aqueduct and sewer construction, and armor and weaponry, were largely assimilated by their opponents on the fringes of the Empire, and eventually brought to bear against Rome. Similarly with the pirates, who availed themselves of the latest ship-building technology to outfit their vessels to match their guerilla needs.

Until the late 19th Century, such non-state groups had essentially local structures, dictated by the necessity of proximity for communication and coordination of activities. Until then, such actors were essentially local 'bands' of like-minded individuals. It is only with the invention of the telegraph and telephone, the first speed-of-light 'network' technologies, that such actors could organize their activities while physically remote from one another. As such, the violent non-state actors of the late 19th Century to the present, many of whom were either nationalist or communist/anti-communist in character (or some combination of these), achieved a larger scale, a more elaborate division of labor (e.g., military and political 'wings'), and an overall structure that was not limited by physical boundaries, but by ideological ones. For example, Chinese communist guerillas were able to extend their organization to much of their country, eventually, but were not simply clients of Soviet Russia, with Maoism being programmatically distinct from Leninism. The critical role of technology also explains why such combatants, once they have achieved some success against the state, target with high priority the control of television and radio broadcasting stations, both for propaganda purposes but also for the enhanced command-and-control possibilities they make possible, especially as the guerillas find it necessary to morph themselves into a state-like apparatus upon achieving victory (e.g., Castro and Guevara).

These historical remarks have been made as evidence for the first point I wish to make, that the current crop of violent non-state actors, in making use of the Internet specifically and computational technologies generally—in a phrase, the cyber domain—represent simply the latest stage in the development of a long line of technologically-enabled combatants with interests opposed to the system of states in which the actors find themselves. Further, in the same way that the telegraph, telephone and television provided the first 'speed of light' technologies toward globalization, as sailing ships had provided the first 'speed of wind' technologies of globalization before, and Roman roads had provided the first 'speed of walking' globalization even earlier, the current cyber domain provides greatly enhanced connectivity and bandwidth, greatly facilitating communication and trade, the hallmarks of globalization.

Every successful new technology produces competing effects, as Schumpeter's term for innovation, 'creative destruction,' suggests (Schumpeter, 1942). On the one hand, new technologies introduce new capabilities that can be harnessed to simplify production, reduce costs, improve productivity, and enhance profits, while providing greater goods and services to end users. On the other hand, they devalue existing investment in older, substitute technologies, upset existing work rules and regimes, challenge cultural practices, and put pressure on extant social conventions. Truly *disruptive innovations* can spark potentially radical evolution in political, economic, and/or social institutions.

The Internet is, in many respects, a disruptive innovation. It has changed many things: how retailing is practiced, how news is disseminated, how intra-firm communications are managed, even how taxes are filed. How to make money from the Internet—finding the right 'business

model'—remains more art than science, with many traditional businesses yet finding it difficult to profit online but forced to be online because competitors are a presence there.

The cyber domain is a force in globalization, a key player in the progressive development and articulation of worldwide trade and economic integration, but it is not the main driver of globalization. International free trade agreements, minimal controls on capital migration across borders, near open access to very large-scale low-cost labor pools, widespread political stability, relatively smooth fluctuations in currency values, and increasingly ubiquitous communication technologies have all facilitated globalization. It is easy to see that each one of these factors is closer to necessary than sufficient for the process of globalization, for without any of them the pace of the process would be much reduced, while no one factor by itself could have led to the level of global integration we have today.

The present pace of globalization will likely continue for some time, influenced in a limited way by the ebb-and-flow of the various factors mentioned above. For example, political uncertainty due to the Iraq War and currency instability due to US trade deficits and devaluation of the dollar will each contribute to diminishing the amount of globalization that would otherwise have been realized, but the off-shoring of jobs to low labor cost countries will continue, alongside the repatriation of profits to foreign owners. There will continue to be some rearguard actions against globalization, as disenfranchised labor in the developed world seeks compensation for lost jobs and reduced standards of living, but such efforts will be marginal and will have little effect on the overall character of the emerging globally-integrated economy.

The continued process of globalization will produce a great variety of global-scale social phenomena, from the rise of middle classes (and billionaires) in developing countries to environmental progress (e.g., the end of the printed newspaper) to the formation of mega-cities of one hundred million inhabitants. But of these many effects, I would like to focus on the three that I think are the most significant for our purposes.

First, globalization is currently causing a shake-out in all production technologies that feature economies of scale. That is, for industries where the unit cost of making the $(n+1)^{st}$ unit is less than for the n^{th}—typically heavy industry—there is enormous economic incentive to move production to a single regional location where the benefits of increasing returns can be fully extracted. Consider automobiles, where there is tremendous pressure on Detroit at the moment and for the foreseeable future, to become a 'world class' producer or go out of business. In essence, a fierce worldwide competition has been ignited between a few automotive manufacturers—Toyota, General Motors, Daimler—to see who will dominate 21st Century vehicle production. This process of global-scale competition is happening in many industries, and will produce, over the next few decades, a few global winners, with world-scale production concentrated in a few hands, a few centers of power. This process is quite different from what T. Friedman argues is happening in *The World is Flat*. We are seeing the centralization of power and resources as a result of globalization, which is a 'flattening' only in the sense that those not in the centers will see their income and power considerably homogenized. Just try to buy a locally designed, engineered, or manufactured vehicle in 2050! This global shake-out will produce winners and losers and for many it will not be a pretty picture.

This leads to the second great effect of globalization, the spontaneous generation of great disparities of income, wealth, living standards, and quality-of-life. While such disparities have long (always) existed (Smart, 1912), are present today, and would occur in the future with or without globalization, the size of the gaps in the globalized world will lead to strife and unrest. While the poor of the future will no doubt have a better life than the present day poor, and future middle classes are likely to be better off than their analogs today, there will be more super-rich to envy, especially at the global 'centers' that win the world class manufacturing crowns in autos, steel, ship-building, semiconductors, software, and so on. The discrepancies between economic classes will play out in myriad ways, and little can probably be predicted in advance for the kinds of conflict that may arise in any particular region. But suffice it to say that inequitable divisions of the products of human labor and ingenuity have been the source of much conflict throughout recorded history. In under-developed and developing regions, such disparities may serve as the 'root cause' of movements that will limit globalization's ultimate reach, whether because political forces antithetical to globalization gain power, or because such movements simply wreak such havoc that they effectively cut-off the local march toward global integration. Such movements may not be peaceful and therefore the formation of violent, non-state actors may be viewed as a direct consequence of globalization. The cyber-domain and global economic integration lead to status disparities, and knowledge of such disparities, and this fuels anti-global movements.

The third way that global integration is most likely to powerfully manifest itself in the future is through severe financial disruption. If we look at financial history, the first great wave of industrialization in the US—gilded age railroad, steel and other heavy industry, mostly in the Northeast—was an early example of deep economic integration, 'globalization' on a regional scale. It largely ended in the 'Panic of 1893,' in which the US stock market fell markedly, precipitating four years of recession/depression, then the birth of the Progressive Era followed by the break-up of the large trusts. A generation later the Roaring Twenties in the US was another era of economic integration, this time fueled by technological developments like the automobile, airplanes, radio and motion pictures. This era too ended with financial disruption, as the US stock market 'Crash of 1929' brought twenty-five percent unemployment rates to the US by the early 1930s, and propagated around the world hitting essentially all developed countries. It took over a decade for the world to rise from that economic and financial catastrophe, and led to a truly global war.

In summary terms, a main reason for these financial collapses in the wake of economic integration is that the new institutions that grow up in the context of economic growth are not designed to handle large-scale downturns, and so when crisis happens new institutions must be brought into existence to manage the myriad problems that result. Building new institutions sufficient to the job may take years, especially in the context of trying to manage the human tragedies produced by such events (e.g., the New Deal). In somewhat more biological terms, populations are vulnerable to severe fluctuations (and possibly extinction) when they are insufficiently diverse. As economic integration proceeds, firms and industries and regions become more alike—they share the same risks, use the same accounting practices, hire from the same executive pools, etc.—so when exogenous shocks arrive (e.g., bad harvests, technological innovations) the response of the many actors is highly correlated, leading to amplification of the shock. It is only through the diversification of actors or the establishment of organizations to attenuate the shocks that the effect of such events can be limited.

Today, it is being overly generous to call the worldwide financial 'system' a system at all. Rather, it is a hodgepodge of loosely connected electronic markets and regulatory structures, with trading firms providing most of the connectivity between markets, while central (national) banks intervene at the margins. There are important international institutions in place, like the IMF, but the focus of these entities is to provide credit primarily to developing nations and not the overt management of international financial markets. Therefore, given this landscape, as the current wave of globalization proceeds, and economic actors push the existing apparatus to its feasible limits, there will arrive one or more events that trip this system into crisis. When this happens, because the world is largely integrated, it will cause an economic downturn on a global scale. As to the severity of the downturn, if new institutions for managing the crisis internationally can be quickly legislated into existence, and if these function effectively, then perhaps a global recession will be the only result. However, if the situation deteriorates before such institutions are brought to life then a global depression could result. If this were to happen, surely there would be huge demand by affected citizens to form global financial institutions, and incentives for politicians to do so, but in the quagmire of such a global downturn, it might take decades to create truly global institutions with enough power to make a difference on a worldwide scale.

At the moment we do not know if such a global financial meltdown is highly likely, merely possible, or unlikely, but it is surely possible. Prudence demands that we make some plans in advance for how to survive such an event, and survival may be at issue for some, since increasing fractions of people live in urban centers and rely on industrial production for their daily consumption, production that could be interrupted if systematic economic disruption were to occur.

So far my remarks have been more about globalization than the cyber-domain. Indeed, the way I see it, it is not so much that the cyber-domain affects globalization as it is the other way around, that more or less exogenous processes of globalization have great effect on the cyber-domain. That is, as global-reach of low-cost production brings high performance computing and fast Internet connections to great numbers of households around the world there is increasing confrontation of globalization's urgencies with traditional cultural systems. From such confrontations there can arise conflict or cooperation, depending on the context. Surely in some environments people will view the intrinsic value system of globalized production as sufficiently opposed to their traditional values that they will form organizations actively opposed to the further encroachment of the global economy on their lives. Such organizations could work peacefully or use violent means, and today we do not have a deep understanding of the determinants of one strategy over the other. However, we do not even have a good behavioral understanding of the previous effect, that is, the kinds of contexts out of which active opposition emerges. Surely simple behaviorist theories that one often finds in the press, say, are too simplistic, that mere contact with Western standards and beliefs breeds disdain. For it is a basic research question as to the exact way people sort information containing confirmatory evidence of their world view versus how they assimilate disconfirming evidence.

Ultimately, there is a kind of dialectical connection between processes of globalization and the cyber-world: one begets the other and has a tendency to turn it into its opposite. More accurately, there is a kind of co-evolution afoot of the cyber domain and globalization processes, and it is difficult to see just exactly where it will end up. Anyone willing to offer hard forecasts is

probably guessing, at best, or trying to sell something in the typical case. In order to properly understand the connection between the two processes we need to do basic research on the inter-relation between information technology, on the one hand, and global business practices on the other. Such a research program is eminently do-able with available knowledge and research methodologies today, but it is not clear who would be the primary consumer of such research, and therefore who should fund it. We would all profit from having a stream of basic research bearing fruit concerning how the developing world is using their access to the cyber world, whether it is shaping their views of Western values (or lack thereof), and how this depends on educational background, religious affiliation, income level, and so on. Short of having such a research program, we are left to guess about how all this will turn out, and what it means for US interests, in the small, and for future generations of humans, in the large.

2.C Innovations in "Cyberism:" An examination of the changes to Cyberspace in the coming decade

by Ken Steinberg, Savant Protection

Preface

The intent of this paper is twofold; firstly, to provide visibility into the innovations being made in "cyberism" and technology which will shape our world in the coming decade, and secondly, to understand the potential role these innovations will play regarding deterrence against cyber-warfare.

The topics covered in this paper represent only a few of the changes cyberspace will experience in the coming years but they are perhaps some of the more profound. Cyberism is still in its infancy and many of the uses of cyberspace have turned out to be inadvertent afterthoughts, not deliberate planning. The natural growth of technology and the Internet has created both wonderful and worrisome outcomes. If we are smart about how we design the advances of the next decade, the chances are good that the world can continue to benefit from the electronic fabric we are weaving into our lives without suffering the potential pain it may bring.

Prudent and effective development can only be done with forethought and only through collaboration. As is often the case in capitalism, and intentionally so, an environment is created that fosters innovation but discourages collaboration. The time may be here for the government to step in and take the leadership through its science and technological agencies. It may be time for science and society to step forward together and take an active part in the next phase of the world's digital development. Cyberism is not technology. It is the use of technology in society. It is this use, for good or evil, which we need to meter.

The Age of Intelligent Data Marshalling

Computing, over the past twenty years, has passed through two distinct stages of development. The first decade, after the introduction of the personal computer, was focused primarily on the refinement of hardware and the central processing unit (CPU). While other advancements of note were made, most of the true innovation was aimed at increasing CPU capability while decreasing size and power consumption. In contrast, the last decade has been spent developing the infrastructure necessary to take advantage of the new-found computing power in collaborative and distributed environments, as is made evident by the growing presence of the Internet. While both areas will continue to benefit from innovation, cyberism is about to make a shift into a new, yet complementary arena.

Over the next twenty five years, cyberism will usher in a new stage of growth. This growth will focus on data, its storage and new appreciations of its use. The underpinning for this growth will be a movement away from CPU-centric computing to data-centric interaction. Computers, and computing, will become relegated to nothing more than data access interfaces as the introduction

of two new concepts change the way users think about computing: Intelligent Memory Cores (IMCs) and Data Marshalling Units (DMUs).

Intelligent Memory Cores (IMCs) will form the foundation for the strides of the next decade in cyberism. IMCs are a combination of high density, static memory storage (ex 500 GB) with intelligent, specialized, mesh network-enabled CPUs. IMCs, due to their intelligent nature, will be tasked with classifying and relating all information that is under their immediate control. All data; upon creation, manipulation, and destruction will be meta-tagged and semantically analyzed. This omnipresent "marshalling" of data will redefine how humans interact in cyberspace as information is thought of in terms of its use and relation instead of its edges. The use of cyberspace will, though data marshalling, better approximate the natural way humans process and access information. DMUs will facilitate relational and fuzzy connectedness so that humans can concentrate on data use, not on constant organization. The concept of "edges" (i.e. where data is stored, how to get at it etc.) will move away from physical space and embrace n-space with the only constant edge being ownership.

Cyberspace, when facilitated by IMCs, will be uniquely customized based upon the data view desired and the capabilities utilized to gain access to related data (see topic on Sphere of Influence). Present-day computers will be replaced with more tightly integrated, micro-scale/man-machine interfaces through which cyberspace users will command DMUs to find, analyze, use and present information in line with a particular need. The concept of file systems and storage devices will quickly dissolve as the combination of IMCs and smaller, cheaper, less power-hungry DMUs emulate human thought patterns allowing for a far more intuitive use of information.

Immediate Data Transmission

Closely accompanying the concepts of edges and data-centric computing, serious consideration must be given to the hypotheses being put forward in quantum mechanics as they related to computing and in particular networking.

Over the last ten years, network speeds and access ubiquity have grown at an exponential rate. Gigabit terrestrial networks can be bought for the home. Internet Service Providers (ISPs) can deliver multiple megabits of throughput via fiber to each household and wireless access continues to climb by tens of megabits every other year as advancements in frequency use and digital data transmission are introduced.

What has not been openly discussed is the potential for immediate data transmission using quantum entanglement techniques. Quantum entanglement will allow for the immediate transmission of sub-molecular states between two particle pairs regardless of the distance separating the two. This will allow changes in one particle to be immediately reflected in the second regardless of distance. A simple application would be to consider counter-clockwise and clockwise spin as a values of 1 and 0 respectively. Change the spin on one member of a pairing and the "value" is realized in the other pair member instantaneously. This is no different than the physical transmissions seen today except for the lack of true particle movement.

This will create opportunities for transmission of information without physical media. While mind-numbing to imagine, this is akin to informational teleportation using quantum complexity. The net result will lead to the ability to transport terabytes (or more) of data instantaneously to one or more points on the planet's surface (or further).

Working within Spheres of Influence

As the physical nature of cyberspace blurs, with the merging of laptops, servers, handhelds and cell-phones, users will simultaneously embrace and reject ubiquitous means of information access. Signs of this reality can already be seen in the arguments regarding the introduction of open operating systems for handheld devices and the loss of control this will force on service providers, both terrestrial and wireless.

This contiguous informational point-of-view will apply to both inbound and outbound data acceptance, dissemination, and control. As a result, users will strive to gain better and more granular control over where, when, who, why, and how they will interact with the cyber-fabric. This control mechanism can be best visualized as Spheres of Influence (SOIs).

Spheres of Influence are analogous to present-day rules systems that will allow a user to define personal data flow (inbound and outbound) based upon a number of parameters which might include trust, time, place, privilege, and speed. Through the use of SOIs, users will control not only the parameters by which information is reaching them (voice, video, data and/or combinations thereof) but also outbound data sharing and broadcasting.

The maturation of personal IMCs will usher in new methods of interaction as each portable, mesh network capable device functions far beyond simple data and voice access. Personal IMCs, coupled with innovations in data transmission and audio-visual capabilities, will allow each user to offer vicarious experience as IMCs become individual broadcast stations with two-way communications. Spheres of Influence will allow users to knowingly broadcast certain types of information either on-demand or by choice to SOI consumers being inbound aware. Clear examples are; teenagers broadcasting their current music selections to a circle of friends or battlefield commanders gaining multi-dimensional situation awareness through direct data sharing with front-line soldiers.

While it is easy to imagine the progression of computing devices towards broadcast capable qualities, the maturation of these hardware/software components will be severely hindered until SOI controls are in place. As lives continue to be invaded by new digital media devices and as these devices adopt full duplex communications (vicarious transmission), consumers will demand more control over this media. More attention will be paid to how media is allowed to impact private lives and how sharing occurs. Spheres-of-Influence will provide the foundation for how consumers compartmentalize their lives and regain the privacy they require in order to stay functional in a digital world. The inability to disconnect from the flurry of digital information, if left uncontrolled, will either have a profound effect on social behavior or drive wholesale public rejection of certain media efforts. SOIs are a critical underpinning for the acceptance of digital media and the potential invasion of privacy it represents.

Blurring the Man-Machine Interface

It is generally accepted that the physical interface between man and machine will blur and blend over the next century. Not generally considered, are the two means by which this will occur and the repercussions they will cause.

- Physical Blurring

  Near range, low power wireless networking has made possible what would have previously been impossible due to medical considerations. Although there has been significant discussion regarding the use of subdermal (below the skin) and transdermal (protruding from below the skin) implants, the appearance of MRSA (Methicillin-resistant Staphylococcus aureus) bacteria has significantly reduced the amount of work going into transdermal interfaces. The risk of exposed wound sites is too large given the manner in which MRSA invades the body.

  Subdermal interfaces linked with surface wrapped interfaces will be used in the new age of computing where the man-machine interface will remove the need for keyboards, mice and screens. Voice synthesis algorithms and input devices have made significant technological advancements to the point where vocal pickups will become more effective, especially in subdermal interfaces where environmental influences (random noise) can be filtered. Optionally, input pickups using nano-technology may allow for tendon and muscular flex monitoring to simulate keyboard use as well as real-time line-of-sight tracking for mouse movement. The largest obstacle to eliminating viewing screens has been the vertigo affect users have experienced when using projected screen enhanced view goggles. Nano-technology should allow for the creation of glasses or contact lenses that will provide visual computer interfaces at focal points, that will not cause nausea due to focus change.

  Note: The implantation of subdermal interfaces will provide interesting opportunities for data security with respect to how access to information "feels". It will become possible to make a user feel "uncomfortable" when accessing information they are not privileged to access as a means of deterrence.

- Machine Blurring

  While true artificial intelligence is still many decades in the future , rules based interaction with machines via embedded processors with wireless interfaces is likely within this decade. The first instances of direct machine interfacing will most probably occur in medicine or warfare technology. Users (physicians guiding internal nano-bots to wound sites or commanders interacting with swarms of drones) will interface with machinery via direct query and command instead of via dials and ports. This will allow users to add intelligence to decision making processes from safe distances and query the ongoing status of operations without the slow serialization of polling. Certain large scale (whether the battlefield is a body or a country) deployments of semi-sentient devices will require human interaction in order to provide logistical and decision making capabilities.

Creation of Cyber-relative Nation States

Cyberspace and the manner in which cybercitizens use and interact with digital fabrics will go through some radical and yet familiar changes as the perceived threat to nations is reflected in their Internet policies. In many ways early signs of cyber-nationalism are already making themselves apparent through the requests being made of ICANN, the agency in charge of managing the naming structure of the Internet. There are several driving factors:

- Nation State Security

  Currently, most infrastructures are relatively open, but the problems associated with terrorism, both physical and electronic will soon change the means by which cybercitizens access national infrastructures. It is extremely probable that a high profile data loss incident will occur at the 2008 Summer Olympics. This incident or one similar will create the level of pain necessary to jumpstart serious discussions concerning infrastructure control. Safeguards will be put into place that will function similarly to passports. This form of access validation and control will allow intelligence and national security agencies to better track domestic activities of Violent Non-State Actors (VNSAs) as they use electronic media. Past efforts in the creation of a global signature based on technology, such as X.500, will be revisited as a means of access and use validation. This namespace will then be used by ISPs to control and report on access to cyberspace.

- Censorship and Content Control

  Many nations have already voiced their displeasure with the information which is readily published on the Internet and seeping into their cultures. What is deemed a matter of free speech or expression in one nation may be highly offensive to the population of others. Pornographic material, capitalistic efforts, and implied propaganda are three areas that have drawn the most complaints. As a result, many nations will request control over the content entering and leaving their cyber-nation states through a variety of both electronic and manual methods.

  While there are many viewpoints held regarding the sovereign rights of nations in cyberspace, given the lack of precedence, many will take it upon themselves to institute their own control mechanisms. This is already apparent and growing. The impact of these efforts will not be felt by the general populous as technology will outpace most control mechanisms implemented.

- International Commerce

  With the nationalization of cyberspace will come the opportunity to introduce the foundation for taxes and tariffs on electronic sales. Not the sale of physical goods electronically but the sale of electronic goods via the Internet, such as software and information. Currently there are no means by which to identify and hold accountable both the buyer and the seller, but national control of infrastructure boundaries will allow governments to institute banking laws which will lead to online sales tax.

> There are still obstacles present for charging tariffs such as alias websites but as a whole, taxation, especially in international transactions will become standard practice. The introduction of international Internet tariffs is only predicated by the need for the first nation to declare nation-based Internet boundaries. It is likely that this will begin with those nations who wish to censor Internet content, creating the necessity for electronic boundaries. This will cause other nations to respond accordingly, thus creating the conditions necessary for tariff implementation.

All of these factors will lead to the creation of cyber-borders. These borders will be policed as well, if not better than, their physical counterparts. These factors coupled with growing unease and the reality that all networks, both terrestrial and wireless, are under the ownership of companies who function within governing systems will lead to the creation of more control and monitoring on the part of the infrastructure providers.

Realizing Release-based Consumerism

Online transactions and the fear of personal identity theft will increase until mechanisms are put in place that will better control personal information misuse. It is unreasonable to expect that every online vendor will provide complete and full security for all customer data. There will continue to be data leaks which will lead to felonious data misuse.

While the theft of data cannot be fully thwarted, there are algorithms that can keep this stolen information from being used, regardless of place and time, within the bounds of use ethics. One such algorithm is that of Release-based Consumerism. Consumers who make a purchase, whether online or in-person, including thieves, will be required to authenticate the purchase via another media mechanism. Examples of these mechanisms may be cell phone, email, or even a significant other.

An example of appropriate credit use utilizing release-based consumerism, might consist of the following steps:

Example of valid transaction:

1. A consumer purchases a book online using their credit card or bank account.
2. The purchase is acknowledged by the retailer but not authorized until the consumer validates the desire to purchase via another form of prearranged communication, for example a text message.
3. The consumer responds to the transaction request via the second communication in one of two ways:
    - 3.1. Approval, after which the purchase takes place
    - 3.2. Denial, after which the purchase is denied, logged, and depending on certain criteria authorities may be contacted.

Example of invalid transaction:

1. A consumers data is stolen and used to buy gas at a station (or an item online)
2. The real owner of consumer data receives an email requesting validation
3. The consumer, knowing they have not made the purchase denies the transaction. No gas purchase is allowed and the thief arrested.

The role of Deterrence in Homeland Security

All of the previously detailed advancements in cyberism will aid a nation's ability to provide homeland security from both a physical and cyber standpoint. Many of the aforementioned solutions will increase the amount of information governments will have access to as they seek to detail the efforts of non-state violent actors. Changes in cyber-nationalism and consumerism will provide more visibility into the flow of finance and the use of infrastructure by all cyber-citizens. Those who seek to restrict visibility into these financial aspects will, by nature, raise suspicion. There is no doubt that information gleaned from electronic surveillance will increase national security efforts. Increasing the capabilities of these advancements will hinge on the ability of the government and industry to work together towards mutual security goals.

One of the problems with current efforts to correlate and model the actions of VNSAs in cyberspace is that many of the collection points were designed after implementation. This has made correlation, in particular, a very labor and computation intensive operation fraught with the potential for many false positives. If changes in cyberism are to be used effectively, data collection and correlation should be designed into new systems before deployment. Without inherent design, much of the useful data used in cyberspace will remain elusive allowing VNSAs to continue to function in plain sight without fear of retribution. If disparate systems are designed to provide the basis for data analysis, the time in which it takes to recognize related data flow will be significantly reduced.

In addition to the tangential benefits which will arise as a result of advancements not specifically aimed at cyber-deterrence, there are also explicit efforts that have yet to be proposed but are feasible given the state of technology.

Tracking Cyber-Miscreants using Digital Dye Marking

Perhaps the largest problem area national cyber-security efforts will face over the next decade is the protection and retention of data, in any form. Over 90% of the information used by the top financial institutions on a daily basis is unmanaged and unmarked. The misuse and theft of this information on a large scale is virtually assured given the lagging state of the security industry in data loss protection and e-discovery. This technology void combined with the exponential growth of mobile computing ensures national security issues on an ongoing basis. Current retention policies (full disk encryption, device control etc) are only effective for data at rest and are generally ineffective for data in use.

Potential does exist for the use of digital dye marking, similar to the dye-bag technology currently used in the banking industry, as a means of both deterring and tracking the use of improperly obtained data. Significant benefit can be realized by embedding trackable data into current and future information. Digital data used for tracking can be changed frequently and across multiple sources creating a significant level of doubt in the mind of would be data thieves. Knowledge of what data is real and which is acting as a tracking mechanism is kept by the information owner or by a third party. The owner of the information, when using marked data in internal processes, can disregard this data. Those using stolen data will not know whether using this information, will expose them to tracking efforts or not. Similarly those who would procure

stolen data will be similarly disincentivized to buy or trade misappropriated information if the fear of being discovered is looming.

An interesting factor in using digital dye marking is the need for publicizing either the use or the results. The deterrence is truly effective when the cybercriminals are made to realize the potential outcomes, namely prosecution by law enforcement with severe penalty. There are two opportunities for deterrence clearly presented through the use of marked data. One would be to use the digital markers as a means of tracking VNSAs without their knowledge. A second would be to publicize the prosecution of caught criminals as a means of creating fear and uncertainty in the cyberspace community. In either case, the embedding of tracking data in information stores will better facilitate the capture of data thieves and simultaneously increase deterrence.

The Use of Social Networking to Reduce Extremism

The age of cyberism has produced the capacity to extend social networks beyond the boundaries and limits of one's own immediate contacts or geography. It is now common for social and business networks consisting of individuals who have never physically met but still maintain close ties. These social networks are fostered and supported by the expanse of the Internet and the ready access to the tools necessary to find others of like interest.

The capacity to develop relationships and continue to foster them over long distances represent a unique opportunity to establish relations which may contain the seeds of moderation. It is through moderation and familiarity that the words of extremists are beaten back to the fringes of society and become drowned out in the drum of discussion that beats throughout the deep central populous.

It is harder to imagine extremist words driving wedges between those who converse and support each other on a regular basis, either in person or remotely. The social networks of the world and the capacity to provide all with "connectivity" fosters familiarity, making it far harder for extremist words of derision to take root. Humans are not prone to shooting their friends or blowing up those who befriend them.

The more the Internet is promoted and the more local actors interact with foreign actors, the wider, deeper and more accepted the voice of the main stream becomes. The ability to experience foreign cultures without leaving the boundaries of one's own town/city creates familiarity. Familiarity creates tolerance. Tolerance is the enemy of extremism. As nations work together around the world, opportunities arise to bring social networking to all corners of the world. These social networks can be used to reinforce familiarity and extend understanding. Deterrence can take many forms and cyberspace is not always a battlefield. It can also be a playground and a learning ground.

3 Reevaluating Deterrence Theory & Concepts for Use in Cyberspace

by Allison Astorino-Courtois, National Security Innovations, & Matthew Borda, Creighton University

Introduction

Twentieth century US deterrence thinking was founded in the logic of the Roman adage "*si vis pacem, para bellum"* (if you want peace, prepare for war). That is, the overwhelming threat of severe physical punishment or war will bring about the absence of war. Indeed, until September 11, 2001 a general policy consensus maintained that the overwhelming superiority of US forces, both conventional and nuclear, served as an effective deterrent against major attacks against the US or its interests and allies. After the terror attacks of that day however, the *para bellum* and state-centric underpinnings of deterrence policy appeared to many to have been violated, and in fact were pronounced dead by President Bush a few months later:

> *"… new threats also require new thinking. Deterrence -- the promise of massive retaliation against nations -- means nothing against shadowy terrorist networks with no nation or citizens to defend. Containment is not possible when unbalanced dictators with weapons of mass destruction can deliver those weapons on missiles or secretly provide them to terrorist allies."*[12]

The concept of *deterrence* – preventing someone by threat of severe retaliation from doing something he would otherwise do – is as old as man. In the area of global affairs the notion of deterring one's adversaries from acting also predates the nation-state centric models of mutual deterrence that evolved in the context of the Cold War, and with limited exception continues to inform deterrence thinking today. This section explores the conceptual bases of deterrence thinking with reference to two characteristics that genuinely distinguish the late 20th from the 21st century: the expanded abilities of non-state actors of all sizes to pose serious national security threats, and the expansion of *cyberspace*. Our main question is this: *Do current models of deterrence apply to non-state actor cyber threats and cyber aggression?*

Deterrence: Model & Concept

There exists an uncharacteristic degree of agreement in the voluminous literature on deterrence on a number of aspects of the basic concept. First, there is little debate that deterrence is "the use of threats of harm to prevent someone from doing something you don't want them to do," (Morgan, 1983: 17). Second, most agree that effective deterrence is a function of both good defenses and retaliatory capabilities, and that the two most critical components of any effective deterrent are the credibility and the potency of the threatened retaliation. In other words, *Can the threatener actually do what he threatens? Will he do so?* And, *Will I be worse off if he actually acts on his threat?* The point is not that these questions be answered with certainty by a deteree,

[12] 2002 graduation speech at the United States Military Academy, West Point

but that a successful deterrent must meet some threshold of sufficient credibility and potency in order *to inhibit actions the adversary would otherwise have taken* (George and Smoke, 1989).

Beyond this agreement there are various schools of thought regarding how the deterrence concept should be operationalized, studied and tested. The perspective that has dominated the US policy arena however, champions cost-benefit analysis-based "rational" deterrence models typically founded in expected utility and/or game theoretic methodologies.[13] Without going into a discussion of math modeling and mechanics, it serves our purpose to note that as a category these models presume that an opponent will be deterred if, using backward induction, he calculates that the retaliation threatened by a defender is both credible and more costly than his failing to attack. That is, the net value of the losses he expects to suffer as a result of a threatened retaliatory action exceeds the total gain he expects from taking the action he is considering.

Supporting this model of deterrence is a set of six basic assumptions about the decision maker to be deterred, his environment and information flows: he/it is conceived as an identifiable, security-focused rational actor with a set of known and consistent preferences who operates in an environment of complete information about the probabilities of future events and the values of both sides. Broken down, these are:

- ***Known adversary***. The adversary is a readily identified nation-state, unitary actor (i.e., with physical assets, a population, etc. that can be held at risk). In fact, it is implicit in most rational models that retaliatory (deterrent) threats are directed at a specified enemy; deterrence is by definition narrow in scope.
- ***Rational actor***. The adversary is a "rational calculator" in the sense that his choices and actions are not random, but relative to a set of interests and objectives. He seeks to avoid loss or pain across a number of interests and a limited set of available courses of action and will never do something that he believes will result in a net loss for him.
- ***Identified Preferences***. The adversary knows his own preferences over all possible outcomes of a situation in advance of circumstances. These preference ranks are not only known but are consistent and transitive (i.e., if A>B>C, C<A).
- ***Probability Estimation***. Both sides in a conflict can and do estimate nearly perfectly the probabilities of the expected outcomes of their decisions.
- ***Perfect Communication***. There is communication between the sides such that the adversary hears, understands and believes threats as the communicator intends them and, that the communicator can detect that this is the case. There is also the presumption that each side understands the adversary's own values and cost-benefit calculations as well as his willingness to take risks.
- ***Security Focus***. Adversaries are singularly security focused. There is limited linkage between military and other domains, and the adversary is more concerned with security than other issues.

Again, in its most basic form, a rational deterrence model represents a strategic interaction "game" between two players: an opponent and a defender. Both players have complete

[13] An alternative set of deterrence models, neither as elegant nor as well-defined as rational models are those that incorporate cognitive limitations and incomplete information to explain deterrence effect (and failures.) In these models, Achen and Snidal (1989: 148) note, "deterrence is seen as a fundamentally psychological process, in which cognition failures, fear, or simple time pressures disrupt the rational calculations assumed by deterrence theory."

knowledge of the choices available to the other as well as the other's preferences over them. The defender prefers to avoid attack (or some other threatening behavior) by the opponent who begins the game either by attacking, for example, or not. The defender can choose to fight or to capitulate. The commodity that generates the defender's ability to deter an attack in the first place is the opponent's uncertainty about the defender's ability and commitment to retaliate. That is, successful deterrence depends on two things: the defender's credibility, and that the net utility the initiator expects to derive from attacking (benefit) is less than that of not attacking.

This sort of rational deterrence formulation has been a useful (and fruitful) basis for both theorizing and deterrence policy development. However, in reassessing "deterrence" for use in cyberspace it is important to recognize that much of our formal understanding of deterrence and deterrence policy is based on this relatively strict and simplifying set of assumptions.[14] Put another way, these assumptions likely were and are sufficient to offer insight into strategic deterrence of physical invasion, land capture, or direct attack on US or allied territories by the former-Soviet Union and Peoples' Republic of China: two large, extremely security-concerned, non-democratic nuclear nation-states. The question remains however as to whether they are too severely violated to be of use in designing means of deterring non-state actors operating in or through cyberspace. Before considering the implications of these assumptions and the deterrence policies that we have derived from them, we first should characterize the environment, threats and actors of concern.

Cyberspaces & Cyber Actors

The *Washington Post* recently identified the official, extremely broad designation of cyberspace as contained in the January 2008 National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD 54/HSPD 23):

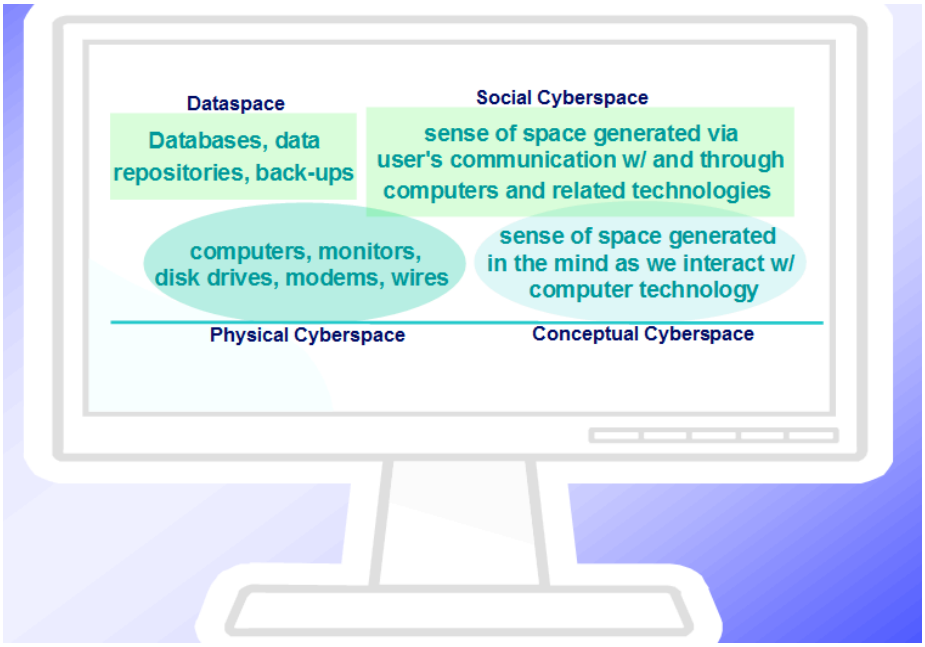
"Cyberspace means the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries".

Perhaps more useful for our purpose however, is Mitra's (2002) unpacking of the "cyberspace" concept – what Whittaker (2004) points out is actually "a myriad of rapidly expanding cyberspaces" – into cyber "building blocks." These building blocks are physical cyberspace, dataspace, and conceptual and social cyberspace as depicted below.

- ***Physical Cyberspace***. Although cyberspace is most generally, "a metaphor for describing the non-physical terrain created by computer systems," (Der Derian, 2000: 773), physical cyberspace refers to those physical components like computers, routers, hardware, power supplied and even in many cases, electricity necessary for use.
- ***Dataspace***. Dataspace is the non-physical information and data storage sector where our websites, on-line newspapers, e-zines and other sources of information and education reside.

[14] Note that the counter-intuitive implications of these models include the rationality of convincing your opponent that you are a bit crazy (e.g., Nixon's efforts in the bombing of Laos and Cambodia at the end of the Vietnam War), why complete nuclear disarmament anti-first strike measures like ABM systems may have negative impacts on security, and the advantages of strategic parity with the Soviet Union.

- ***Social Cyberspace***. It is most commonly "social cyberspace" that people mean when referring to their interactions with the cyber world. This is the virtual space in which people communicate, play and interact via e-mail, blogs, and discovering virtual communities, etc.
- ***Conceptual Cyberspace***. Conceptual cyberspace refers to one's perception of the cyber realm as a "space", a place to "go". It is another complete, real but non-physical world with its own culture, rules and norms of behavior; that space that computer game designers work so hard to achieve.



Distinguishing among these four cyberspaces helps to us explore a vast array of potentially threatening cyber activities. Beginning with physical cyberspace, a first category of threats can be defined in terms of adversarial efforts to compromise, degrade or destroy US physical cyber assets. Kinetic attacks, including theft, on these assets and systems often can be mitigated by defensive measures such as hardening. They also are not conceptually distinct from other sorts of kinetic attack on physical assets that are more commonly the subject of deterrence thinking.

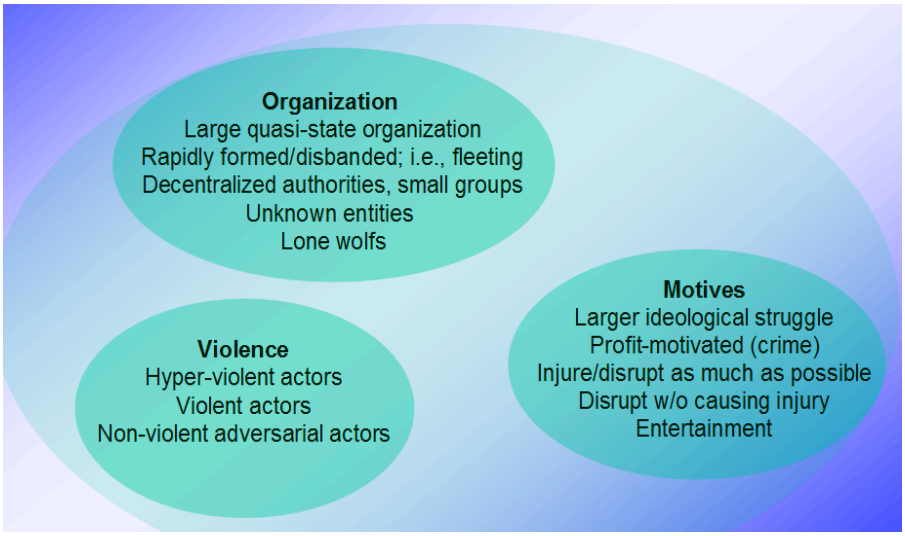
The second category of potential cyber threats are non-physical (e.g., virtual) efforts to compromise, degrade or destroy dataspace. These can range from relatively small-impact identity theft to compromise or manipulation of for example, military targeting packages or air traffic control systems.

A third class of threats relates to social cyberspace and the rapid, expansion of perspectives, communities and movements antithetical to US national interests. This is the part of the cyber world where we have seen the indoctrinating power of militant, radical Islamist ideas, and the sense of common purpose that lone or small groups of individuals can find with geographically distant groups. It is in social cyberspace where new cyber communities and cultures form, and it is a key arena in the so-called battle to "win" hearts and minds.

The fourth and perhaps most insidious class of cyber threat, are efforts to compromise, degrade or destroy others' perceptions of reality by manipulating signals, sensors, communications and

other information that, for example, serve to guide US net-centric military operations, or the presence of incoming missiles.

Of course, equal to identifying of the types of cyber threats is the increasingly complex task of recognizing and distinguishing among the types of actors who may pose these threats. However, because the impact of cyberspace is a relatively new development and technology and innovation occur so rapidly, a thorough appreciation of all current and potential cyber adversaries is difficult to ascertain. One way to attempt to differentiate the various types of cyber actors -- and the magnitude of the threats they pose is in terms of three major characteristics: the type and size of the organization, its motives, and general or known level of violence. Crossing just these three characteristics produces sixty-eight relevant actor types. Even limiting our sample to those most likely to pose serious national security threats, namely, hyper-violent organizations motivated by ideological struggle, profit and a desire to injure or disrupt, produces twenty cyber adversary profiles. *Do we seek to deter each type? Are we interested in all of them?*



Reevaluating Rational Deterrence

During the Cold War period and since, deterrence policy has been indelibly linked to military force.[15] Indeed, the idea of deterring aggressive activities simply by possessing a punitive retaliation capability is a parsimonious and very attractive proposition. It is also an area where the US has tended to hold the advantage. However, in the context of a greatly expanded number and variety of mobile, fleeting and/or unknown adversaries operating within a variety of cyberspaces, much of the assumptive foundation of that deterrence construct may become too restrictive to serve as the basis of policy.

Assuming the continued emergence of adaptive adversaries, one of the key deficiencies of current thinking is its implicit state-centrism. The implication is a tendency to discount domestic or internal determinants and causes of behavior by assuming that actors are more significantly

[15] There certainly have been numerous attempts to influence, assure and persuade outside the military realm, but these have typically been identified as "diplomatic" rather than part of a deterrence policy.

influenced by external factors like a deterrer's threat (Morgan, 1983). Even retaining the rational actor assumption, albeit relaxed to allow for goal-directed gain "maximizers" with broader ranges of interests and goals, the luxury of this degree of analytic simplification may be too costly. We do not mean to suggest that cost imposition – if no longer mainly kinetic – and provision of benefits are no longer valid modes of influencing the behaviors of would-be cyber aggressors. Rather that, no longer assuming an adversary with a set of essentially static basic objectives (e.g., economic prosperity, territorial sovereignty and security, etc. derived from its identity as a nation-state) means more work and a radically increased demand for information about the opponent within his own (subjective) context.

Likewise, the presumption of complete or nearly complete information about the adversary's core values, cost-benefit calculations and risk propensities – as we believed we possessed about the Soviet Union – may be a significant miscalculation. A cyber deterrence concept that required this quantity of context- and actor-specific information over a range of potential adversaries – to the extent that they are knowable – would be an enormous burden on national capabilities.

The bottom line is this: There appears to be *level of generality* problem in using our current rational deterrence thinking as the primary bases of security policy. That approach is a largely simplified model for assessing the strategic interactions between actors assumed to be singularly-focused and with relatively few and simple options available to them. Security policy is generally most effective when it is tailored to address specific actors and actions in context; actors that typically have a range of incremental options available to them spanning the space between conflict and cooperation. When the focus is shifted from identifiable state actors to possibly unknown adversaries in unknown locations both in cyber and physical space, this deficiency becomes more apparent.

It is clear that today's policy planners and practitioners must confront a series of concepts most likely unconsidered by their mid- 20th century counterparts: cyberspace, cyber defense, cyber attack and cyber terrorism, and thus *cyber deterrence*. At the end of the day, the purpose of a cyber deterrence policy is to influence a range of moderate to extreme individuals, and influence a range of actions from tacit support of anti-Western activities to acts of enormous violence. US actions will need to be at times tailorable to target populations and specific undesirable behaviors. At other times, action will be necessary under extreme uncertainty regarding the exact adversary and his specific plans. A number of issues deserve careful consideration as US deterrence thinking is reshaped to serve as a policy guide for protecting US interests in the cyber-networked world.

- ***Defining Concepts***. One approach to assessing the nature of cyberspace has been presented here, but there are certainly other ways to take a comprehensive and insight-generating look at the cyber realm. It is such a rapidly developing, and in many ways still untapped communication and interaction arena that overlooking its fundamental aspects risks forming an inaccurate understanding of its importance and influence as well as its limitations. Similarly, a broader, less restrictive understanding of deterrence than currently is suggested in official publications is likely warranted. *Does refining our deterrence concept as encompassing a range of actions including the ability to shape a potential adversary's choice environment before negative intent is generated help reduce the problem of multiple potential threats in multiple cyberspaces? Is influencing opponents through international and cyber*

community norms a valid approach to deterring the unknown threat? Does expanding the "deterrence" concept to include providing benefits as well as imposing costs help policy makers address the multiplicity of cyber threats?

- ***Defining Thresholds.*** There is the critical issue of communicating to the adversary what exactly is considered to be an "attack" as well as the thresholds between nuisance, disruption, serious security breach and acts of war. *Does hacking into a system to make preparations for a future attack, for example, constitute an attack? Are all breaches to be treated the same way? Do those causing disruption but no damage or loss of life receive attention at all?* Setting these thresholds and the response principles (e.g., response in kind, proportional response, massive retaliation, flexible response, etc.) that will accompany them in the cyber realm should be the first order of business.

- ***Attribution Capabilities.*** Precise and timely attribution of cyber activities is of critical importance for a number of reasons. First, the more precisely we can identify the adversary the more information we can collect about his interests, goals and what he sees as the benefits of the actions we would seek to prevent. The more we understand these factors, the more closely US deterrent threats and actions can be tailored to that adversary. Second, a precise attribution capability will be required to demonstrate and maintain the credibility especially of cost imposition deterrent threats. The threat of retaliation can be perceived as inherently weak when an opponent lacks a fixed location and critical infrastructure to target. If the adversary does not believe he can be seen, discovered or located he is not likely to fear threatened retaliation. Third, the ability to precisely attribute cyber aggressions is extremely important in avoiding the kinds of spoofing and deception in our conceptual cyberspace that could make us believe an attack was coming from somewhere other than where it is. This is the problem at the base of the threat of "catalytic warfare" where an actor successfully misrepresents its actions in order to prompt conflict between others. *How precise do our attribution capabilities need to be?, and critically, how do we convince a potential adversary of a cyber capability without inviting counter-measures?*

- ***Second-order Effects.*** In the introduction to *Beyond Nuclear Deterrence*, Arbatov and Dyorkin (2006) provide a cautionary tale of the effects on Russia security thinking of a US effort to deter terrorists and other adversaries. They cite Russian decision makers' reactions to a US plan to build nuclear 'bunker-buster' warheads able to penetrate underground facilities in terrorist-held areas and rogue states. In fact, many Russians believed this effort was actually aimed at Russia's own deeply-buried and hardened sites. They conclude with a quote from Defense Minister, Sergei Ivanov, who explained that,

> *"Moscow is attentively tracking the developments in the US strategic nuclear force. In particular, we are not indifferent to the US programs of developing mini-nuclear weapons, for each new type of weapon adds up new elements to the general picture of global stability. We are to take it into account in our military planning."*

In light of such thinking, how should deterrence policy be reconceived in order to capture and control this type of signaling – both material and communicated – or secondary effect?

> *Are efforts to shape international cyber standards and ethics the issue here? How do we gauge the deterrent effects of US actions in cyber- and non-cyber spaces?*

These are weighty and difficult questions and unfortunately we offer no simple solutions within this report, just a reference to Der Derian's (2000) riff on Von Clausewitz where he asks whether "virtualization is the continuation of war (and politics) by other means?" Perhaps. It is certainly something to consider.

4 The Cyber-Physical Nexus: Movement between the Worlds: Non-State Actor's Use of the Internet

by Dr. S. K. Numrich, Institute for Defense Analyses

> *Mazer then grew serious and said, "Ender Wiggin for the last months you have been the commander of our fleets. There were not games. The battles were real. Your only enemy was the enemy. You won every battle. And finally today you fought them at their home world, and you destroyed their world, their fleet, you destroyed them completely, and they'll never come against us again. You did it. You."(Carr, 1977)*

On that fateful day, Ender Wiggin, student in the flight academy, found himself quite unwittingly in the cyber-physical Nexus – the place where simulator space had become physical space. Without his consent, Wiggin's teachers, people we would probably call manipulators, enabled the student's actions in cyber media to destroy people and places in his and their real world. The alternate reality and the physical reality met and physical reality was conquered.

The Nexus: A Vital Intersection

In the world of synthetic training, "Ender's Game" has been the tacit ideal for developing synthetic worlds, worlds in cyberspace – worlds so real to the student that tactics, command and control and overall skills learned and practiced in the cyber world could translate immediately to the physical world. The cyber world today, like the simulator in Wiggin's world, is becoming a critical tool in the hands of modern manipulators, terrorist organizations among others, and the most frightening consequences of cyber use emerge in the Nexus, where the cyber world intersects with the geophysical world in which we live.

The world of the Internet, developed in science and engineering laboratories to facilitate collaboration across facilities and delivered to the public by the Department of Defense through the ARPANET project, has subtly revolutionized today's world as did prior technological developments of the printing press and industrial machines changed the world in their eras. The information highway that has given us direct communication capability through electronic mail and chat, online conferencing, a huge distributed library of data and information (everything from trash to the highest quality technical references) and virtually immediate global access has grown beyond the computer-based Internet to hand-held devices linked to the Internet via cellular communications. As the capability has grown, the cost of entry into cyberspace has decreased -- from the availability of low cost cellular devices to development of software that makes publishing simple for the novice. Once the domain of the technocrats, cyberspace is a domain where anyone can find a place, given access.

Our dependence on the cyber world for daily life has increased dramatically. As individuals we shop, bank, maintain records and contacts online. We depend upon cyber resources to control our air traffic, our "fast pass" toll capabilities on highways, our banking and other financial networks, our power grids, our dams, our traffic lights and trains. We depend on credit cards and

cash from automated teller machines to enable both our life at home and our travels abroad. Our understanding of the world around us comes through cyber media, not just the online press, but the images captured by the individual and posted to the Internet through which we feel we have both global presence and immediacy with events anywhere in the world.

The specter of cyber crime weighs heavily upon us simply because activity in cyberspace can and does impact the way we live our daily lives.

Terrorist Uses of Cyber Media – It's More than the Internet

On the international scene, the Internet was championed as a way of enabling the free exchange of ideas, as a means for organizations and individuals to communicate with each other, as a way of breaking down barriers and creating the opportunity to form the "global village". But with the good has come the bad. The Internet has also enabled the spread of pornographic and violent content and the same facilities that fostered international business led to the use of the Internet by criminals of every sort, including terrorists. The attributes of the Internet – its decentralized structure, anonymity and ease of communication – align readily with the loosely networked structures and anonymity desired by criminal and terrorist groups. In examining the use of cyberspace by terrorists, Maura Conway (Conway, 2005) summarized current literature on the topic in the following table.

Table I Terrorist Uses of the Net

Author(s)	Furnell & Warren (1999)	Cohen (2002)	Thomas (2003)	Weimann (2004a)
Uses	-Propaganda & Publicity - Fundraising - Information Dissemination - Secure Communications	- Planning - Finance - Coordination & Operations - Political Action - Propaganda	- Profiling - Propaganda - Anonymous/Covert Communication - Generating "Cyberfear" - Finance - Command & Control - Mobilisation & Recruitment - Information Gathering - Mitigation of Risk - Theft/Manipulation of Data - Offensive Use - Misinformation	- Psychological Warfare - Publicity & Propaganda - Data Mining - Fundraising - Recruitment & Mobilization - Networking - Sharing Information - Planning & Coordination

Conway chooses to categorize the use of cyberspace by terrorists as information provision, financing, networking, recruitment and information gathering, subsuming under these four all those listed in Table I. Weimann's list, reiterated in his more recent book *Terror on the Internet* (Weimann, 2006), provides a somewhat more fruitful ground for examining the intersection of the cyber and physical worlds. The categories he uses in his book differ somewhat from those listed above.

The War of Minds and Hearts – Psychological Warfare

We often think of the war against terrorists and insurgents as a war to win the minds and hearts of the people. However in this context, it is relatively easy for the terrorist to gain the upper hand. Terrorists often engage in psychological warfare by using one or more incidents of physical damage to create a sense of fear and uncertainty that extends far beyond the original

physical act. The cyberspace is a wonderful medium for extending an incident in time and space. Images of children killed and maimed by explosives, captives with eyes blindfolded beheaded by captors, and videos of people jumping from the collapsing World Trade Center broadcast and rebroadcast across the world with an immediacy hitherto unavailable brings acts of terror into the living room. By using and reusing such footage, the terrorist seeks to provoke a reaction disproportionate to the original act.

With the memory of the collapse of the World Trade Center in mind, the mere threat of a repeated act of violence can cause the population to react out of fear. The reaction can produce very real consequences in physical space. While we can argue the relative benefits of security measures at airports, stadiums and large public gatherings, the long term consequences of anti-Islamic sentiment on both the Islamic and non-Islamic communities has yet to be calculated. Anne Speckhard (Speckhard, 2007), based on interviews with radicalized individuals in France, Belgium, the Netherlands and United Kingdom, has determined that personal issues of social alienation, marginalization, and instances of acting out strong feelings of secondary traumatization (for example, experiencing vicariously the suffering of another through violent videos) are strong motivations for involvement in terrorist groups.

Publicity and Propaganda: Websites, Blogs, Listmail

Terrorists seek to publicize singular events for political gain. Prior to the availability of cyber media, gaining publicity involved securing the attention of television, radio or print media. These traditional media are well governed and subject to editorial processes that take the event out of the control of the terrorist. The "wild west" of cyberspace has no such controls and terrorists are free to shape their messages to manipulate their own images and those of their enemies. Well-designed sites give a message a sense of legitimacy independent of the author, thus allowing minority opinion to be perceived as orthodox belief. Perhaps more significant that the website and its message is the link to active blog spaces that permit "free" exchange of ideas. The freedom and openness of blogs or email lists is also open to manipulation by those with an interest in outcomes. Blogs permit the like-minded to share thoughts and build relationships, relationships that can be steered toward violence. In her study of Islamic websites and blogs, Cheryl Benard (Bernard, 2005) found that many websites exploit the ordinary tribulations of adolescents of the Muslim diaspora with advice likely to make the youth's life more difficult and increase the alienation that predisposes him to terrorist recruitment. She summarized primary and secondary effects in the following table.

Table II. Effects of Internet manipulation on Muslim Youths

Primary Effects	Secondary Effects
Build "walls of resentment	Foster non-rational, non-critical thinking
Prevent (social) integration	Discourage problem-solving approach
Make social and economic failure more likely	Encourage obedience to clerical authority
Create psychic preconditions for violence	
Deliberate effort to heighten alienation	Unintentional consequence of the mental and geographic location of the authoring clerics

Data Mining

The web is a vast distributed library with a wide variety of information and information sources available to those who care to search. Search engines abound and through their use we access information that makes our daily lives easier. Google Earth gives us not only maps, but visual images of streets, neighborhoods, shopping and business centers, ports, airports and railway stations. The same site that lets us check on the availability of flights, gives terrorists access to international flight schedules for purpose of targeting. Our laws are publicly available on the web, as are our transportation schedules, school curricula and the capabilities of our communication systems. Use of the Internet by terrorists places us in a difficult balancing act between giving away targeting information to our adversaries and being able to manage our daily lives in the information age.

Networking: It's Not What You Know But Who You Know

Jon Anderson (Anderson, 2003b) describes the Internet as being built by scientists and engineers as a collaboration tool and as such was founded on principles of open access, flattened hierarchies, freedom of information and notions of transient, purposeful connections among people and pieces of information. The flat nature of the Internet allowed terrorist organizations to depart from their prior hierarchical structure and capitalize on the loosely connected cellular structure provided by the Internet. Using the Internet, groups can self-organize, announce their intent, be connected with a desired capability, be passed instructions across the media either openly or in encrypted fashion, and disorganize rapidly in the aftermath of the desired activity. This decentralized activity affords a large degree of protection of the organization while enabling local groups. Rather than becoming an easily targeted hierarchy, the terrorist organization can operate much as a venture capitalist, enabling worthy entrepreneurs whenever and wherever they arise. Motivation and strategic direction may still come from the highest leadership, but the action is decentralized. Terrorists have rapidly learned to use what our businesses have desired to adopt and an efficient management structure: centralized direction and largely independent, self-organized local execution.

Recruitment and Mobilization

The availability of cyber media has dramatically increased the role of social networking in the recruitment of terrorists. Recruiting is a mix of cyber and social contact, particularly among the Muslims in non-Muslim environments. Marc Sageman in his book, *Understanding Terror Networks* (Sageman, 2004), stresses the importance of social networks as a means of providing social and psychological security. Terrorists use the full panoply of web technology to attract, study and recruit those who visit their sites. According to Zanni and Edwards,

> *The information age is affecting not only the types of targets and weapons terrorists choose, but also the ways in which such groups operate and structure their organizations. Several of the most dangerous terrorist organizations are using information technology (IT) – such as computers, software, telecommunication devices and the Internet – to better organize and coordinate dispersed activities…just as companies in the private sector are forming alliance networks to provide complex services to customers, so*

> *too are terrorist groups "disaggregating" from hierarchical bureaucracies and moving to flatter, more decentralized, and often changing webs of groups united by a common goal.* (Zanni and Edwards, 2001)

In his discussion of recruitment, Gabriel Weimann cites numerous case studies of network-based recruitment including recruitment of US citizens to the work of al Qaeda (Weimann, 2006, pp 117-123). The New York City Police Department, in trying to understand the spread of radical Islamic ideology in the United States found that the Internet was a "driver and enabler for the process of radicalization." (Silber and Bhatt, 2007, p. 8-9).

- In the Self-Identification phase, the Internet provides the wandering mind of the conflicted young Muslim or potential convert with direct access to unfiltered radical and extremist ideology. It also serves as an anonymous virtual meeting place—a place where virtual groups of like-minded and conflicted individuals can meet, form virtual relationships and discuss and share the jihadi-Salafi message they have encountered.
- During the Indoctrination phase, when individuals adopt this virulent ideology, they begin interpreting the world from this newly-formed context. Cloaked with a veil of objectivity, the Internet allows the aspiring jihadist to view the world and global conflicts through this extremist lens, further reinforcing the objectives and political arguments of the jihadi-Salafi agenda.
- In the jihadization phase, when an individual commits to jihad, the Internet serves as an enabler—providing broad access to an array of information on targets, their vulnerabilities and the design of weapons.

Instructions and Online Manuals

The Internet not only enables recruitment and mobilization, but it serves a the source of training and instructions for developing specific skills and weapons required for terrorist activity. Information provided over the Internet includes maps, photographs, directions, codes and instructions on using a variety of weapons. Among the sources readily available are *The Terrorist's Handbook, The Anarchist's Cookbook,* and *the Mujahadeen Poisons Handbook.* According to Weimann (Weimann, 2006, p. 125), in 2004 al Qaeda started publishing the online version of its training manual, *al Battar.* Based on these references alone, the role of the Internet is to provide the local cell with the material needed to act in his own geophysical space.

Planning and Coordination

Effective command and control has always been a hallmark of successful military and paramilitary activity. The same technology used by commercial concerns to manage large, multi-national conglomerates enables command and control of dispersed units in terrorist organizations. Modern technology has reduced the cost and time to communicate across disparate groups. Dialog among dispersed members enhances flexibility by allowing members to adjust tactics rapidly based on local conditions. Groups brought together by common goals and agendas can terminate their relationships and re-disperse readily. Satellite phone terminals can be used to coordinate activities and countermeasures can be employed to protect such assets during their use. Terrorists can also use readily available commercial technology including encryption programs to protect their information in transit on cyber media. By use of these modern technologies, terrorists are able to operate in and across any country as long as they have

access to the necessary IT infrastructure. Captured terrorist computers and mass storage devices have revealed this type of activity on the part of numerous terrorist organizations.

Fund Raising

All political organizations require funding to support their activities. Terrorists use a wide range of network-based sources to acquire resources, including charitable organizations, non-governmental organizations, financial organizations and criminal networks. Al Qaeda, Hammas, Chechen rebels and Lashkar e-Tayba have all been known to use the Internet as a vehicle for raising funds. Websites sympathetic to the terrorist cause will often have links to organizations willing to take charitable contributions. It is difficult for the unwitting user to determine that the charitable organization to which he has contributed is a direct path to a terrorist bank account.

In Person or in Cyberspace? – The Right Blend of Both

The Nexus exists on at least two planes. Terrorists use cyber media to recruit, finance, plan, and execute actions that have both direct and indirect impact on the physical world, thus creating an intersection between cyber space and the physical world. Within the greater terrorist organization there is an intersection between the local social network and the network aided and abetted by cyber media. For those terrorist organizations that remain hierarchical and function by establishing individual personal contact among local cells, there is a degree of security that is ostensibly absent in the open world of cyber media. The personal contact with individuals known over many years is one way of mitigating the risk of infiltration. The anonymity of the Internet increases the risk of admitting to the organization a mole from an adversarial group. As cyber media matures, commercially available tools provide authentication, encryption and various forms of security. While helpful, these measures do not provide as much security as personal knowledge of an individual. Thus, the most successful terrorist organizations employ a hybrid of cyber and personal contact to enable their operations.

Leadership and Trust

When personal contact is the hallmark of leadership, followers make many demands on the individuals who assume that role. We speak of strong, charismatic leaders, leaders with an imposing presence and a record of winning in some arena whether it be political or military. Cyberspace changes that expectation. Leadership becomes the ability to persuade through cyber means. When physical presence is no longer required, the leader could be the "skinny guy with coke bottle glasses in the second row" – the same individual we would totally disregard were the leadership manifested in a personal, physical presence.

It is ironic that Islamic fundamentalists who have a great distrust for globalization have made such excellent use of cyber media, one of the most significant tools for establishing global business and economy. In traditional Islamic societies, the flow of communication and lines of trust are firmly and hierarchically established. Cyber media bypasses the traditional gatekeepers and adjudicators of belief. Terrorists make use of this to get their message out, but at the same time it creates a break in the conventional lines of trust firmly established in traditional societies. What we have seen to date is a major engagement of the Islamic diaspora and minimal cyber presence in the Middle East itself. In cyberspace, where users can also be producers playing a

pro-active part in the content as well as consuming it, there exists "intense engagement in political, social and cultural issues that moves around traditional gatekeepers, with their qualifications to interpret and monopolies on educational technology, and admits claims to authority and legitimacy based on other -- frequently on 'scientific' -- intellectual techniques, sureties and communities."(Anderson, 1997b) In this way, modern argument enters the cultural and religious world and the traditional authority figures lose control of perceived truth. Cyber media is a two edged sword for radical Islam.

Return to Ender's Game

Orson Scott Card may have been prophetic in his vision of a synthetic world that was so close to the real world that the boundaries could be crossed unwittingly; however, games of various sorts are catching up with that vision. In 2003 a US-based hate group called "National Alliance" released a video game, *Ethnic Cleansing*, in which "Kikes and Niggers" (sic) await their deaths at the hands of the Klansman. National Alliance did not have the capability to build this game from the ground up, but used the growing market in which sellers of game engines and open-source 3D software packages make it possible for novice groups to create engaging games with minimal investment. Terrorists have used the same capability to great effect. *Counter-Strike*, one of the earlier popular games, permits play of terrorists against counter-terrorists using weapons that behave remarkably like their real counterparts. On the other hand, with the same technology, it would be easy to build and rehearse in a target of choice – an Airbus, perhaps. Hizbollah's *Special Forces* pits the Israelis against Palestinians – the resistance always wins. Films of Palestinian children, boys and girls, playing Jihadist games and discussing how they aspire to die for Islam are testimony to the effectiveness of gaming as a medium for inculcating ideas. Playing games is fun, it's engaging and inspires the quest for actual jihad in the hearts of the children.

The games cited above are all *fps* or first person shooter games. Another class of games is the role playing game and in some of these games, the boundary between the physical and the synthetic is porous. In such games, the user is able to build his own territory, buildings and services and sell them to other players, but in real world currency. Such games are now making news as environments where terrorists can lurk.[16]

Nascent economies have sprung to life in these 3-D worlds, complete with currency, banks, and shopping malls. Intelligence officials who have examined these systems say they are convinced that the qualities that many computer users find so attractive about virtual worlds – including anonymity, global access, and the expanded ability to make financial transfers outside normal channels – have turned them into seedbeds for transnational threats….Because of the nature of the systems, the companies also have almost no way of monitoring the creation and use of virtual buildings and training centers, some of them protected by nearly unbreakable passwords.

The threat of financial markets within the games is mitigated by the fact that they are only a problem when they touch real world finances which we understand how to track. Crime in

[16] "Virtual personalities called a threat to U.S.", Washington Post, February 8, 2008, http://www.detnews.com/apps/pbcs.dll/article?AID=/20080208/BIZ04/802080311/1013

cyberspace may best be pursued and defeated in the geophysical domain in which the criminals live. However, the use of cyber media as a strategic communication tool is far more problematic. Synthetic worlds are engaging and in that they are persistent, physical (apparently) and interactive, they mimic the real world. Gamers, typically young adults in their twenties, spend upwards of 20 hours a week living in an alternate universe and absorbing its culture and messages. We talk of memes that transfer ideas within cultures. Role playing games may be the viral form of transferring memes.

Are There Winning Strategies?

The sense of open communication in which the Internet was developed is probably the most critical element of cyber media to preserve. The spread of interactive communication among people via blogs, websites and games is natural, human, social and creative. For the terrorist, cyber media is a two edged sword, an enabler that also erodes his hierarchical authority and dilutes his view of the world.

As cyber media expands into the Middle East, the adopters will likely resemble the inventors – individuals who value human communication and who put a premium on intellectual achievement. Their discourse is more apt to be in harmony with the core values of the US than with the radical terrorist organizations. We may find natural allies among these individuals if we hold to our core values.

The anonymity of cyber media makes it difficult to retaliate or pose an immediate threat to the terrorist; however, since the terrorist organizations retain a hybrid system in which cyber media is coupled with human social networks, it may be best to consider countering terrorists in the physical world rather than in the cyber world.

Finally, encouraging moderate voices of the Islamic community to be a welcoming presence on the Internet as an antidote to the current jihadist websites would provide the diaspora with a creative alternative as they seek to explore their cultural identities.

5 Models of Emergent Behavior of Violent Non-State Actors in Cyberspace

by Robert Popp, National Security Innovations; Laura Mariano, University of Connecticut; Krishna Pattipati, University of Connecticut; Victor Asal, State University of NY at Albany; and Katya Drozdova, National Security Innovations.

Executive Summary – Chapter 5

For violent non-state actors (VNSAs) on a mission to spread their message, or cyberterrorists who just want to create mischief, cyberspace offers limitless resources and opportunities for achieving these goals. The Internet is unparalleled in its ability to grant individuals access to a mass audience in an environment that has almost no enforceable personal conduct regulations or monitoring capabilities. According to a report compiled by Dr. Gabriel Weimann of the United States Institute of Peace, as of 2004, all active terrorist groups had established a Web presence of some kind, with the intention of exposing current and potential supporters, as well as enemies, to their ideologies (Weimann, 2004). The behavior of such groups in cyberspace has been studied extensively and can be broadly classified by the impact it has on the cyber and corporeal realms. Figure 1 below depicts this interaction and categorizes the behavior according to its origin and impact. Cyber-psychological activities include dissemination of propaganda and disinformation, intimidation, and indoctrination via cyber-based communication channels. Cyber-cyber interactions describe efforts to negatively impact the cyber infrastructure, while attacks planned via cyber means that target the corporeal realm are illustrative of the cyber-corporeal connection. A final category of interaction that is germane to this discussion is the corporeal-cyber connection, which represents actions originating in the corporeal realm that affect the cyber infrastructure. Table 1 below provides examples of recent actions from each of these categories. This chapter focuses on the cyber-psychological and cyber-corporeal connections, with further discussion of the use of cyberspace by VNSAs to disseminate propaganda, recruit members, create publicity, collect and share data, network, plan, coordinate, raise funds, and wage psychological warfare (Weimann, 2004).

The wide-ranging and covert nature of VNSA activity in cyberspace makes modeling their emergent behavior a difficult task that requires a large-scale, multidisciplinary effort. The current paradigm combines technology and perspectives from the sub-disciplines of data collection, data mining and analysis, and predictive modeling; each of these contributes a piece to the puzzle. Automated data collection techniques address the issue of extracting "clean," meaningful, and relevant information from the seemingly limitless datasets that constitute the cyberspace. The methodology must be able to locate a "needle-in-a-haystack", since the activity is often intentionally hidden, scattered across many sites, and frequently moved or removed. However, without the kind of content-rich datasets that data collection techniques can provide, modeling is cumbersome and time consuming, if not infeasible. An example of such a dataset is the so-called 'Dark Web' collection, which contains about two terabytes (2 TB) of extremist/ terrorist related content collected using a semi-automated Web-crawling approach developed by researchers at the University of Arizona's Artificial Intelligence Lab (Univ. of Arizona, 2008).

Once a raw dataset is available, data mining and analysis techniques can be applied with the goal of extracting usable knowledge from the information. The results of these analyses often generate the datasets that inform predictive models. The field has been heavily researched, and

consequently there are many types of data mining and analysis techniques that are well-suited to counter-terrorism applications; indeed, numerous studies have been conducted to evaluate their effectiveness. Some of the techniques discussed in this chapter include link and social network analysis, automated classification of Web content by machine learning techniques, and a qualitative assessment of the technical sophistication, Web interactivity, and content-richness of terrorist/extremist sites on the Internet. Predictive modeling techniques identify discernible patterns of behavior that have the potential to assist analysts with situational assessment, forecasting, and deterrence strategies (Asal et al, 2008). In addition, modeling can be used to simulate the impact of counter-terrorism strategies on the performance and strength of covert VNSA networks. The modeling techniques discussed in this article include the use of hidden Markov models and dynamic Bayesian networks to detect, track, and counteract terrorist networks, and agent-based techniques for assessing terrorist network destabilization strategies.

The terrorist attacks on September 11, 2001, "spurred extraordinary efforts intended to protect America from the newly highlighted scourge of international terrorism" (Jonas and Harper, 2006). These efforts included a significant interest in the potential use of predictive modeling techniques as a means of uncovering covert terrorist networks and plots, and since then, the implementation of such techniques has been surrounded by controversy. According to the National Commission on Terrorist Attacks upon the United States, if the government had pursued leads available at the time, the attacks could have been prevented (Jonas and Harper, 2006). This raises the question: Could data mining and predictive modeling techniques have played a role in averting the tragedy? Experts agree that these techniques have their place in the counter-terrorism domain, as long as they are employed with a clear understanding of their limitations. The consensus is that meaningful results should only be expected if the models are well-informed, particularly by seed information from authoritative outside sources (Last, 2005). Predictive modeling should be used as a "power tool for analysts and investigators - a way to conduct low-level tasks that will provide clues to assist analysts and investigators" (DeRosa, 2004).

Research on the application of modeling techniques to the study of emergent behavior of VNSAs in cyberspace is ongoing. The continued growth of clean, content-rich raw datasets like the Dark Web collection is critical for the further development of modeling techniques, as is the development of information portals that provide efficient access to the data (Univ. of Arizona, 2008). Multilingual techniques for the classification of Web content are another critical area of research, particularly for Arabic Web content. The ontology of the Arabic language poses significant challenges for classification techniques that are based on English phenomenology. Consequently, continued development of language specific techniques are needed (Abbasi and Chen, 2005). However, it is the advancement of methodologies for the simulation of counter-terrorism measures that could have the largest impact on the use of predictive models for decision support. Further development of this application can help realize one of the main goals of predictive modeling: to provide analysts with the ability to accurately predict the outcome of multiple counter-terrorism strategies before selecting a course of cyber or corporeal action. Overall, it is evident from the current status of this field of research that when used responsibly and with a clear understanding of their limitations, data mining and predictive modeling techniques have the potential to be powerful counter-terrorism tools.

This chapter discusses seven topics as follows:

Deterring VNSA in Cyberspace

- Emergent Behavior of Violent Non-State Actors in Cyberspace
- Overview: Data Collection, Analysis, and Predictive Modeling
- Data Collection
- Data Mining and Analysis
- Predictive Modeling
- Benefits, Challenges, and Caveats
- Research and Development Directions

Emergent Behavior of Violent Non-State Actors in Cyberspace

For violent non-state actors (VNSAs) on a mission to spread their message, or cyberterrorists who merely want to create mischief, cyberspace offers limitless resources and opportunities for achieving these goals. The Internet is unparalleled in its ability to grant individuals access to a mass audience in an environment that has almost no enforceable personal conduct regulations or monitoring capabilities.

According to a report compiled by Dr. Gabriel Weimann of the United States Institute of Peace, as of 2004, all active terrorist groups had established a Web presence of some kind, with the intention of exposing current and potential supporters, as well as enemies, to their ideologies (Weimann, 2004). The behavior of such groups in cyberspace has been studied extensively and can be broadly classified by the impact it has on the cyber and corporeal realms. Figure 1 depicts this interaction and categorizes the behavior according its origin and impact.

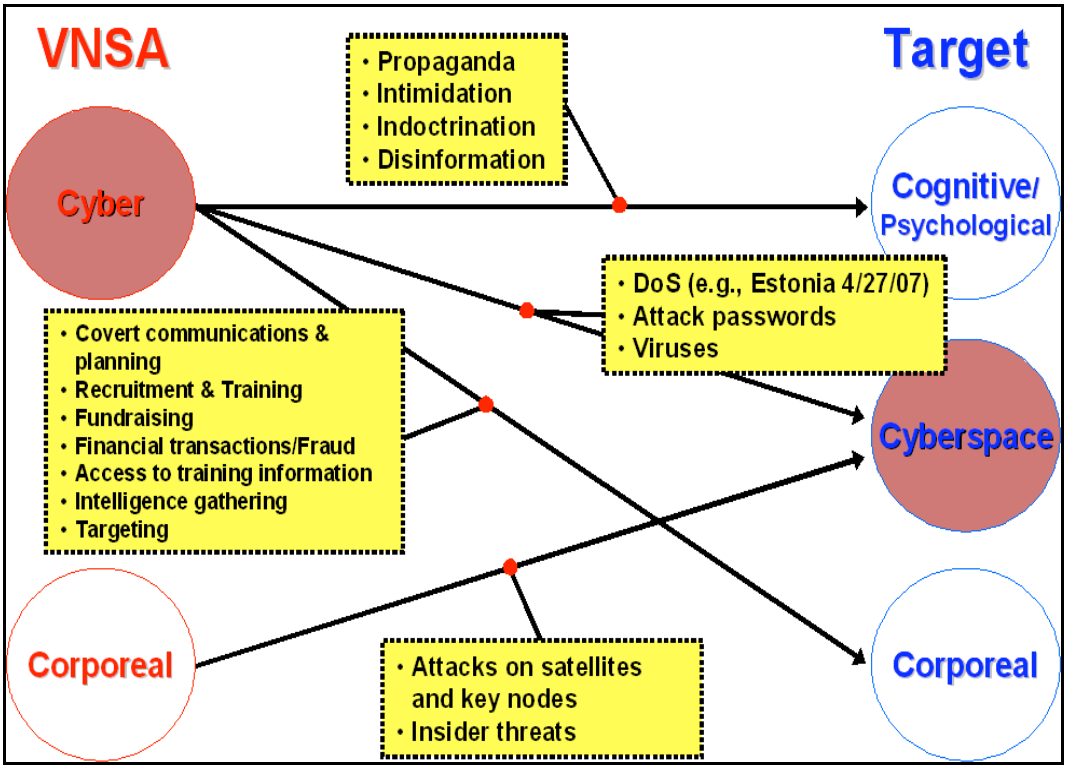


Figure 1: Interaction between cyber and corporeal actions of VNSAs (Asal et al, 2008).

Cyber-psychological activities include dissemination of propaganda and disinformation, intimidation, and indoctrination via cyber-based communication channels. Cyber-cyber interactions describe efforts to negatively impact the cyber infrastructure, while attacks planned via cyber means that target the corporeal realm are illustrative of the cyber-corporeal connection. A final category of interaction that is germane to this discussion is the corporeal-cyber connection, which represents actions originating in the corporeal realm that affect the cyber infrastructure. Table 1 provides examples of recent actions from each of these categories.

VNSA Activity	Example
Cyber → Psychological ▪ Propaganda ▪ Intimidation ▪ Indoctrination ▪ Disinformation	• **Beheading video (Graphic)** http://www.bigducky.com/videos/beheading_videos/beheading.htm • **Bin Laden video** http://english.aljazeera.net/English/archive/archive?ArchiveId=7403 http://youtube.com/watch?v=cI5dNgbE5n0
Cyber → Cyber	• **11/18/2001 Nimda virus** "Richard Clark, Chairman of the President's Critical Infrastructure Protection Board, said the problem of cybersecurity and data protection had its own 9/11 on 18 September 2001 when the Nimda virus spread through the Internet-connected computers around the world, causing billions of dollars of damage." http://www.iwar.org.uk/cyberterror/resources/cyberplanning/alqaeda.htm • **Denial of Service attack on Estonia** Estonian attack see Spears: spearb7@mac.com • **Oak Ridge National Laboratory attack 12/7/07** http://www.industrialdefender.com/general_downloads/incidents/2007.12.07_hackers_launch_major_attack_on_us_military_labs.pdf
Cyber → Corporeal ▪ Covert Communications ▪ Planning ▪ Recruitment & Training ▪ Fundraising ▪ Intelligence Gathering ▪ Training	• **Alneda.com** "which US officials said contained encrypted information to direct al Qaeda members to more secure sites, featured international news on al Qaeda, and published articles, fatwas (decisions on applying Muslim law), and books." http://www.iwar.org.uk/cyberterror/resources/cyberplanning/al-qaeda.htm • **Google maps** http://maps.google.com/maps?q=3601+Wilson+Blvd&ie=UTF8&oe=utf8&client=firefox-a&hl=en&near=Arlington,+VA+22201&f=l • **The Web of Jihad: Strategic Utility and Tactical Weakness** "Eyes-on surveillance is priceless." http://www.stratfor.com/web_jihad_strategic_utility_and_tactical_weakness • **Steganography** Conway, M. 2004. "Code Wars: Steganography, Signals Intelligence and terrorism." Technology and Terrorism.
Corporeal → Cyber	• **Destruction of equipment needed to connect to cyber and media world:** Example of government doing this: http://www.nytimes.com/2006/08/15/world/middleeast/15briefs-004.html?_r=1&oref+slogin

Table 1: Examples of recent actions of VNSAs via cyber-psychological, cyber-cyber, cyber-corporeal, and corporeal-cyber means (Asal et al, 2008).

This chapter focuses on the cyber-psychological and cyber-corporeal connections, and the following sections further elaborate on the use of cyberspace by VNSA to disseminate propaganda, recruit members, create publicity, collect and share data, network, plan, coordinate, raise funds, and wage psychological warfare (Weimann, 2004).

Psychological Warfare

Terrorists wage psychological warfare in cyberspace by spreading disinformation, delivering threats, and posting horrific images of violence, such as the video of the brutal murder of kidnapped American journalist Daniel Pearl that was posted on several terrorist websites. This type of warfare can generate fear in both cyber and corporeal spaces. "Cyberfear" (Weimann, 2004) surrounds the concern over what an attack on computer infrastructures can do, such as the denial-of-service attacks on Estonia in April of 2007 that forced Internet security experts to cut off all Internet access in the country (Kirk, 2007). Threats originating in cyberspace can have a very real effect in the corporeal world as well. Since the attacks on Sept. 11, 2001, Al Qaeda has been using the Internet to create and fuel a "widespread sense of dread and insecurity throughout the world and especially in the United States" by posting announcements on their websites that allude to plans for another "large-scale attack" on the US (Weimann, 2004).

Publicity, Propaganda, and Recruitment

Before the Internet, the only means of generating publicity and disseminating information to a large audience was through traditional outlets such as television, radio, and print media, forums which have little interest in furthering the cause of known terrorists. The Internet provides these groups with unlimited time and freedom to express their ideologies as they choose, in the process shaping how the world sees them and their enemies (Weimann, 2004). According to the Weimann report (Weimann, 2004), most terrorist sites do not celebrate their group's violent actions. Instead, the majority call attention to restrictions they feel have been placed on their freedom of expression, and invoke sympathy for comrades that are political prisoners or who have sacrificed their lives for the cause (Weimann, 2004). It is theorized that this methodology is tuned to resonate with Western audiences, who "cherish freedom of expression and frown on measures to silence political opposition" (Weimann, 2004). The majority of sites also attempt to justify their use of violence by claiming that a weak, oppressed organization, such as theirs, has no other recourse but to turn to violence. They also tend to refer to themselves as "freedom fighters," and couch their ideologies and methods as a means of "regain[ing] the dignity of their people" from the oppressors (Weimann, 2004). Through the use of persuasive audio/video media items, the groups seek to recruit supporters, and they will troll online chat rooms and cybercafés looking for interested parties who might be willing to take a more active role in the organization.

Data Collection and Sharing

According to former Secretary of Defense Donald Rumsfeld, "an Al Qaeda training manual recovered in Afghanistan tells its readers [that by] using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all the information required about the enemy" (Weimann, 2004). This statement speaks to the potentially key role cyberspace plays in the investigation of targets and planning of attacks by terrorists. Information

about nuclear power plants, public buildings, and airports is easily accessible on the Internet, and with programs such as GoogleEarth, high definition reconnaissance images can be viewed from any computer. In terms of the technical knowledge required to create a chemical or explosive weapon, the Internet contains dozens of sites that provide homemade "recipes" for such devices, in addition to the more well-known manuals such as *The Terrorist's Handbook* and *The Anarchist Cookbook* (Weimann, 2004).

Networking, Planning, and Coordination

Terrorist networks are becoming increasingly decentralized, and are now primarily composed of semi-independent cells that have little discernable hierarchy. The Internet provides the means by which these loosely connected groups can communicate quickly, cheaply, and anonymously, and thus it is used heavily to plan attacks. For example, the Al Qaeda members responsible for 9/11 communicated with each other via thousands of encrypted messages posted in a password protected area of a website. These messages were recovered from the computer of Abu Zubaydah, the alleged mastermind of the attacks. The operatives maintained their Internet anonymity by using public Internet cafes and e-mail sources. Steganography, an encryption method that hides messages inside graphics files, is also used to disguise instructions involving maps, photographs, directions, and technical documents (Weimann, 2004).

Fundraising

VNSA groups use the Internet to generate funds through legal and illegal means. Frequently they will ask for donations directly from their websites or offer an online store that sells items such as books, T-shirts, and bumper stickers supporting their causes (Conway, 2006). Exploitation of charities is another common fundraising scheme. In several instances, fake charities have been established that purport to represent a humanitarian cause, when in reality they are fronts that funnel the donated money to terrorist organizations. In December 2001, the US government seized the assets of a Texas based charity called the Holy Land Foundation for Relief and Development when it was discovered that its funds were being diverted to Hamas (Weimann, 2004). The government also froze the assets of the Benevolence International Foundation, the Global Relief Foundation, and the Al-Haramain Foundation, three sham charities that had funneled money to Al Qaeda (Weimann, 2004).

According to Weimann, a great deal of attention has been paid to the "exaggerated threat of cyberterrorism," overlooking "the more routine uses of the Internet" by violent non-state actor groups. He asserts that "it is imperative that security agencies continue to improve their ability to study and monitor terrorist activities on the Internet and explore measures to limit the usability of this medium by modern terrorists." The modeling techniques discussed below attempt to address these issues by creating a picture of the emergent behavior of violent non-state actors in cyberspace through the use of state-of-the-art data collection, data analysis, and predictive modeling techniques.

Overview: Data Collection, Data Analysis, and Predictive Modeling

The daunting task of modeling the emergent behavior of violent non-state actors in cyberspace requires a massive, multidisciplinary effort that combines technology and perspectives from the

fields of data collection, data mining and analysis, and predictive modeling. Each approach contributes a piece to the puzzle, and the integration of these techniques creates a cohesive approach to the problem. Figure 2 illustrates the relationships among these components and their place in the sequence of the overarching modeling process.

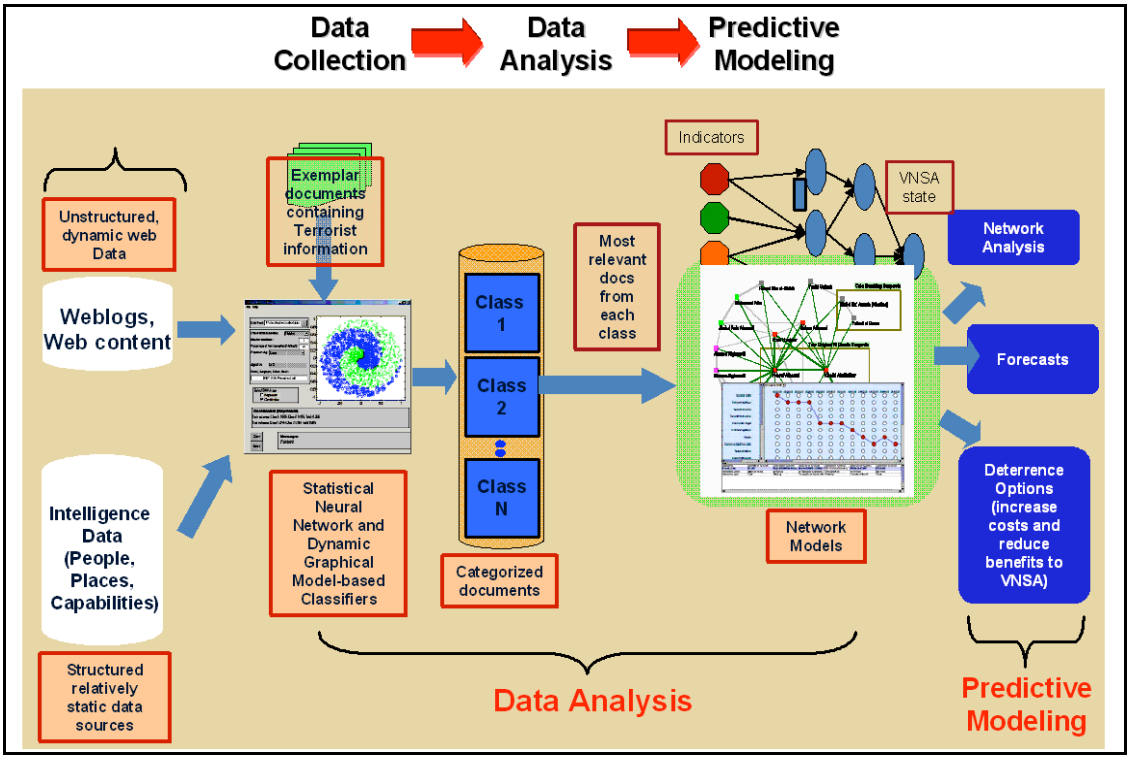


Figure 2: The integration of data collection, data analysis, and predictive modeling techniques creates a cohesive approach to the problem of modeling the emergent behavior of VNSAs in cyberspace (Asal et al, 2008).

Automated data collection techniques address the technical issues of extracting meaningful, relevant, usable information from the seemingly limitless datasets that constitute the cyberspace. The methodology must be able to locate a "needle-in-a-haystack", since the activity is often intentionally obscured, scattered across many sites, and frequently moved or removed. However, without the kind of content-rich datasets that automated data collection techniques can provide, modeling is cumbersome and time-consuming, if not infeasible.

Once a raw dataset is available, data mining and analysis techniques can be applied with the goal of extracting usable knowledge from the data. The results of these analyses often generate the datasets that inform predictive models. The field has been heavily researched, and consequently there are many types of data mining and analysis techniques well-suited to counter-terrorism applications and numerous studies have been conducted to evaluate their effectiveness. Some of the techniques discussed in this chapter include link and social network analysis, automated classification of Web content by machine learning techniques, and a qualitative assessment of the technical sophistication, Web interactivity, and content-richness of terrorist sites on the Internet.

Predictive modeling is the final piece of the puzzle. Modeling techniques rely on the knowledge extracted by data mining techniques to identify discernible patterns of behavior that have the potential to assist analysts with situational assessment, forecasting, and deterrence strategies (Asal et al, 2008). The results of applying these techniques to the counter-terrorism domain provide analysts with information that may not have been readily apparent, potentially influencing strategic decision-making. In addition, predictive modeling can be used to simulate the impact of various counter-terrorism strategies on covert networks. The modeling techniques discussed in this chapter include the use of hidden Markov models and dynamic Bayesian networks to detect, track, and counteract terrorist networks, and agent-based techniques for assessing terrorist network destabilization strategies. An elaboration of each of the three elements described above follows.

Data Collection and the Dark Web

Researchers at the University of Arizona's Artificial Intelligence Lab, headed by Professor Hsinchun Chen, have undertaken the task of mining the so-called 'Dark Web,' a moniker describing the cyberspace equivalent of clandestine back-alley meetings, recruitment efforts, and propaganda dissemination by VNSAs. Using a systematic web-mining approach, the Dark Web Project tackles the "needle-in-a-haystack" search for the covert movements and communication patterns of extremist and terrorist groups in cyberspace, providing researchers with the kind of content-rich datasets that can inform various analysis and predictive modeling techniques.

The data collection process utilizes a semi-automated Web spidering technique, which offers a significant increase in efficiency over manual collection methods (Zhou et al, 2006). The process begins with the identification of extremist groups and a seed batch of Web sites based on information provided by authoritative outside sources, such as the US State Department and the UN Security Council reports, and studies published by private terrorism research centers. Information on these entities, such as group and leader names, and group-specific jargon are manually compiled to create a keyword lexicon that is used to query major search engines for additional content. The set of seed sites, consisting of those identified by outside sources and the manual lexicon queries, is expanded by extracting their out-links and back-links. The spider collects the complete contents of the target sites, including all Web page text, hyperlinks, multimedia content, and available attachments (Zhou et al, 2006). Currently, the Web site collection consists of the complete contents of 1,000 sites, and partial information from approximately 10,000 linked sites (Univ. of Arizona, 2008).

Additionally, the researchers collected the complete contents of forums containing extremist/ terrorist content that have been identified in the manner described above. Forums are of particular interest, since they are a public communication medium uniquely suited to the propagation of ideas in a dynamic way. The content collected from the forums can offer insight into the real-time communication patterns of NSAs in cyberspace, as well as potentially identify developing trends and sympathizers (Qin et al, 2007). Encrypted or password protected forum content is a particularly significant finding for obvious reasons. In such cases, membership to the forum as a "curious neophyte" is requested manually, giving the spider access to this content (Qin et al, 2007). Researchers collected the complete contents of 300 terrorist forums, including authors, headings, postings, threads, time-tags, and any attached media (Univ. of Arizona, 2008).

The Dark Web Collection currently contains about 2 TB of extremist/terrorist related content from 500,000,000 pages, files, and postings from over 10,000 sites in Arabic, Spanish, and English. New Web-content is collected every 2 to 3 months. The researchers believe that the "Dark Web collection is the largest open-source extremist and terrorist collection in the academic world," and are currently developing a multi-lingual knowledge management system called the 'Dark Web Portal' that will provide efficient access to the Dark Web Collection (Univ. of Arizona, 2008). The Portal utilizes document summarization, categorization, and visualization techniques to allow users to quickly locate the information they seek (Zhou et al, 2005).

Data Mining and Data Analysis

A step beyond the collection of a content-rich raw dataset, exemplified by the Dark Web collection, is the extraction of useful knowledge from this data through data mining and automated data analysis techniques (Jensen, 2003). Data mining identifies predictive patterns in the raw dataset which can be used by automated data analysis applications to "find previously unknown knowledge through links, associations, and patterns" in the data (Jensen, 2003). Automated data analysis techniques can be broadly classified as either subject-based or pattern-based. For subject-based queries, analysis begins with knowledge of the subject, such as a suspicious individual, place, or phone number identified by authoritative intelligence sources. Subject-based queries seek additional information that will provide a broader understanding of the subject, such as activities an individual has engaged in and links to people, places, and things with which they are familiar (DeRosa, 2004). Link and social network analysis are subject-based query techniques that have been widely used both in the public and private sectors, and they have significant potential to be a useful weapon in the counter-terrorism arsenal (DeRosa, 2004). Several examples of the application of link/social network analysis to the counter-terrorism domain are described below, including a hyperlink interconnectivity analysis of Jihadi communities on the Internet, and the social network mapping of the Al Qaeda cell responsible for the 9/11 attacks.

Pattern-based queries seek to identify pre-defined patterns of behavior within datasets, and the models can come from data mining techniques or other intelligence sources (DeRosa, 2004). Perhaps the most well-known example of pattern-based searching in the private-sector is its use by credit-card companies to detect fraud. The banks create a model of fraudulent activity by searching databases that are known to contain a combination of valid and invalid transactions. An example of such a pattern would be for the thief to make a small purchase with the stolen card to confirm that it works, immediately before making a substantial purchase (Jonas, 2003). The bank monitors all credit card transactions for instances of fraudulent patterns, and issues an alarm if one is detected. For a case such as this, the bank is looking for a broad pattern in unrelated financial transaction data. This methodology does not generalize to the domain of terrorist activity, however. There is no broad pattern of activity associated with terrorist organizations; they tend to be loosely connected semi-autonomous cells, and it is the "relational" data describing the connections between people, places, and things that are of importance (DeRosa, 2004). Several examples of the application of the pattern-based methodology to the counter-terrorism domain are described below, including content-based monitoring of Web browsing behavior, automatic classification of Web content, and authorship identification of anonymous documents.

Data Analysis: Link/Social Network Analysis

The researchers at the University of Arizona, who are responsible for the Dark Web Collection, have been analyzing the data set from several different perspectives, including link/social network analysis. Using the Dark Web collection methodology, they studied Jihadi communities on the Internet in an effort to better understand how these groups interact and communicate in cyberspace. The data collection process began with three Jihad seed Web sites: www.qudsway.com of the Palestinian Islamic Jihad, www.hizbollah.com of Hizbollah, and www.ezzedine.net of the Izzedine-Al-Qassam, the military wing of Hamas (Reid et al, 2005). The Google back-link search service was used to find all the sites linked to the initial three, and after performing manual keyword lexicon searches to expand the set and filtering to remove outliers, a testbed of 39 sites remained. Web spidering collected approximately 300,000 documents from these sites and those linked to them. In order to identify hidden communities, a similarity measure was computed between all website pairs based on the number of hyperlinks shared between the sites. The hyperlinks were weighted proportionally according to how deeply they are embedded within a site, with the most weight given to links available from homepages.

A multidimensional scaling (MDS) algorithm (Duda et al, 2001) was used to generate a two-dimensional graph of the link structure, from which clusters representing highly-linked communities were extracted. Six main clusters were identified, and the results conform to what has already been established regarding the relationship among these groups (see Figure 3).

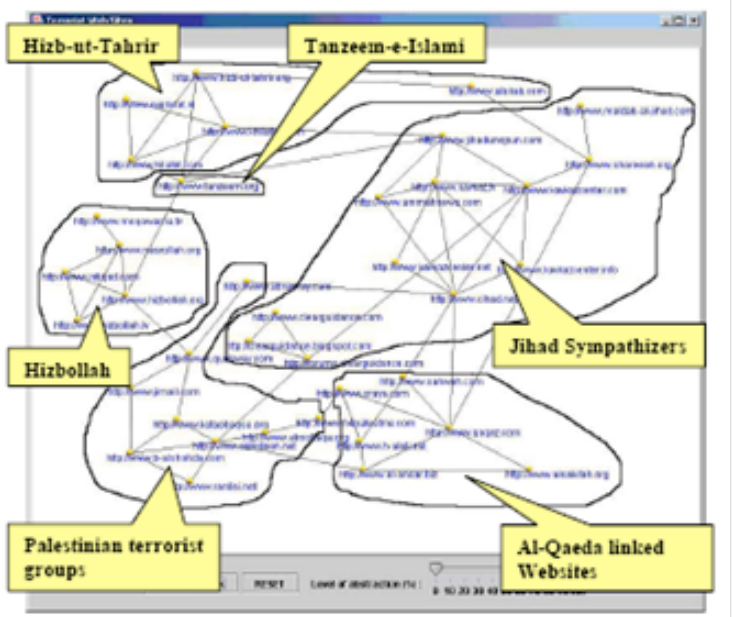


Figure 3: 2D graph of the link structure of hyperlinked Jihadi communities on the Web (Reid et al, 2005).

For example, the figure indicates a strong link between the Hizbollah cluster and Palestinian organizations, which is not surprising since Hizbollah is a known sympathizer with the Palestinian cause. At the top-left portion of the graph is the Hizb-ut-Tahrir political party cluster. While not officially recognized as a terrorist group, the results indicate that they have links to the Hizbollah cluster. The demonstrated link between the Al Qaeda and Hamas clusters

was also expected. While this particular study did not produce any results that do not mesh with the current sociological and ideological understanding of the relationships between the Jihadi groups studied, it is possible that this type of link/social network investigation will provide analysts with the ability to identify relationships between organizations and individuals that they might not have otherwise seen, and to allow them to monitor the development of these relationships over time.

Another example of the use of link/social network analysis for terrorism related applications is the work of Valdis Krebs on mapping the structure of the covert network of Al Qaeda members responsible for the Sept. 11th attacks. Krebs used publicly available data from news sources on the Internet to visually represent the social relationships among the 19 individuals identified as hijackers, as well as their relationships with co-conspirators who provided knowledge, money, and skills to the effort, but did not board the planes (Krebs, 2002). Because Krebs relied on publicly released news reports as his data source, his analysis was ill-informed since the amount of relevant relationship information released to the media was limited or intentionally incorrect. To counteract this, he applied the work of social network theorists such as Malcolm Sparrow who study the structure of covert networks under the conditions of missing information, fuzzy node inclusion criteria, and consistently dynamic datasets. Krebs decided to map the strength of the relationships between the key players in terms of how much time they spent together, with the strongest ties belonging to individuals who attended the same school or training programs: the resulting map can be seen in Figure 4.

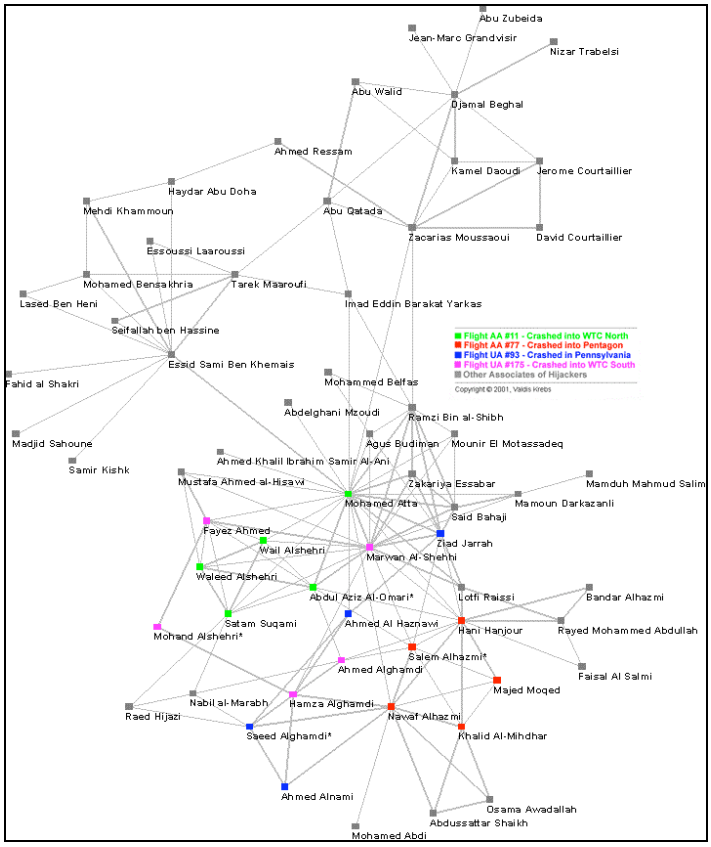


Figure 4: Link analysis of the 19 hijackers and co-conspirators responsible for 9/11. Analysis was done by Valdis E. Krebs using open source news data (Krebs, 2002).

Additionally, attributes of network centrality were computed for each individual, including Degree, Closeness, and Betweenness. The Degree attribute indicates the node's level of activity in the network; Closeness is a measure of the node's ability to access others and monitor ongoing events, and Betweenness describes the node's ability to control the flow of communication in the network (Krebs, 2002). Krebs' analysis of the network structure revealed Mohamed Atta to be the most likely ring leader of the group, since he obtained the highest score of all participants for each of the centrality attributes described above. This result has been confirmed many times over by intelligence experts, and by bin Laden himself, who verified Atta's leadership role in a video tape (U.S. Department of Defense, 2001).

While not directly illustrative of how link/social network analysis has been used to model the emergent behavior of VNSAs in cyberspace, the Krebs example demonstrates both the potential and limitations of using link/social network analysis for such an application. With the benefit of hindsight in this case, it is natural to ask the question: Given the amount of information that was available prior to the 9/11 attacks, could we have predicted and prevented them had we simply known how and where to look? According to the National Commission on Terrorist Attacks upon the United States, the government may have been able to prevent the tragedies had they pursued leads that were available to them at the time (Jonas and Harper, 2006). This finding does not imply, however, that techniques such as link and social network analysis can be used to reveal the structure of any and all covert VNSA organizations. Krebs asserts that uncovering covert criminal networks is an extremely difficult task, since their behavior is so unlike that of a normal social network. In the case of the 9/11 hijackers, the strong ties between nodes that were "formed years ago in school and training camps…remain[ed] mostly dormant and therefore hidden to outsiders," unlike normal social networks (Krebs, 2002). The lack of transparent connections among group members, coupled with the self-imposed isolation of network members from the outside world make social network analysis a blunt instrument when it comes to its predictive and preventive capabilities. Krebs cautions that "we must be careful of 'guilt by association'. Being linked to a terrorist does not prove guilt - but it does invite investigation," making social network analysis more aptly applied to "the prosecution, not the prevention of criminal activities" (Krebs, 2002).

Data Analysis: Web Monitoring

Law enforcement agencies have been interested in monitoring the Internet activity of suspicious individuals ever since the emergence of the Internet as a standard communication medium in the 1990s. Programs such as Carnivore provided the FBI with the ability to monitor specific types of electronic communication described explicitly by a court order, such as e-mails and browsing records. The architecture of the Carnivore system consisted of a Windows-based computer installed at an ISP with a 1-way tap into the Ethernet segment to which it is attached. The computer filters the packet traffic and stores those packets that conform to filter specifications defined by the court-order. Restrictions on packet collection ranged from permission to access the full contents of communication to only address information, such as To and From e-mail addresses and IP addresses involved in FTP and HTTP sessions (Smith et al, 2000). The data was mined for information at a later time.

The FBI discontinued the Carnivore program (since renamed DCS1000) several years ago; however, the Carnivore methodology is exemplary of most electronic communication

surveillance protocols in use today. That is, a mass of data conforming to certain content parameters is collected and analyzed later using various data mining and analysis techniques. Researchers at Ben-Gurion University of the Negev, Israel, propose a new methodology and objective for monitoring these electronic communications based on real-time surveillance of users' browsing behavior. They have developed a content-based model for classifying and identifying browsing activity called the Advanced Terror Detection System (ATDS), which they have applied specifically to the identification of behavior that conforms to a "typical terrorist signature".

The underlying assumption of the ATDS is that the content of a user's Web browsing behavior can be used to create a signature of interest that can be compared to a pre-classified set of signatures, such as one that might describe "typical terrorist" or normal Internet usage (Shapira, 2005). The method begins with a learning phase, during which the system is provided with a set of Web pages representing the browsing behavior of a "normal" set of users. Each document browsed is converted to a vector of weighted terms, where the weighting criteria corresponds to the relative frequency with which the term appears on the page and the term's position, i.e. if the term is found in the page title, it is assigned a higher weight, since its contribution to the document's content is assumed to be higher. A cluster-generator receives the vectors and performs cluster analysis on the data, identifying discrete areas of interest based on the frequency of the weighted terms across the set of vectors derived from the user's browsing session. These discrete areas of interest are the centroids of the cluster, and they are the elements that make up the set of normal user's browsing interests (Elovici et al, 2005).

The monitoring process consists of an on-line packet sniffer, which captures the data sent and accessed by a group of users at a network level, much like the Carnivore system. The packets are sent to a filter which excludes pages without any textual content from further analysis. Each text item is vectorized and compared to the centroids of the normal user signature using the Cosine method of computing the distance between vectors. If the distance between the monitored page vectors and any of the centroids is higher than the dissimilarity threshold, the user has demonstrated an interest that is not reflected in the set of normal user interests, possibly signifying abnormal browsing behavior. Whether or not an alarm is raised depends on parameter choices such as the sensitivity of the dissimilarity threshold, and the number of "normal" pages required to classify the overall browsing behavior as normal (Elovici et al, 2005).

Researchers evaluated the performance of the ATDS by monitoring 38 computer stations in a teaching lab for one month from which they collected 13,300 English pages corresponding to what would be considered "normal" browsing behavior. They also collected 582 terror-related pages for the simulation of an abnormal sequence of accesses, and chose a random 582 pages from the normal set, which they used to simulate the normal browsing behavior. The system was evaluated to determine the optimal alarm thresholds and queue size of pages to monitor. Queue size of 2, 8, 16, and 32 pages were tested for alarm thresholds of 50% and 100% of the queue having dissimilar interests to the normal profile. The system reached almost ideal performance for a 32 page queue and 100% alarm threshold (Elovici et al, 2005).

The researchers assert that the intention of the ATDS is to aid law enforcement officials in tracking down suspected terrorists based on the content of their Web browsing. They envision that the system would run in real-time and would be able to monitor a large group of users

simultaneously without being detected. Ideally, officials would also have access to individuals' identification information based on their IP addresses, which would require the cooperation of the ISPs or a court-order (Shapira, 2005). The scalability of this technique is potentially an issue, since each Web page has to be vectorized and compared in near real-time; this may not be feasible for monitoring large groups (Shapira, 2005). Additionally, researchers have yet to evaluate the methodology with a testbed of Web pages that mixes normal and abnormal page accesses, which would more accurately reflect the usage patterns of a real individual (Elovici et al, 2005). Currently, no new data have been published that address these issues.

While the full capabilities of the ATDS have not yet been fully investigated, the underlying concept provides a new idea about what Web monitoring can mean and introduces a framework indicating that it may be possible to achieve real-time monitoring of Web-content. Much future work is needed, however, to establish this type of methodology as a technique that can feasibly be used by law enforcement officials to identify suspicious individuals with minimal numbers of false positives.

Data Analysis: Automatic Content Classification

The investigation of emergent behavior of VNSAs in cyberspace is a problem that is confounded not only by the difficult task of obtaining a clean, relevant dataset, but also by the sheer volume of data that is available. Raw data requires pruning to isolate terror-related content, and manual sorting techniques are simply not efficient enough to handle data sets of the magnitude of the 2-TB Dark Web collection. Automatic classification of Web content is currently being investigated as a means of addressing this problem. Classification techniques are typically applied to a "function that has a discrete set of possible values," and the algorithms have the goal of automatically identifying which of these values describe a previously unclassified piece of data (Last, 2005). The discrete values can be any number of properties, as long as there is a way to quantify the presence or absence of the property within the data in question, making classification algorithms applicable to a broad range of problems. The type of data to be classified determines the appropriate method of classification. For example, the most general classification models are based on a decision-tree methodology to represent the conditional dependence between inputs. The branches of a decision tree "can be interpreted as *if-then* rules of varying complexity," and traversing the branches of the tree applies the rules of the model to each new piece of data. Examples of decision-tree based algorithms are C4.5 and ID3. Other pattern recognition approaches utilize Probabilistic Neural Networks (PNN), Bayesian learning methods, Support Vector Machines (SVM), Principle Component Analysis (PCA), Gaussian Mixture Models (GMM), K-nearest neighbor (KNN) algorithms, and linear and quadratic discriminants (Duda et al, 2001), (Bishop, 2006). An in-depth discussion of these techniques is beyond the scope of this report.

In the counter-terrorism domain, the automatic classification of Web content as terror-related or not is perhaps the most straightforward type of classification problem, since it has only two possible outcomes. The application of classification algorithms to Web content is not so straightforward, however, and a significant component of the analysis process resides in manipulating the data into a form that is friendly to the preferred algorithms. Researchers at Ben-Gurion University of the Negev, Israel, have tackled this problem using a graph-based classification technique with the goal of automatically recognizing terror-related websites in

English and Arabic (Markov and Last, 2005). Their technique translates the textual HTML content of a Web page into a graph where each node is a unique keyword and the connections between the nodes describe their position relative to each other and location in the document (title, link, text). Figure 5 depicts a CNN news page and its corresponding graphical representation. This representation of the document is an alternative to the vector representation utilized by the content-based Web monitoring methodology described above, and the technique was chosen because it captures the inherent structural information of the original document, such as order, proximity, and location of terms (Markov and Last, 2005).

Iraq bomb: Four dead, 110 wounded

A car bomb has exploded outside a popular Baghdad restaurant, killing three Iraqis and wounding more than 110 others, police officials said. Earlier an aide to the office of Iraqi Prime Minister Ibrahim al-Jaafari and his driver were killed in a drive-by shooting.

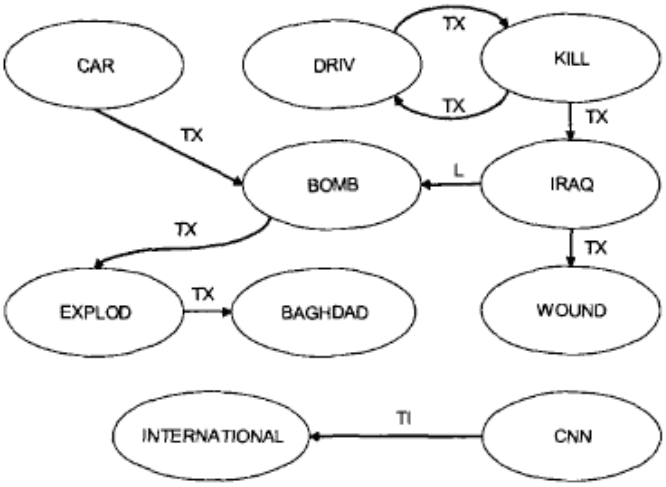


Figure 5: Left: CNN News page used as part of the automatic content classification methodology described above. **Above:** Corresponding graphical representation (Markov and Last, 2005).

The classification process begins with a training set of pre-classified Web documents and their corresponding graph models. Sub-graphs representing the key concepts of the document are extracted from the larger graph using the *Smart* and *Naïve* extraction algorithms (Markov and Last, 2005). The sub-graphs are analogous to the centroids of Internet browsing interests described in the content-based Web monitoring methodology. Previously unclassified documents are processed similarly and their sub-graphs are compared with the training data. The algorithms that can compute the similarity between classified and unclassified content directly from their graphical representations, such as the K-Nearest Neighbor (KNN) algorithm, are computationally intensive and therefore not suitable for real-time classification of large amounts of Web content. Accordingly, the researchers converted the unseen graphs to vectors of Boolean features where a "1" represents the presence of a sub-graph that matches the training data. Many different classification models can be applied to data in this type of vector format, such as neuro-fuzzy networks, artificial neural networks, the Naïve Bayes, SVM, decision tree (C4.5, ID3), and PNN Classifiers.

The researchers tested this methodology on 648 manually collected Arabic Web documents, 200 of which were pre-classified as "terrorist-related" and 448 as "non-terrorist." They used the ID3 decision tree classifier algorithm and tested the technique to determine the optimal number of nodes per graph, classification rate threshold, and sub-graph extraction algorithm. The results

can be seen in Figure 6. The most accurate classification results were obtained using the *Smart* sub-graph extraction technique on 100 node graphs. Nine documents were classified incorrectly; five non-terrorist sites were classified as "terrorist", and four "terrorist" sites were missed (Markov and Last, 2005). While the testbed of this study was relatively small, the results indicate the potential for this technology to be successfully applied to much larger datasets.

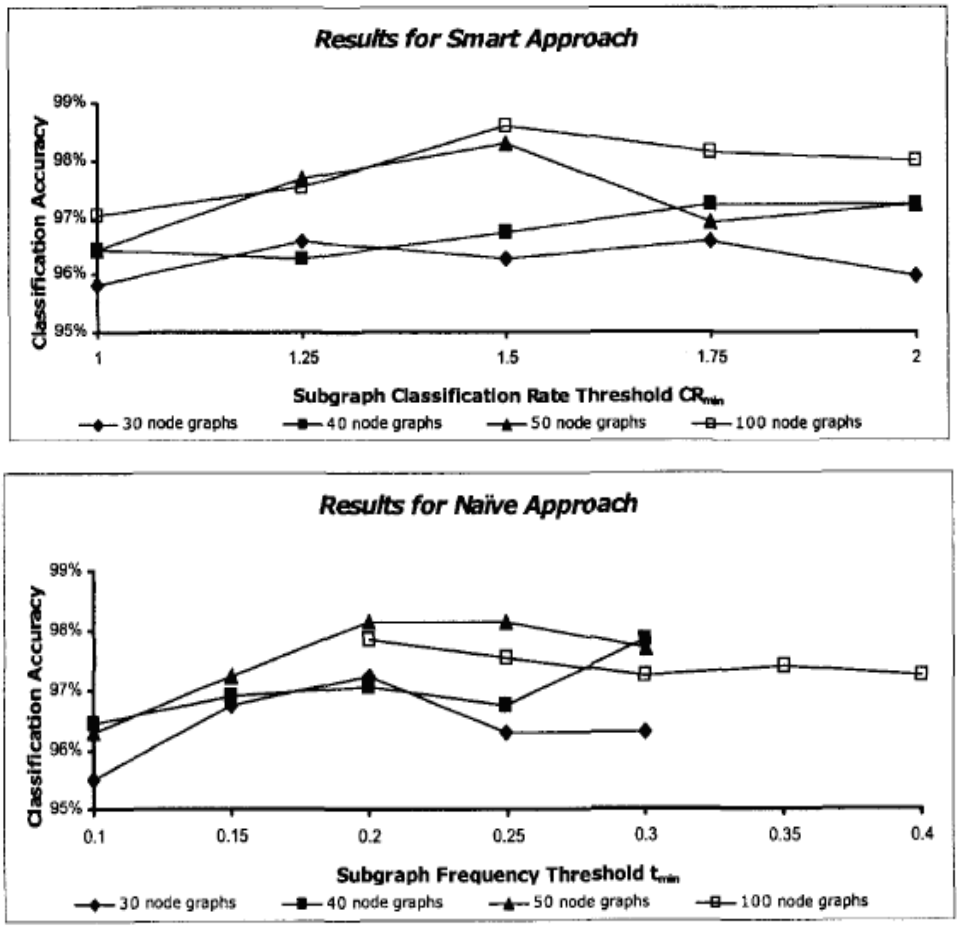


Figure 6: Results for *Naïve* and *Smart* sub-graph extraction techniques of Arabic Web documents. The most accurate classification results were obtained using the *Smart* sub-graph extraction technique on 100 node graphs (Markov and Last, 2005).

Data Analysis: Authorship Identification

Communication channels such as forum postings, chat room dialog, and email offer a fast, inexpensive, and largely anonymous way to reach millions, making them an ideal communication method for VNSAs who wish to namelessly disseminate extremist propaganda. The application of authorship analysis techniques to this type of data can offer insights into the character and identity of the creator of an anonymous textual document. Characterization techniques "attempt to formulate an author profile by making inferences about gender, education, and cultural backgrounds on the basis of writing style," while identification is a classification task that has the goal of assigning authorship to an anonymous document based on a stylistic comparison with previously classified documents (Abbasi and Chen, 2005).

The linguistic discipline of stylometry is the basis for most authorship analyses (Abbasi and Chen, 2005). The stylometric methodology applies statistical analysis techniques to a textual document, with the goal of extracting features that are indicative of the author's unique writing style. This feature set can then be compared to documents with confirmed authorship that have been evaluated in a similar manner. There are four major categories of stylistic features that are the focus of such an analysis: lexical, syntactic, structural, and content-specific. A lexical feature breakdown contains information, such as word frequency, number of words per sentence, total number of characters, and characters per sentence.

Certain generalizations about the author's writing style can be made from a lexical analysis. For example, the inclusion of a large number of relatively long words can indicate that the author has a large vocabulary and a more complex writing style. Syntax features refer to the order and pattern of words used to construct a sentence, which can be established through punctuation and the use of "function words" such as *while* and *upon* (Abbasi and Chen, 2005). An example of a syntactical signature would be an author's consistent choice to use the word *thus* instead of *hence* in the same context. A document's structural features, such as the layout of the text, structure of greetings, number of paragraphs, and average paragraph length, and the use of content-specific words are also of interest in a stylometric analysis. For example, in a forum where the topic of discussion is computers, an author's use of the content-specific word *RAM* as opposed to *memory* is a distinguishing writing style characteristic.

As part of the Dark Web project, researchers at the University of Arizona have applied authorship identification techniques to English and Arabic Web forum postings collected using the spidering methodology described previously. The testbed for the study consisted of 20 Web forum messages for each of 20 authors, for a total of 400 messages per language. The English forum texts were downloaded from sites associated with the White Knights of the Ku Klux Klan, and the Arabic messages were collected from strongly anti-American forums associated with the Palestinian Al-Aqsa Martyrs Brigade. The researchers had to adapt traditional authorship identification techniques, which were developed for use on literary texts, to the personality of Web forum texts. The latter tend to be shorter and more informal, and contain a substantial amount of misspellings and abbreviations. The large number of potential authors further limited the efficacy of traditional techniques for this application.

Extracting features from the Arabic text posed additional challenges due to the language's morphological characteristics. In particular, the diacritics that mark phonetic values in Arabic words are rarely used in online communication, which confounds feature extraction algorithms based on a methodology designed for English documents. In addition, Arabic words are shorter, which limits the usefulness of the text's lexical information for establishing a unique writing style. For example, longer words in English documents indicate a more complex writing style, but this generalization does not translate to Arabic documents.

The researchers resolved these issues by implementing separate feature extraction methodologies developed specifically for Arabic and English text. In addition, the problems posed by the short, noisy nature of forum text were offset by the availability of data that is unique to Web content, such as the presence of hyperlinks and embedded images, font size and color choice, greeting structure, and in some cases contact information. This information expanded the breadth of the

structural features category and further informed the classification techniques that were used to identify authorship (Abbasi and Chen, 2005).

After automatic feature extraction, classification algorithms were applied to the data in order to identify authorship based on comparison with pre-classified feature sets. The researchers experimented with two different machine learning classification algorithms: C4.5 and Support Vector Machines (SVM). The C4.5 technique is a decision-tree based algorithm chosen because of the ease with which decision trees can be visualized. SVM was chosen because it is a computational learning method that can handle noisy data. The study produced results that pleasantly surprised the researchers, especially in light of the results obtained by Zheng *et al*. (Zheng et al., 2005), Peng *et al*. (Peng, et al., 2003), and Stamatatos *et al.* (Stamatatos et al, 2001) in previous authorship attribution studies (Abbasi and Chen, 2005).

The SVM classification technique produced the best results for both languages, achieving 97.00% accuracy for English and 94.83% for Arabic when all four feature categories were incorporated into the analysis. Using this multilingual methodology, the group plans to investigate the scalability of the technique for application to a much larger group of potential authors. In addition, they plan to perform a more comprehensive analysis of the English and Arabic feature sets across texts to see if some of the attributes, such as the use of persuasive or violent language, are indicative of a stylistic signature of the group as a whole.

Data Analysis: Qualitative Content Analysis

The majority of content analysis techniques that have been applied to the study of the behavior of VNSAs in cyberspace are quantitative in nature. The classification techniques described above are representative of approaches, where the goal of the analysis is to automate the process of identifying terrorism-related content within a dataset by comparing it to a "terrorist-content" template of some kind. This type of analysis does not address the qualitative properties of the data, however, which is a perspective that is being investigated by the researchers from the University of Arizona responsible for the Dark Web collection. Using a dataset collected by the semi-automated spidering methodology described above, they used quantitative methods to study qualitative attributes of the dataset, including technical sophistication, content richness, and Web interactivity, with the goal of gaining insight into the level of advancement and effectiveness of terrorists' use of the Internet (Qin et al, 2007). The researchers also performed a benchmark comparison of the terrorist/extremist sites to US government sites, which have been identified as the top in the world in terms of Web technical sophistication and interactivity by the CyPRG group of the University of Arizona (CYPRG, 2008).

The study focused on a qualitative analysis of the Web presence of Islamic terrorist groups rooted in the Middle East, such as Al Qaeda, Palestinian Islamic Jihad, and Hamas. About 220,000 multimedia Web sites and documents were evaluated for 13 technical sophistication attributes, five content richness attributes, and 11 Web-interactivity attributes which compose the so-called Dark Web Attribute System (DWAS).

The level of a site's technical sophistication was measured by its use of basic HTML techniques (lists, tables, frames, and forms), advanced HTML techniques (DHTML/SHTML, predefined and self-defined script functions), and embedded multimedia content, such as background

images, music and streaming of audio/video. In addition, a site's use of dynamic Web programming languages, such as CGI, PHP, and JSP/ASP, for functions such as user login and online transaction processing was also evaluated. As shown in Table 2, each attribute was assigned a weight based on the opinion of Web experts obtained through an email survey (Qin et al, 2007).

Technical Sophistication attributes	**Weights**
Basic HTML techniques	
• Use of lists	1
• Use of tables	2
• Use of frames	2
• Use of forms	1.5
Embedded multimedia	
• Use of background image	1
• Use of background music	2
• Use of stream audio/video	3.5
Advanced HTML	
• Use of DHTML/SHTML	2.5
• Use of predefined script functions	2
• Use of self-defined script functions	4.5
Dynamic web programming	
• Use of CGI	2.5
• Use of PHP	4.5
• Use of JSP/ASP	5.5
Content Richness Attributes	**Scores**
Hyperlink	No. of hyperlinks
File/Software download	No. of downloadable documents
Image	No. of images
Video/audio file	No. of video/audio files
Web Interactivity Attributes	**Weights**
One-to-one interactivity	
• Email feedback	1.75
• Email list	2.25
• Contact address	1.25
• Feedback Form	2.75
• Guest book	1.5
Community-level interactivity	
• Private message	4.25
• Online forum	4.25
• Chat room	4.75
Transaction-level interactivity	
• Online shop	4
• Online payment	4
• Online application form	4

Table 2: List of technical sophistication, content richness, and Web interactivity attributes and corresponding weights (Qin et al, 2007).

The content richness attributes evaluated the variety and volume of information offered by a site, and was measured by the number of hyperlinks and number of downloadable documents, images, and audio/video files it contained. The third attribute category, Web interactivity, evaluated the sites for three types of interactivity: one-to-one level interactivity, community-level interactivity, and transaction level interactivity such as online shops, online payment options, and online application forms that provide functionality for activities such as donating to extremist groups or applying for access to restricted content (Qin et al, 2007).

Attribute information was automatically extracted from the terrorist/extremist dataset and from 277,000 documents collected from US government sites. The results of a statistical analysis of the datasets indicate that US government sites are significantly more advanced in the use of basic HTML techniques to organize the sites and the implementation of dynamic programming languages to provide functions such as user login and online applications. The results also indicate that there is significantly more embedded media available on terrorist sites as compared to the government sites. The researchers believe this to be a significant finding that demonstrates the extent to which the Internet is used by NSA groups as a means of disseminating information.

Since multimedia content is more attractive and leaves a more lasting impression than text, the effort these groups have expended to include such content indicates a desire to make a strong statement to both supporters and enemies. Examples of such content include movie clips of suicide bombing attacks in Iraq posted to online forums, video clips of the beheading of American Nicholas Berg posted on a Malaysian terrorist site, and pictures of executed Iraqi "traitors" who cooperated with US forces (Qin et al, 2007).

The US government sites demonstrate a higher degree of content-richness based on the much larger volume of downloadable multimedia contents they provide. This result seems incongruous with the analysis of embedded media discussed above, but it is actually indicative of the nature of the majority of the terrorist sites investigated. While US government sites are usually hosted on dedicated Web servers, the NSA groups' sites are often hosted by free ISPs, which restrict the sites' size and use of bandwidth. It is theorized that this explains the extra effort expended to include embedded multimedia content as an alternative to downloadable files.

The results of the Web interactivity comparison indicate that the US government sites support significantly more one-to-one level interaction, while the terrorist/extremist groups support much more community-level interaction through online forums, bulletin boards, and chat rooms. This confirms the results of studies that indicate that NSAs are using the Internet as an integral method of communication. Forums such as www.shawati.com and www.kuwaitchat.net have tens of thousands of members and hundreds of thousands of postings, where the members are a mix of NSAs, supporters, and sympathizers. In some cases, forum members can receive regular messages from members of terrorist groups, such as the late terrorist leader Abu Mus'ab Zarqawi in Iraq, who used to post messages directly to the forum www.islamic-f.net.

The results of the statistical analysis of the two data sets demonstrate that although there are significant differences between the US government and terrorist/extremist sites sub-attributes, there is no appreciable difference in the broader categories of technical sophistication, content richness, and Web interactivity. This implies that NSA groups employ the same level of Internet

sophistication as the US government when it comes to communicating with the public (Qin et al, 2007).

The significant volume of forum and chat room postings that were uncovered during the data collection process indicates that they are methods of communication heavily employed by terrorists/extremists, and the authors of the study suggest that security and law-enforcement experts "should pay more attention" to these types of online communication. The researchers continue to pursue this type of qualitative analysis; future research directions include incorporating additional attributes to the DWAS, expanding the analysis to Web sites from other parts of the world, performing a time-series analysis of the Dark Web data, and exploring the use of more advanced machine learning techniques to search for patterns in the media content collected from the sites (Qin et al, 2007).

Predictive Modeling

An adequately informed application of predictive modeling techniques has the potential to provide analysts with situational assessment, forecasting, and deterrence strategies (Asal et al, 2008). Traditionally, a realistic model can only be constructed from a training set of historical records, but (fortunately) terror-related plots are small in number, with "only one or two major terrorist incidents every few years - each one distinct in terms of planning and execution" (Jonas and Harper, 2006). Thus, the models often have to be augmented by input from outside authoritative sources, and rely heavily on hypotheses that are based on historical patterns of behavior. This makes the availability of a clean, content-rich dataset crucial to the success of the model. While they do not specifically model the emergent behavior of VNSAs in cyberspace, the examples that follow are indicative of state-of-the-art research in the application of predictive modeling techniques to the counter-terrorism domain. The models focus on the corporeal behavior of VNSAs; however, they are more well-informed by the inclusion of information regarding their cyberspace activities obtained by the collection and analysis methods described above.

Predictive Modeling: Hidden Markov Models and Bayesian Networks

Researchers at the University of Connecticut are developing a tool for modeling and detecting terrorist networks that can "assist analysts with: 1) identifying terrorist threats; 2) predicting possible terrorist actions; and 3) elucidating ways to counteract terrorist activities" (Allanach et al, 2004). The architecture of the so-called Adaptive Safety Analysis and Monitoring (ASAM) tool "is based on the premise that terrorist networks can be evaluated using transaction-based models" and suspicious links between people, places, and things. For example, a sequence of events (transactions) that may or may not be cause for concern could consist of an individual withdrawing money from the bank, buying chemicals that could be used to create a chemical weapon, and then purchasing a plane ticket to the United States. The ASAM tool models the evolution of such transactions using hidden Markov models (HMMs) and dynamic Bayesian networks (DBNs). An HMM is a type of stochastic signal model used to evaluate the likelihood of a sequence of observations and to infer the most likely sequence of events from a noisy sequence of observations. The model represents the interconnection between a hypothetical series of transactions that lead to the completion of the task that is being modeled. Figure 7 depicts a Markov chain model developed by the researchers to represent a plot by members of Al

Qaeda to execute a truck bombing during the 2004 Olympics in Athens, Greece. There are 9 states in this model and the probability of transition between the states is printed by the edges that connect them (Singh, Allanach et al, 2004). The HMM models are parameterized by the transition probability matrix, emission matrix, and the initial probability vector.

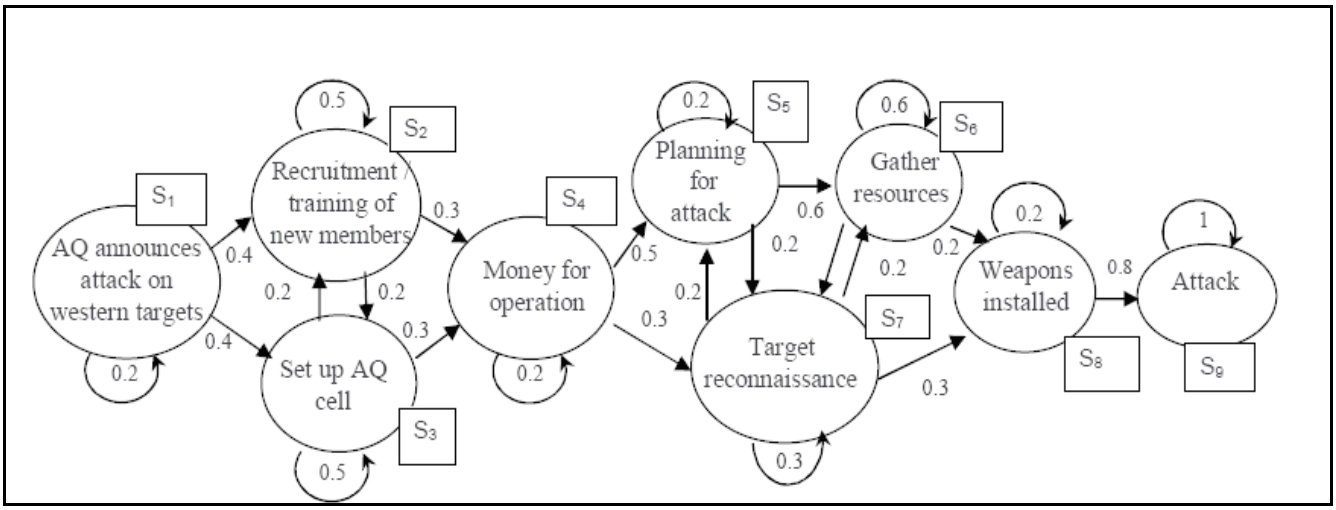


Figure 7: Markov chain representing a hypothetical plot by members of Al Qaeda to execute a truck bombing at the 2004 Olympics in Athens, Greece (Singh, Allanach et al, 2004).

The HMMs are the foundation of the ASAM tool, since they provide the "template models" for potential terrorist activity; new transactional data is compared to these templates as a way of tracking the development of scenarios. In general, if there is enough historical data available, the parameters of the model can be generated automatically from a "learning" algorithm called the Baum-Welch algorithm (Singh, Tu et al, 2004). For counter-terrorism applications, it is nearly impossible to collect adequate historical data to make this approach feasible, so the researchers designed the models and assigned parameters based on the recommendations of intelligence analysts.

The information gathered from the HMMs is reported to probabilistic models that represent larger scale terrorist activities. These overarching plots are represented by dynamic Bayesian networks (DBNs), and the ASAM system utilizes a hierarchy of subordinate dynamic Bayesian networks (sub-DBNs) that report upwards to a final comprehensive DBN that evaluates the overall probability of terrorist activity.

Figure 8 depicts the DBN representing the global threat model for potential terrorist activity at the 2004 Olympics (GeNle 2.0, 2003). Each node in the model represents a terrorist sub-plot that is described by an underlying HMM, and the links between nodes represent direct probabilistic dependencies between the subplots. The conditional probabilities of each node are updated whenever they receive information from their corresponding HMM, and the global threat level at any given time is a function of the current conditional probabilities assigned to each subplot. Simply stated, the global threat level increases as the terrorist groups successfully execute the subplots described by each node in the overarching network.

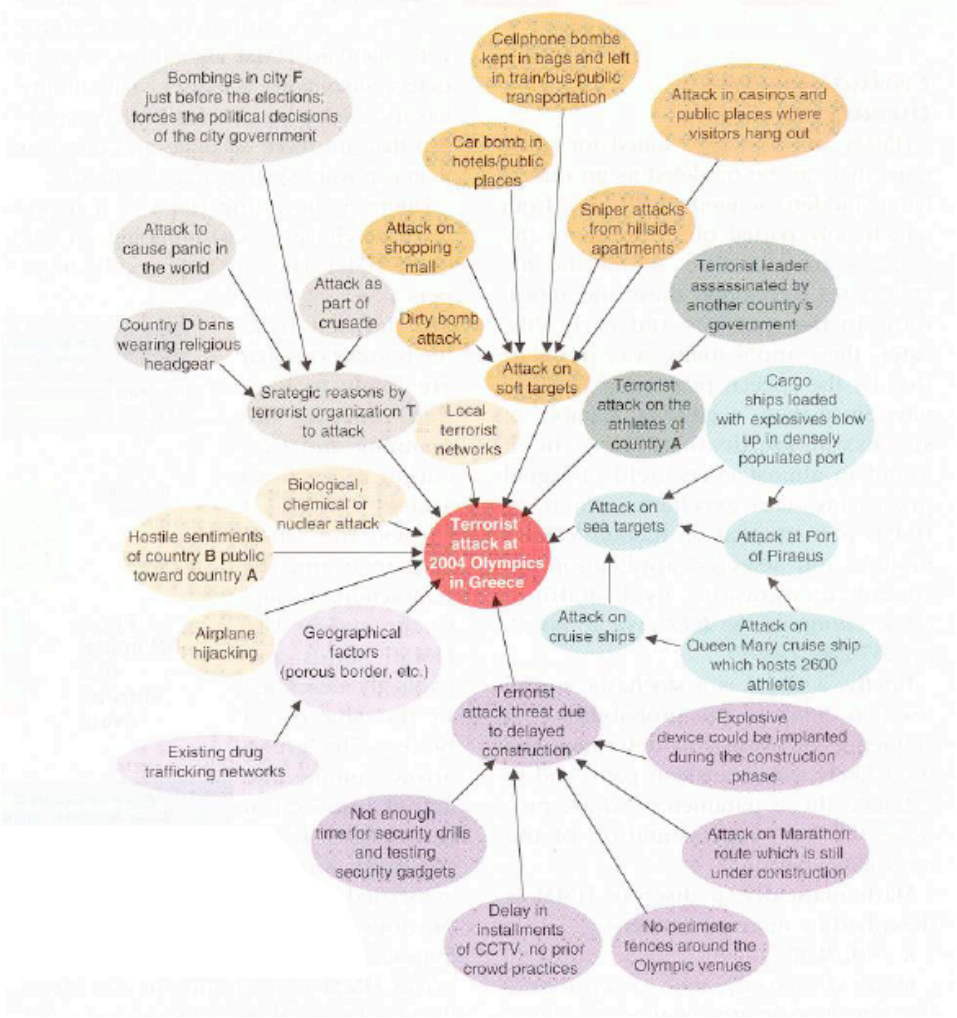


Figure 8: Dynamic Bayesian network representing the global threat level for a terrorist attack at the 2004 Olympics in Athens (GeNle 2.0, 2003).

The inputs to the ASAM system are relevant transactional data, such as proven communication between suspicious individuals and financial transactions. Table 3 shows the transactions that would characterize the states of the HMM of the truck bombing scenario shown in Figure 7. This type of transactional information could be generated by a program such as the Evidence Extraction and Link Discovery (EELD) project, a government initiative with the goal of extracting relevant data from large quantities of classified and unclassified data sources (Allanach et al, 2004), (EFF, 2008).

As the incoming transactions fulfill the state transition requirements of the HMMs, the transaction space evolves and the probability of the terrorists successfully executing the plot can be evaluated. Each state transition that is detected can be visualized as the completion of a link between nodes on a graph, as shown in Figure 9. Using a probabilistic graph matching methodology, the pattern these links create can be compared to the HMM state representing successful task completion, resulting in a measure of the probability that the terrorist group is executing the subplot.

State	Transactions
1	AQ announces attack on western targets: • Spiritual leader gives inflammatory preachings in Middle-East. • Al Jazeera, a Middle-East based media, reports that AQ website announces an attack on western targets
2	Recruitment/training of new members: • The ring leader in AQ recruits terrorists to carry out the truck bombing attack. • AQ cell recruits operators to execute the attack and drive the vehicle.
3	Set up AQ cell: • The terrorists are embedded in Greece a few months or a year before the Olympics and set up a cell. • AQ ring leader assigns the operators, planners and facilitators for the attack. The facilitator provides driving licenses, passports, etc. to the operators. • AQ cell members rent two or three apartments and they pay rent by cash.
4	Money for operation: • The AQ ring leader sends money to the AQ cell members via messengers.
5	Planning for attack: • The terrorists reconnoiter the target location multiple times. • The terrorist cell members communicate with the ring leader.
6	Gather resources: • Terrorists purchase or steal chemicals, blasting caps and fuses for explosives in Turkey and transfer via trucks to Greece. • Terrorists purchase or steal respirators and chemical mixing devices in Greece. • Terrorists purchase electronic parts such as satellite cellular phones from illegal sources. • Terrorists rent a truck.
7	Target reconnaissance: • Suspicious persons (bomb building experts, persons on the watch lists) reconnoiter the potential targets. • Terrorists perform dry runs of routes to identify speed traps, road hazards, etc.
8	Weapons installed: • Terrorists modify the truck to handle heavy loads and neutralize any security arrangements at the target.
9	Attack: • The terrorists drive the truck into the target and detonate the bomb.

Table 3: Transactions for the truck bombing Hidden Markov Model depicted in Figure 7 (Singh, Allanach et al, 2004).

This information is then reported to the corresponding sub-DBN and used to compute the global threat level. The ASAM tool can provide analysts with three types of results: 1) A likelihood of observations, which is a "measure of the confidence of the match between the observed events and the template models"; 2) Evidence from observations such as transaction type, description, and time; and 3) Probability of a terrorist attack, which is a function of the global threat level based on the overarching DBN.

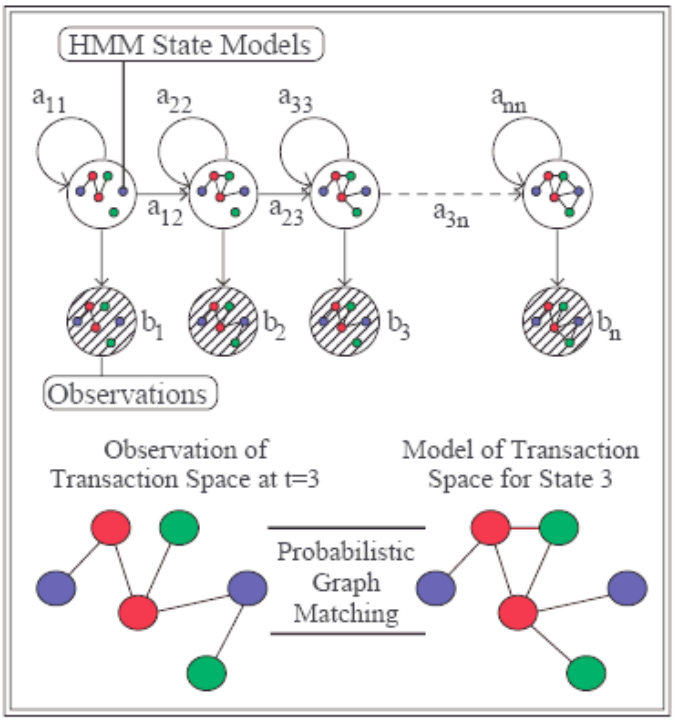
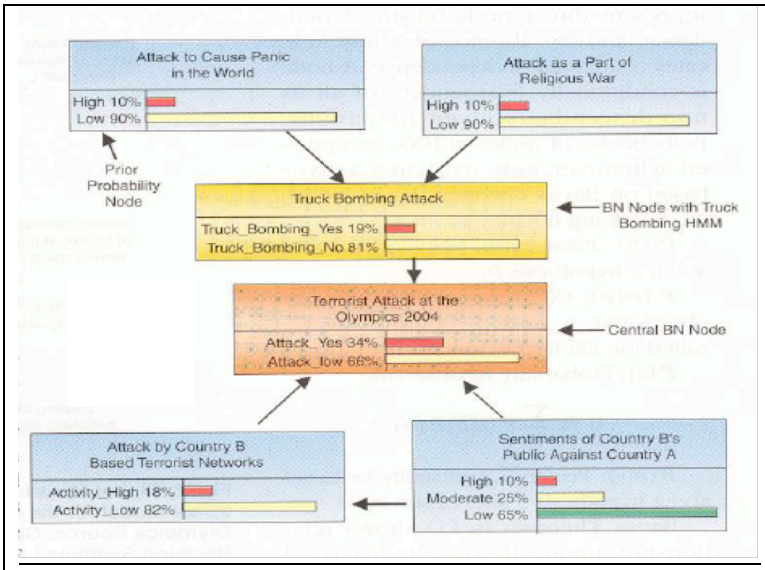


Figure 9: Graphical representation of state transitions in a Hidden Markov Model (Allanach et al, 2004).

The researchers performed several simulations using the ASAM tool, including one which utilized the truck bombing HMM shown in Figure 7. They generated synthetic transaction data to simulate the events corresponding to the truck bombing plot, and mixed the data with background "noise" transactions. The simulation investigated the "likelihood of observations" result, which corresponds to the probability the HMM reports to its DBN node (Figure 10b), and the global probability of a terrorist attack for the abridged DBN shown in Figure 10a. The results of the simulation indicate that the global probability of a terrorist attack peaks at 48%, which could be interpreted by an analyst as likely. The developers of the ASAM system assert that it is intended to provide analysts with "soft alerts rather than hard decisions." False positives are an inevitable result, but they can be minimized by obtaining accurate model parameters from the input of multiple intelligence analysts. Future work includes the addition of feedback capabilities via influence diagrams, which will allow analysts to simulate the impact of counter-terrorism measures on the threat level.

The ASAM system is also a component of a larger collaborative tool for counter-terrorism analysis called the Network Modeling Environment for Structural Intervention Strategies (NEMESIS). The NEMESIS environment "provides a forum for information exchange among multiple modeling or analysis tools, and model-based team collaboration" (Popp et al, 2004). The platform utilizes Organizational Descriptive Language (ODL), which allows users to experiment graphically with different types of models. In addition to ASAM, NEMESIS incorporates the Organizational Risk Analysis (ORA) tool developed by researchers at Carnegie Mellon University. ORA is a "network tool that detects risks and vulnerabilities in an organization's design structure," which makes it useful for simulation of terrorist network destabilization strategies, such as those discussed below (Popp et al, 2004).



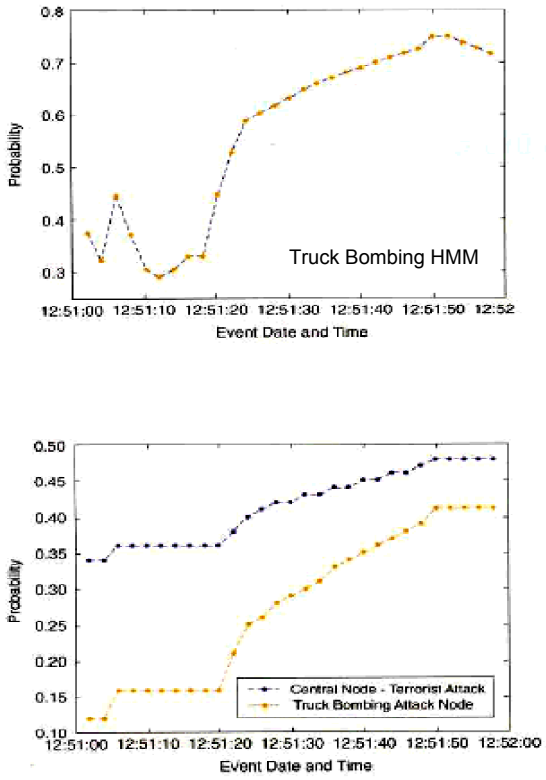


Figure 10a (Above): Simplified global threat model used in simulation of impact of truck bombing attack

Figure 10b (Right): Likelihood of observation result from the application of the truck bombing HMM **(top)**, and corresponding global probability of terrorist attack **(bottom)** (Singh, Tu et al, 2004).

Predictive Modeling: Destabilization of Terrorist Networks

The modeling techniques discussed so far have approached the problem of modeling the emergent behavior of VNSAs in cyberspace from a passive perspective, excluding analysis of the impact counter-terrorism measures may have on the group's ability to function. This type of analysis is currently being investigated by researchers at the Carnegie Mellon center for Computational Analysis of Social and Organizational Systems (CASOS). They propose a Dynamic Network Analysis (DNA) approach, which "extends the power of thinking about networks to the realm of large-scale, dynamic systems with multiple co-evolving networks under conditions of information uncertainty with cognitively realistic agents" (Carley et al, 2003). The approach takes into account the dynamic and covert nature of terrorist networks, which are generally composed of semi-autonomous cells as opposed to hierarchical structures. Attempting to destabilize terrorist networks using strategies developed for well-defined, hierarchical networks will not be effective, hence the development of the DNA approach.

The group approached the problem by focusing on three key questions: "What is the size and shape of the covert network?; "How does the nation in which the covert network exists impact its form and ability?"; and "If we do x to the covert network, what is likely to happen?" The approach they developed (Carley et al, 2003) utilized the following seven step process for assessing various destabilization strategies:

1. Identify key network entities and connections between them.
2. Identify key processes by which entities or connections are added or dropped, or in the case of connections, changed their strength.
3. Collect data on the covert network.

4. Determine performance characteristics of the existing system.
5. Determine performance characteristics of the optimal system, if applicable.
6. Locate vulnerabilities in the network and select destabilization strategies.
7. Determine performance characteristics in the short and long term after destabilization strategy has been applied.

The initial testbed for this methodology was composed of open-source data describing the terrorist network associated with the embassy bombing in Tanzania. Generally, the group defines "entities" as people (agents), knowledge, resources, events, tasks, groups, and countries, but for this analysis a simplified set was used that consisted of people, resources, and tasks.

The performance of the system was simulated using the software DyNet, also developed by the CASOS group. DyNet is a "multi-agent network system for assessing destabilization strategies on dynamic networks," and input to the system is a "knowledge network" composed of the "individuals' knowledge about whom they know, what resources they have, and what task they are doing" (Carley et al, 2003). The group also assessed the efficiency of the network's structure by comparing it to its optimal configuration, which was ascertained by minimizing the vulnerabilities caused by workload and distribution of resources and communication ties. The results indicate that the organization was not particularly well-designed since it required 88 changes to "who is doing what and has what resources to reach the optimal configuration." It was also noted, however, that these results could indicate that a substantial amount of information on the organization's structure is missing.

Next, the impact of four destabilization strategies on the performance of the network was assessed. The strategies included elimination of the person with the highest degree of Centrality, Betweenness Centrality, Cognitive Load, or Task Exclusivity. (Betweenness and Centrality are defined above in the discussion of link/social network analysis). The simulation was a two-step process, beginning with the use of the Organizational Risk Assessment (ORA) tool developed by the CASOS group, which evaluated the "resource congruence" of the group with and without the individuals high in these measures. DyNet was then applied to the altered networks, and the performance was evaluated for changes in the ease and rate of communication flow, and the ability of the organization to adapt to these changes. Table 4 lists the results of the assessment for the two agents whose removal had the largest impact on the performance of the network: agents 5 and 7. The results indicate that the removal of either agent does not significantly affect the network's distance from the "optimal" configuration, so the researchers conclude that the effects of either removal in this case would be small.

Some of the results appear incongruous. For example, removal of agent 5 actually increases the resource congruence of the network, which is not exactly an expected outcome for removal of an important node. However, the researchers explain that "resource congruence is a strict measure such that congruence is decreased when either agents do not have the resources they needed for the task to which they are assigned or when agents have resources that are not necessary for the task they are assigned. Removal of agent 5 is reducing the presence of unnecessary resources … [making] the organizational design leaner." The diffusion results, which indicate the rate and ease with which information can be spread throughout the network, are more intuitive. Removal of agent 7 is disruptive to the flow of communication because it decreases the potential diffusion rate. In contrast, removal of agent 5 actually increases the potential rate of communication

between nodes. The researchers point out that this "potentially makes the organization more vulnerable to information warfare attacks," since both correct and incorrect information can be disseminated more rapidly as a result of removing this agent.

Measure	Original Design	After Removal of 5	After Removal of 7
Hamming from Optimal	88	83	86
Resource Congruence	.475	.525	.475
Performance as Accuracy - Initial Impact	78.5625	78.22	82.72
Performance Recovery – Percentage Increase in Performance	95.55	89.72	93.7
Diffusion Initial	21.62291	14.70212	13.27369
Diffusion Recovery – Percentage Increase in Diffusion	71.23304	89.05325	50.87843

Table 4: Impact of agent removal on terrorist network's performance characteristics (Carley et al, 2003).

The results of this study demonstrate the potential of this methodology, but it is clear that much future work is needed to perfect the process. As emphasized by the CASOS group, it is important to take into account the fact that covert network assessments will be ill-informed and constantly changing, and the lack of complete information on the structure of the Tanzania terrorist network is a likely cause of the somewhat inconclusive simulation results. These issues further emphasize the importance of having a content-rich dataset that can adequately inform predictive models.

Benefits, Challenges, and Caveats

The terrorist attacks on September 11, 2001, "spurred extraordinary efforts intended to protect America from the newly highlighted scourge of international terrorism" (Jonas and Harper, 2006). These efforts included a significant interest in the potential use of predictive data mining techniques as a means of uncovering covert terrorist networks and plots, and since then, the implementation of such techniques has been surrounded by controversy. According to the National Commission on Terrorist Attacks upon the United States, if the government had pursued the leads available at the time, the attacks could have been prevented. This raises the question: Could data mining and predictive modeling techniques have played a role in averting the tragedy? According to a report by Jeff Jonas and Jim Harper for *Policy Analysis* (Jonas and Harper, 2006), the answer to that question is no. They describe data mining as "not well-suited to the terrorist discovery problem," and they have defined data mining as "the process of searching data for previously unknown patterns and using those patterns to predict future outcomes." In particular, they do not feel that predictive data mining would have made an impact on preventing 9/11. They assert that what law enforcement officials needed was not new technology, but "a sharper focus and perhaps the ability to more efficiently locate, access, and aggregate information about specific suspects."

The report also emphasizes the high likelihood of false positives - cases where individuals are incorrectly classified as "suspicious" due to some combination of activities that correlated with a

"terrorist-behavior" pattern. They cite the use of predictive data mining in consumer direct marketing campaigns that utilize demographic profiles of potential customers to target mailings to individuals that are statistically likely to buy certain products. Despite having access to millions of customer profiles to train their algorithms, the positive response rate for this type of advertising is in the single digits, corresponding to a minimum 90% false positive rate (Direct Marketing Assoc., 2004). In comparison, terror-related plots are much smaller in number, with "only one or two major terrorist incidents every few years - each one distinct in terms of planning and execution" (Jonas and Harper, 2006). This lack of historical data prohibits the creation of valid predictive models, opening the door to the possibility of an overwhelming number of false positives that would waste valuable financial and law enforcement resources.

While Jonas and Harper strongly disagree with the use of predictive data mining for the detection of covert terrorist plots and networks, their opinions are not contrary to what most researchers believe to be the limitations, realistic expectations, and proper application of predictive modeling techniques. The consensus is that these techniques should only be expected to produce meaningful results if they are well-informed, particularly by seed information from outside authoritative sources (Last, 2005). Predictive modeling should be used as a "power tool for analysts and investigators - a way to conduct low-level tasks that will provide clues to assist analysts and investigators" (DeRosa, 2004).

Another controversial issue surrounding the use of predictive data mining techniques is their potential to infringe on individuals' privacy if not executed in a responsible manner. If "data mining or automated data analysis…is deemed acceptable given the potential harm of catastrophic terrorism,…there will be great temptation to expand to use of [the] tools" to other high profile illegal behavior - a phenomenon known as "mission creep" (DeRosa, 2004). Experts propose the implementation of a four step plan "designed to protect privacy and prevent abuse," should the government gain access to large databases of private information (DeRosa, 2004). The plan consists of: 1) Developing technology to address inaccurate data and false positives; 2) Developing technology designed to "mask or selectively reveal identifying data"; 3) Implementing audit technology; and 4) Implementing "permissioning" technology.

As mentioned previously, reducing false-positives can be accomplished by utilizing "cleaner" datasets and perfecting the models used for pattern-based analyses. Anonymization will provide analysts with access to identifying information, such as names, addresses, and social security numbers, on a need-to-know basis only. Audit technology is a secondary level of defense intended to "watch the watchers;" that is, protect against authorized users with access to identifying information who would abuse their authority. Finally, permissioning technology involves the implementation of rule-based processing where policies are built directly into the search engines that have access to private data. Users would be required to present evidence of permission to access content, such as a warrant, and the system would automatically grant access to only that content (DeRosa, 2004).

Research and Development Directions

Research on the application of modeling techniques to the study of emergent behavior of VNSAs in cyberspace is ongoing. As evidenced by some of the results discussed above, there is room for significant progress to be made in this field. The University of Arizona group responsible for

the Dark Web collection continues to analyze the data from several different perspectives. Forthcoming publications include a study of "sentiment and affect" analysis of Web content. The analysis allows them to quantify the levels of radical sentiment and violence in Web content with the goal of identifying sites that warrant further investigation (Univ. of Arizona, 2008). The study also examines the process by which "ideas become infectious based on their contents," and the group implemented visualization techniques that can be used to monitor the change in sentiment and affect over time among a group of people.

The continued growth of clean, content-rich raw data sources, such as the Dark Web collection, is critical for the further development of modeling techniques, as is the development of information portals that provide efficient access to the data. The Dark Web Portal is an example of a database access tool that utilizes document summarization, categorization, and visualization techniques to allow users to quickly locate, browse, and analyze the multilingual information they seek (Zhou et al, 2005).

Given the magnitude of the Dark Web collection, an access tool such as the Portal is a necessity, and work is ongoing to include additional natural language processing techniques such as entity and relations extraction to improve its ability to interpret user search commands. The further development of multilingual techniques for the classification of Web content is also a critical area of research, particularly for Arabic Web content. The ontology of the Arabic language poses significant challenges for classification techniques that are based on an English phenomenology, so continued development of language-specific techniques, such as those employed by the Dark Web group in the authorship identification study described above, are needed.

Given the interdisciplinary nature of the modeling process, collaborative tools like NEMESIS are particularly useful in the counter-terrorism domain. Having a platform that incorporates multiple modeling methodologies (such as ASAM and ORA) that can combine inputs from multiple users is an invaluable tool, and further development of these types of collaborative tools can help make predictive models more effective.

It is the advancement of techniques for the simulation of counter-terrorism measures, however, that could have the largest impact on the use of predictive models for decision support. Further development of this application can help realize one of the main goals of predictive modeling: to provide analysts with the ability to accurately predict the outcome of multiple counter-terrorism strategies before selecting a course of corporeal action. Overall, it is evident from the current status of this field of research that when used responsibly and with a clear understanding of their limitations, data mining and predictive modeling techniques have the potential to be powerful counter-terrorism weapons, particularly as tools that may be applied to better understand and predict the behavior of violent non-state actors.

References

Abbasi, A., and Chen, H.
2005 "Applying Authorship Analysis to Extremist-Group Web Forum Messages," *IEEE Intelligent Systems, Special Issue on Artificial Intelligence for National and Homeland Security*, Sept/Oct 2005, pp. 67-75.

Achen, Christopher H. and Snidal, Duncan
1989 "Rational Deterrence Theory and Comparative Case Studies," *World Politics*, Vol. 41, No. 2, pp. 143-169.

Allanach, J.; Tu, H.; Singh, S.; Willett, P.; and Pattipati, K.
2004 "Detecting, Tracking and Counteracting Terrorist Networks via Hidden Markov Models," *IEEE Aerospace Conference*, Big Sky, MT, March 2004.

Anderson, Jon W.
1997a Globalizing Politics and Religion in the Muslim World. Journal of Electronic Publishing 3(1). http://www.press.umich.edu/jep/archive/Anderson.html.

1997b "Cybernauts of the Arab Diaspora: Electronic Mediation in Transnational Cultural Identities", Couch-Stone Symposium on Postmodern Culture, Global Capitalism and Democratic Action, University of Maryland, April 1997

2003a New Media, New Publics: Reconfiguring the Public Sphere of Islam. Social Research 70(3):887-906.

2003b "The Internet and Islam's New Interpreters", In New Media in the Muslim World: The Emerging Public Sphere, Ed. Dale. F. Eickelman and Jon W. Anderson, Indiana University Press, Bloomington , IN, p. 48.

2007 Transnational Civil Society, Institution-Building, and IT: Reflections from the Middle East. CyberOrient: Online Journal of the Virtual Middle East. http://cyberorient.net/index.php?option=com_content&task=view&id=19&Itemid=28.

Arbatov, Alexei and Dvorkin, Vladimir,
2006 "Beyond Nuclear Deterrence: Transforming the US-Russian Equation," Washington, DC: Carnegie Endowment for International Peace.

Arquilla, John; Ronfeldt, David; and Zanini, Michele
1999 Networks, Netwar, and Information-Age Terrorism. In Countering the New Terrorism. Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini, eds. Pp. 39-84. Santa Monica, California: RAND.

Asal, V. H.; Drozdova, K.; Mariano, L.; Pattipati, K.; Popp, R.; Rousseau, D; and Santos, E.
2008 "Models of Emergent Behavior in Cyberspace," *Presentation: Promoting and Protecting U.S. Interests in the Cyber World: Violent (and non-Violent) Non-state Actors*, Arlington, VA, Jan. 9-10, 2008.

Atran, Scott and Stern, Jessica
2005 Small Groups Find Fatal Purpose through the Web. Nature 437(7059):620.

Atran, Scott
2006 A Failure of Imagination (Intelligence, WMDs, and 'Virtual Jihad'). Studies in Conflict and Terrorism 29:263-278.

Benard, Cheryl
2005 "Cybermullahs and the Jihad – Radical Websites Fostering Estrangement and Hostility among Diapora Muslims", published in "A Future for the Young", Cheryl Benard, RAND working Paper, WR 354, Sept. 2005

Bishop, C. M.
2006 *Pattern Recognition and Machine Learning*, Springer.

Bodnar, John W.
2003 Warning Analysis for the Information Age: Rethinking the Intelligence Process. Washington, D.C.: Joint Military Intelligence College.

Carley, K.; Reminga, J. and Kamneva, N.
2003 "Destabilizing Terrorist Networks," *NAACSOS Conference Proceedings*, Pittsburgh, PA.

Carr, Orson Scott
1977 First Meetings in Enders Universe, Tor, New York, 2003, p.151, "Ender's Game", first published in Analog magazine, 1977

Chesser, Nancy, ed.
2007 Deterrence in the 21st Century: An Effects-based Approach in an Interconnected World. Washington, D.C.: Prepared for US Strategic Command Global Innovation and Strategy Center (USSTRATCOM/GISC), Strategic Multilayer Analysis Team.

Conway, Maura
2004 Terrorism and IT: Cyberterrorism and Terrorist Organizations Online. In Terrorism and Counterterrorism: Understanding the New Security Environment. Russel D. Howard and Reid L. Sawyer, eds. Pp. 271-288. Guilford, Connecticut: McGraw-Hill/Dushkin.

2005 "Terrorist Use of the Internet and Fighting Back, prepared for Cybersafety: Safety and Security in a Networked world: Balancing Cyber-Rights and Responsibilities, Oxford Internet Institute, Oxford University, UK, 8-10 September, 2005

2006 "Terrorism and the Internet: New Media-New Threat?" *Parliamentary Affairs Advance Access*, Feb. 10, 2006.

2007a Terrorist Use of the Internet and the Challenges of Governing Cyberspace. In Power and Security in the Information Age: Investigating the Role of the State in Cyberspace. Myriam Dunn, Victor Mauer, and Felisha Krishna-Hensel, eds. London: Ashgate.

2007b Terrorism and the Making of the 'New Middle East': New Media Strategies of Hizbollah and al Qaeda. In New Media in the New Middle East. Philip Seib, ed. Pp. 235 - 258. London: Palgrave.

2008 Cyberterrorism: The Ultimate Threat to Critical Infrastructures? In Power and

Security in the Information Age: Investigating the Role of the State in Cyberspace. Myriam Dunn, ed. London: Ashgate.

CTC
2006 The Islamic Imagery Project: Visual Motifs in Jihadi Internet Propaganda. West Point, New York: Combating Terrorism Center, United States Military Academy.

CYPRG website
2008 http://www.cyprg.arizona.edu/

Der Derian, James
2000 "Virtuous War/Virtual Theory," *International Affairs. London: Royal Institute of International Affairs,* Vol. 76, No. 4. pp. 771-788.

DeRosa, M.
2004 "Data Mining and Data Analysis for Counterterrorism," *CSIS Press*, Mar. 2004.

Direct Marketing Association
2004 "DMA Releases New Response Rate Report," news release, October 17, 2004, http://www.the-dma.org/cgi/dispnewsstand?article=2891.

Duda, R. O.; Hart, P. E. and Stork, D. G.
2001 *Pattern Classification, 2nd edition*, Wiley, New York.

EFF website
2008 http://w2.eff.org/Privacy/TIA/eeld.php.

Elovici, Y.; Shapira, B.; Last, M.; Zaafrany, O.; Friedman, M.; Schneider, M. and Kandel, A.
2005 "Content-based Detection of Terrorists Browsing the Web Using an Advanced Terror Detection System (STDS)," *Intelligence and Security Informatics Proceedings*, Vol. 3495, pp 244-255.

Epstein, Joshua M. and Axtell, Robert L.
1996 Growing Artificial Societies: Social Science from the Bottom Up. Cambridge, Massachusetts, and Washington D.C.: MIT Press, and the Brookings Institute.

Fallows, J.
2008 Personal email to SMA core team member Carl Hunt, 8 January 2008.

Fisher, Uri J.
2006 "Deterrence, Terrorism, and American Values," Paper presented at Annual International Studies Association Meeting, San Diego, CA, March 22-25.

Gates, R.
2008 Speech delivered by the Secretary of Defense to the Center for Strategic and International Studies, "Pre-Alfalfa Luncheon," January 2008.

GeNle 2.0,
2003 Decision Systems Laboratory, University of Pittsburgh.

George, Alexander L. and Smoke, Richard
1989 "Deterrence and Foreign Policy," *World Politics*, Vol. 41, No. 2., pp. 170-182.

Gleick, James
1987 Chaos: Making a New Science. New York: Penguin Books.

Gruen, Madeleine
2004 White Ethnonationalist and Political Islamist Methods of Fundraising and Propaganda on the Internet. In Terrorism and Counterterrorism: Understanding the New Security Environment. Russel D. Howard and Reid L. Sawyer, eds. Pp. 289-302. Guilford, Connecticut: McGraw-Hill/Dushkin.

2006 The Khalifate is Way Cool: The Role and Method of Hibz at-Tahrir US in the Proliferation of Party Ideology Worldwide. Hudson Institute Lecture, August 13 2006, Washington D.C.

2007 Hizb-ut-Tahrir's Activities in the United States. Terrorism Monitor 5(16):7-9. http://www.jamestown.org/terrorism/news/uploads/TM_004_002.pdf.

Holland, John H.
1998 Emergence: From Chaos to Order. New York: Basic Books.

Jensen, D.
2003 "Data Mining in Networks," *presentation at CSIS Data Mining Roundtable*, Washington, D.C., July 23, 2003, http://kdl.cs.umass.edu/people/jensen/papers/nrcdbsse02.html.

Joint Chiefs of Staff
2000 Joint Tactics, Techniques and Procedures for Joint Intelligence Preparation of the Battlespace JP 2-01.3. Washington, D.C. http://www.dtic.mil/doctrine/jel/new_pubs/jp2_01_3.pdf.

Jonas, J. and Harper, J.
2006 "Effective Counterterrorism and the Limited Role of Predictive Data Mining," *Policy Analysis*, No. 584, Dec. 11, 2006.

Jonas, J.
2003 "Using Data to Detect and Preempt Bad Things from Happening," *presentation at CSIS Data Mining Roundtable*, Washington, D. C., July 23, 2003.

Kirk, J.
2007 "Estonia Recovers from Massive DDoS Attack: Denial-of-Service onslaught may have Russian origins," *Computer World*, May 17, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019725.

Krebs, V.
2002 "Uncloaking Terrorist Networks," *First Monday*, March 25, 2002, http://www.firstmonday.org/Issues/issue7_4/krebs/.

Lambert, Susan
2006, "Do We Need a "Real" Taxonomy of e-Business Models?" School of Commerce, Flinders University, ISSN: 1441-3906, http://commerce.flinders.edu.au/researchpapers/06-6.pdf

Last, M.
2005 "Using Data Mining Technology for Terrorist Detection on the Web," *Fighting Terror in Cyberspace: Series in Machine Perception and Artificial Intelligence*, Eds: M. Last, and A. Kandel, Vol. 65.

Lesser, Ian O.
1999 Countering the New Terrorism: Implications for Strategy. In Countering the New Terrorism. Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini, eds. Pp. 85-144. Santa Monica, California: RAND.

Markov, A., and Last, M.
2005 "Identification of Terrorist Web Sites with Cross-Lingual Classification Tools," *Fighting Terror in Cyberspace: Series in Machine Perception and Artificial Intelligence,* Eds: M. Last, A. Kandel, Vol. 65.

Morgan, Patrick M.
1983 *Deterrence: A Conceptual Analysis.* Beverly Hills, CA: Sage Publications.

Peng, F. et al.,
2003 "Automated Authorship Attribution with Character Level Language Models," *presented at the 10th Conference of the Association for Computational Linguistics* (EACL 2003); http://users.cs.dal.ca/~vlado/papers/2003-EACL03-139.pdf.

Pennell, C. R., Ed.
2001 Bandits at Sea: A Pirates Reader. New York, N.Y., NYU Press.

Peshkova, Svetlana
2002 i-Islam@hizb-ut-tahrir.org. Anthroglobe. http://malinowski.kent.ac.uk/docs/IslamAtWWW.htm.

Popp, R.; Pattipati, K.; Willett, P.; Serfaty, D.; Stacy, W.; Carley, K.; Allanach, J.; Tu, H. and Singh, S.
2004 "Collaborative Tools for Counter-Terrorism," *IEEEAC paper #1392*, Dec. 19, 2004.

Qin, J.; Zhou, Y.; Reid, E.; Lai, G. and Chen H.
2007 "Analyzing terror campaigns on the Internet: Technical sophistication, content richness, and Web interactivity," *International Journal of Human-Computer Studies*, 65. pp. 71-84.

Reid, E., Qin, J.; Zhou, Y.; Lai, G.; Sageman, M.; Weimann, G. and Chen, H.
2005 "Collecting and Analyzing the Presence of Terrorists on the Web: A Case Study of Jihad Websites," *IEEE International Conference on Intelligence and Security* (ISI 2005), Atlanta, Georgia, 2005.

Rivkin, David B. Jr.
2006 "The Virtues of Preemptive Deterrence" *Harvard Journal of Law and Public Policy* 29(1), pp. 85-104.

Robb, John
2008, Personal email to SMA core team member Carl Hunt.

Sageman, Marc,
2004 Understanding Terror Networks, University of Pennsylvania Press, Philadelphia, PA.

2008 *Leaderless Jihad: Terror Networks in the 21st Century*, Univ. of Pennsylvania Press.

Schumpeter, J. A.
1942 The Process of Creative Destruction, Unwin.

Shapira, B.
2005 "A Content-based Model for Web-Monitoring," *Fighting Terror in Cyberspace: Series in Machine Perception and Artificial Intelligence*, Eds: M. Last, & A. Kandel, Vol. 65.

Silber, Mitchell D. and Bhatt, Arvin
2007 Radicalization in the West: The Homegrown Threat. Pp. 90. New York City Police Department, Counterterrorism Unit, New York http://www.nypdshield.org/public/SiteFiles/documents/NYPD_Report-Radicalization_in_the_West.pdf.

Singh, S.; Allanach, J.; Tu., H.; Pattipati, K. and Willett, P.
2004 "Stochastic Modeling of a Terrorist Event via the ASAM System," *IEEE Conference on Systems, Man and Cybernetics*, The Netherlands, October, 2004.

Singh, S.; Tu, H.; Allanach, J.; Areta, J.; Willett, P. and Pattipati, K.
2004 "Modeling Threats," *IEEE Potentials*, Aug/Sept, 2004.

Smart, W.
1912 The Distribution of Income, Being a Study of What the National Wealth is and of How it is Distributed According to Economic Worth. London, Macmillan and Company.

Smith, S. P.; Crider, J. Allen; Perritt Jr., H. H.; Shyong, M.; Krent, H.; Reynolds, L.L. and Mencik, S.
2000 "Independent Review of the Carnivore System: Final Report," *IIT Research Institute*, Dec. 8, 2000.

Speckhard, Anne
2007 "De-Legitimizing Terrorism: Creative Engagement and Understanding the Psycho-Social and Political Processes Involved in Ideological Support for Terrorism" Democracy & Security.

Stamatatos, E.; Fakotakis, N. and Kokkinakis, G.
2001 "Computer-Based Authorship Attribution without Lexical Measures," *Computers and the Humanities*, vol. 35, no. 2, pp. 193-214.

Tunander, Ola
1989 "The Logic of Deterrence," *Journal of Peace Research*, Vol. 26, No. 4, pp. 353-365.

U.S. Department of Defense
2001.

Univ. of Arizona
2008 University of Arizona Artificial Intelligence Lab Dark Web Terrorism Research site: http://ai.arizona.edu/research/terror/index.htm.

USSTRATCOM
2006 Deterrence Operations Joint Operating Concept. Pp. 77. Omaha, Nebraska: United States Strategic Command (USSTRATCOM) www.dtic.mil/futurejointwarfare.

Weimann, Gabriel
2004 www.terror.net: How Modern Terrorism Uses the Internet, *United States Institute of Peace Special Report* 116, March 2004.

2006 "Terror on the Internet: The New Arena, the New Challenges", United States Institute of Peace Press, Washington DC.

Whiteneck, Daniel
2005 "Deterring Terrorists: Thoughts on a Framework," *The Washington Quarterly* 28(3), pp. 187-199.

Zagare, Frank C.
2004 Reconciling Rationality with Deterrence. Journal of Theoretical Politics 16(2):107-141.

Zanni, Michele, and Edwards, Sean J. A.
2001 "The Networking of Terrorism in the Information Age," in Networks and Netwars: The Future of Terror, Crime, and Militancy, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND corporation) p. 30.

Zheng, R. et al.
2005 "A Framework of Authorship Identification for Online Messages: Writing Style Features and Classification Techniques," *Journal of American Society of Information Science and Technology* (JASIST).

Zhou, Y.; Qin, J.; Lai, G.; Reid, E. and Chen, H.
2005 "Building Knowledge Management System for Researching Terrorist Groups on the Web," *Proceedings of the 11th Americas Conference on Information Systems*, Omaha, NE, Aug. 11-14, 2005.

2006 "Exploring the Dark Side of the Web: Collection and Analysis of US Extremist Online Forums," in *Proceedings of the Intelligence and Security Informatics: IEEE International Conference on Intelligence and Security Informatics* (ISI 2006), San Diego, CA, USA, May 23-24, 2006.

Appendix A: Workshop Participants and Contributors

Participants in 9-10 January 2008 Workshop in Arlington, VA

Name	Organization	Report*
Alrich, Amy	IDA	yes
Anderson, Jon	Catholic University	
Asal, Victor	SUNY Albany	yes
Astorino-Courtois, Allison	NSI	yes
Axtell, Rob	George Mason U and Santa Fe Institute	yes
Barnett, Thomas	Enterra Solutions	yes
Benard, Cheryl	Rand	
Cabayan, Hriar	OSD	yes
Cares, Jeff	Alidade Incorporated	
DeJong, Kenneth	George Mason U	
Hamilton, Bart	STRATCOM/GISC	
Henze, Roger CAPT	STRATCOM/GISC	
Heuring, Terry	IDA	
Hunt, Carl	IDA	yes
Kuznar, Lawrence	NSI (on leave from Indiana U)	yes
Meadows, Brian	SPAWAR	
Numrich, Sue	IDA	yes
Pattipati, Krishna	University of Connecticut	yes
Pease. Michael	IDA	
Popp, Bob	NSI	yes
Robb, John	Global Guerillas	
Rousseau, David L., Prof	SUNY Albany	
Sanford, Mark S.	SRC	
Santos, Eugene	Dartmouth U	
Shannahan, Michael Lt Col	STRATCOM/GISC	
Shaw, Alan	IDA	
Steinberg, Ken	Savant Technologies	yes
Veazie, Todd	Joint Staff	yes
Vlahos, Michael	Johns Hopkins	
Vorce, Jeffrey	Joint Staff	
Wu, Tim	Columbia Law School	yes

Contributors to this report who were unable to attend 9-10 January 2008 Workshop

Name	Organization	Report*
Borda, Matthew	Creighton U	yes
Fallows, James	Atlantic Monthly Magazine	yes
Mariano, Laura	University of Connecticut	Yes
Drozdova, Katya	NSI	yes

* "yes" indicates contribution to this report

Appendix B: Workshop Notes

Edited by Alan Shaw, Institute for Defense Analyses

Workshop: Promoting and Protecting U.S. Interests in the Cyber World: Violent (and non-Violent) Non-state Actors; held 9-10 January 2008 at Directed Technologies, Inc, Arlington, VA

Workshops are, by their nature, only moderately ordered discussions. Agenda topics are often addressed out of sequence, or intermittently; topics not on the agenda often arise in the course of discussions and become foci of interest. Ideas are raised, tested, developed, and often significantly altered. This workshop was no exception. Indeed, because of its exploratory nature, the discussion was perhaps even less orderly than what is typical. That has the salutary effect of stimulating thinking, and allowing ideas to emerge and be developed. This appendix is not a transcript of the proceedings. It is more of a summary "think piece" in which the workshop participants did the thinking, and others attempted to capture the participants' main thoughts as they support the purposes of the workshop. It summarizes the workshop discussion in more or less chronological order, and so complements and supports the main body of the workshop report paper, which captures the main ideas and presents them in an orderly fashion.[17]

This appendix does not include prepared briefings and other presentations.

Workshop Day 1:

Who and what are we talking about deterring?

The basic charge is to consider violent non-state actors (VNSA); the participants noted that, if taken strictly, this could be too narrow. A state can exert leverage on a VNSA. Deterring the VNSA might be facilitated by deterring the state sponsor; or deterring the VNSA may be a tool to affect the state. VNSA implies political actors, but we shouldn't dismiss criminals from consideration.

Similarly, just because a group is non-violent doesn't mean that it isn't very much against us or able to cause us significant problems that we would like to be able to deter. On the other hand, we tend to lump folks whose idea of world order differs from ours together with those who oppose us with violence. By concentrating on violent actors, we may overlook other significant opponents; but treating all who see the world differently than we do as if they were VNSAs could also be a mistake.

The tendency is to concentrate on deterring (or stopping) major acts. However, aggregated small actions can have a large net effect. Small perturbations can create large problems in the

[17] REPORT EDITOR'S NOTE: This transcription is a conversational recap of the events of the 9-10 January 2008 VNSA Workshop as compiled by the editor named above. While not an "Event Minutes," it is a depiction of relevant points and lines of query presented during the workshop and some of the interactions between participants in which these points were raised and discussed. The points and issues contained within this appendix serve to back up the formal observations made in the main body of the report.

aggregate, including creating disorder that states or VNSAs can then exploit. Sequential small changes can be cumulative, leading to a situation that we don't like and is hard to reverse. This leads us to think about deterrence as affecting activities so as to shape the future in a way that we want it to be.

We need to be careful about thinking in terms of the binary US and THEM. This complex environment features a range of players, each of whom is part of the context: good guys, bad guys, neutrals, non-adversaries; violent actors, non-violent actors; real actors and fictitious persona. One suggested part of the approach to deterrence is to deter types of actions rather than specific actors. Trying to conduct a certain type of act brings an automatic, unpleasant response, like the directed energy weapon that causes pain to anyone who enters into the protected area. Or data-base equivalent of retail store dye packs. The hacker can steal the data, but he can't sell it. Maybe it has bad data embedded in the real data, and the hacker cannot separate the two.

The globalized Internet environment

Part of what we are talking about here is navigating through a period of rapid expansion and evolution, which does not, as yet, have an adequate rule set. Although it takes time, a rule set will emerge. So maybe we should be thinking about how we identify the rule set that we want, and then do what we can to steer the world in that direction. However, it is unrealistic to think that there will be an identifiable end state. Things will get more settled, while continuing to evolve.

Globalization is a major factor in this discussion. This is not the first time in history that globalization has occurred. For example, the 13th and 14th centuries were an earlier period of globalization. In these periods, political structures are challenged, and non-state actors challenge states. After some time, new structures, new rules, new alignments take effect, and things get less open and chaotic.

The Internet is an increasingly ubiquitous global medium. This more or less global Internet presence expands opportunities to entities beyond nation states. The Internet allows for the creation of virtual personae. So we can be dealing with an actor who is an on-line persona that differs from any specific physical person. The person behind the virtual persona can be several steps removed and insulated. One physical person can have many virtual personae. Several people can collectively be behind one virtual persona, and so on. Through this medium, a persona can appear or act almost anywhere almost instantaneously.

While a VNSA can operate on the Internet, no violence occurs on the Internet. However, cyber activities can support violent actions. (**note**: later in the discussion, some participants took exception to this, citing virtual violent actions that can have similar psychological effects to actual violent actions, the use of "hacking" to cause physical damage to facilities, and doing violence to cyber assets such as financial databases.)

Examples were offered of violence in cyberspace:
1. An attack on State Department computers that resulted in "fried" hard drives

2. rape in 2nd life – physical persona complains of psychological effects as a result of rape in a virtual world (remember 2nd life entities are built by the real person with considerable investment of time and interest)
3. Pictures of Abu Ghraib atrocities, video footage of beheadings: images of violence that may encourage actual violence. Pictures have more of a visceral impact than words do.

So what can be accomplished in the cyber world? This is the context within which to define deterrence and deterrent actions. We can practice persuasion and dissuasion. We can attempt to "keep bodies at rest" (i.e. inhibit the beginnings of movements or activities that are not in our interest). We can try to practice "deradicalization"; but there was skepticism that this can really be done. We can try to influence "fence sitters" to fall in one direction rather than the other. We can work through public channels or private (i.e. open access or restricted access); directly or through intermediaries (either willingly complicit or unwitting accomplices).

How to deter

Consider the Muslim world. We are worried about the radical activists, but they are only a small subset. The radicals draw recruits from a much larger population. And they vie with other movements for influence. (Later on in the discussion, there will be explicit consideration of playing to, and encouraging the growth of, a Muslim middle class as a counterweight to the radical movements.) The radicals seek a stronger role for Islam. Other Muslims share this goal, but don't necessarily share the detailed view of what Islam is and what that stronger role should be, or endorse the radical approach to achieving it.

Returning to the topic of types of deterrence activities, the following were offered:
1. directly deterring or preventing specific cyber activities, whether criminal or hostile, that would be captured under the general heading of "hacking"
2. fighting information battles
3. dissuasion, persuasion, shaping opinions, and so on
4. creating rules for actions and behavior in cyberspace; creating a stable environment that supports our needs.

It was noted that prosperity can also be a deterrent to radical behavior.

Whatever we think we would like to do has to be formulated within an environment in which the future is highly uncertain, and which our powers to shape are limited.

There was some discussion of terminology and concepts, particularly extending political/ military/ social concepts like "shaping" into cyberspace, and extending the concept of "hacking" into the political/ military/ social realm. Both such extensions were viewed as interesting, but also somewhat stretched.

There is also exploitation of cyber activities, particularly for gathering intelligence, to probe adversaries' networks, support, connections, and thought patterns.

The participants restated two basic issues:
1. Are we concerned with deterring cyber activities (activities conducted in cyberspace), or using cyberspace to deter activities in the physical world?

2. Are we concerned with cyber tools, such as the instruments of hackers and thieves, what they can do and how they can be deterred, or are we concerned with a broader set of activities in the cyber world?

Regarding this, it was noted that the Internet provides both the ability to reach large populations, and a medium through which individuals (or small groups) can achieve disproportionate power. So where is the focus: on the broad world or on the few very dangerous individuals?

Cyber social environment

There is an inherent relationship between rules and tools - and policy stands behind the rules that are established. Rules make some tools viable, while limiting the utility of others. The dynamic is that rules are generated based on current tools and demonstrated activities using those tools. The rules rein in the use of the tools, and therefore stimulate development of new tools that can operate outside the strictures of the rules. This, in turn, provides stimulus for revising the rules. Before we can develop rules to control activities, we need to know our policy, i.e. what we want to allow and what we want to curtail.

The US wants both openness and controls on hacking activities that we consider dangerous.

There are real personae and virtual identities. People can be bolder with their virtual identities than they are when using their real identities. One person can establish multiple virtual identities; several people can all support and contribute to one virtual identity. How individuals relate to their virtual identities is an interesting and important question.

Socialization and social dynamics can be different in cyberspace. Virtual personalities are structured differently from real personalities. The same is true for relationships. Groups of individuals who only interact through passing messages can have different dynamics from groups that interact face-to-face. The time constants can be different. Groups can form, act, and disband quickly in cyberspace. Current models of behavior may or may not work in cyber world. Ties formed on the Internet are not familial, not a deep identity such as that of a tribe, but based on shared ideas, experiences, identity. Self-selection plays a major role in community formation. Cyber space speeds up developments and reactions and takes developments and ideas to places it wouldn't have reached before. Use of the Internet can support greater span of control, or greater individual initiative. The Internet's key technical features that enable these developments are speed and reach of communication. How they are used is a social issue.

The topic of terrorist radicalization via the Internet is worthy of further exploration. How do radicals find each other? Where do they meet in cyberspace, and does that then extend to physical space? By what means are participants kept involved? What is the relationship among cyber activities, virtual personalities, and the real world? The person who is online still has a physical reality, which may be affected by his cyber activities. The Internet offers an opportunity for people who are physically separated to meet and coordinate. It also offers the opportunity to put aside other sources of separation (i.e., other than geographic separation. People only need to agree on the matter being discussed to work together; they can differ on other matters.)

How and when does a cyber group invade physical space? If it does, how do you maintain that universe? The cyber universe makes them more insular, not able to fit in, more uncomfortable in the physical world.

Similar considerations apply to perceptions. How the US (or some other entity) is perceived can be strongly shaped by what information is available on the Internet. At the extreme, the accepted on-line image of the US is how the US will be perceived. There are people who believe that "everything" on the Internet is true. Moreover, there are few checks on bad information. So the Internet offers Islamist radicals an opportunity to present Muslim publics with a very hostile image of the US.

The Internet allows an actor to create content, volume and gain adherents, for almost no cost. We need to be concerned with the psychological impact, too.

Increasingly, the Internet is a visual medium that allows the wide circulation of very powerful images, such as Abu Ghraib and the al Qaeda beheadings. However, the radicals don't have a monopoly on such use of the Internet (unless we cede it to them).

Perceptions and cyber space

Islamists are preoccupied by the "pollution" of western culture that is flooding into Muslim countries via the Internet, including via Arab news media. Arab culture is not penetrating the US public; US culture is penetrating the Arab world. This influence provides us with an opportunity.

(At this point in the discussion, Carl Hunt read an essay that James Fallows had sent him for this meeting. A revised version appears as the Foreword. Mr. Fallows notes that recent history has shown that it is possible to generate a very positive perception of the United States, and that such a positive perception is a powerful generator of deterrence and good relations.)

The best engine for creating a positive image of the US is the projection of American ideals and the benefits thereof through the efforts of the private sector. The public sector can help, but caution should be exercised so as not to do any harm. (This admonition applies particularly to the military.) Some participants voiced skepticism about being able to do "good marketing", but observed that we should at least avoid "bad marketing". There may also be value in "taking down" anti-American marketing by our adversaries.

Some participants observed that cyberspace had offered opportunities to avoid problems that were generated by OIF (Operation Iraqi Freedom), but that the US, for whatever reasons, missed those opportunities and instead made mistakes. The Internet offered at least an underused source of information, and possibly the opportunity to exert influence that might have changed perceptions and thereby events.

Deterrence would seem to take place in social cyberspace. For us, social cyberspace is fixed, static. It is spreading—moving to new communities. When it's new to you, it's almost mystical; the world of myth making is within the realm of cyberspace. Things can happen there that would not happen anywhere else. We don't know much about the social cyberspace world. The world of myth making is not detached from the real world. What is the connection between cyberspace

and the social forms that can transfer to it, can't transfer to it, and can shape it? Behind all of the cyber world, behind these capabilities, there are physical actors who could be deterrable in classic ways. Can actors who are classically deterrable also influence others? How does this myth making serve as a possible means to influence/affect VNSA?

Classical deterrence theory is too narrow for all threats/actors. However, the cost- benefit-risk model is not irrelevant in this case. In the cyberworld we may lack the necessary direct and deep knowledge of our adversary.

We (should aim to) simultaneously persuade, dissuade, deter – we use multiple approaches to shape the actions of the other. Consider "rational actors" - just because something is irrational to you, does not make it irrational, it means their premises are different from yours. Consider subjective rationality – bounded rationality which satisfies one or more but not all interests.

Neither you nor the "adversary" can have full information. Have you thought of a calculus to evaluate their degree of uncertainty or incompleteness of their information? In cyberspace there is an overload of information over which no one has total control. Lack of information cuts both ways. Why do we think we need to know everything? It is better to consider what is the minimal amount of information that we need. We can use the Internet to interfere with the information.

Cyber actions can impact the physical world directly, can impact the cyber world, and can impact the psychological/social world. Cyber attacks can bring down facilities by affecting their information or control systems. Cyber attacks can deny information service. Information, especially graphic pictures and videos, can have intense psychological effects.

Policy and regulatory context

Policy and law—both domestic and international—are important areas to consider. These shape the cyber environment. We need to consider: domestic, legal and governmental challenges, role of corporate America, international law, issues of cyber defense and offense. Government-directed "un-regulation" is driving US policy – don't try to regulate the development of the Internet, except for funding.

American views with respect to the Internet are dominated by a basic theory of openness: protocols are all public, unlike cable television, etc, which are industrially developed products. The US government makes aggressive effort to get other countries to maintain an open Internet – allow Google and Amazon to be everywhere – globalization of the First Amendment.

In contrast with this emphasis on openness, we also recognize the value of regulation, at least in some areas. Our impulse is to exert more control, for example, to protect intellectual property or be able to inspect and control content on the Internet, or to protect user identities. Some degree of regulation is inevitable; if regulation is not instituted to keep the net open, then the door is open to other regulations that tighten it up. If we can't get China to agree to and abide by regulations that foster openness, China could institute internal regulations that are much more restrictive than we would like.

European policy has strong privacy policies as protection from predatory American companies who seek to exploit them. Each country has its own interests: e.g., US is focused on intellectual property, Germany is privacy, China is controlling political threats, etc.

Internet still mirrors the American origins, but other countries are trying to morph it.

One basic challenge is how far we can go in regulation to enforce our interests before we undermine the US image of a free environment, counter to the values of the US as perceived by us and the rest of the world.

The US can use a combination of incentives and punishments to enforce its Internet policies. US funding means that US gets to set rules. Entities that want to do business in the US have to play by US rules, and so on. We can impose conditions for any countries that want to be connected to the US – i.e., must maintain security of Internet or don't connect to US. All such actions will still have to be balanced with considerations such as open Internet and protection of intellectual property.

Workshop Day 2

Who, what, and how to deter

The basic issue is whether we are talking about:

1. deterring hacking – working in the computer network domain; or
2. changing minds and hearts – getting to the "left of boom"

We are not really trying to change their ideology, but there is a way of looking at the swamp they live in and attempt to drain the swamp in some way, shape or form – influence the population to the degree that the most violent alternatives cease to look as attractive.

There are two faces to deterrence: compellence and relationship (or influence). Relationship can be co-optation. During the Cold War, we effectively ceded the Soviets a notion of parity; we bestowed legitimacy on the Soviets. Similarly we are in a position to co-opt some of these groups (VNSAs). Calling this world the swamp makes it look more like an evil place and keeps us from looking at the groups as targets for co-opting. We don't even think about talking with these groups, connecting with then in any positive direction. Consider establishing relationships as the basis for cooptation; basis of legitimacy needed; give the co-opted something positive.

We have to produce the notion of what "deterrence" actually means. We might better use the term "influence" rather than the word "deterrence."

Cold war deterrence started from the principle of symbolic equivalence. What is the principle in the current case? Might be called co-participation in post-modernity. Globalization develops in part from conscious efforts to use it. They are in this with us. We are all in this post-modern world where bounds are blurred and identities are blurred. The trick is to train the larger categories of radicals and potential radicals to understand the implications of the global, post-modern world. Start from a general principle – in this case, we're all in this global world together – competing to define and refine the notion of what post-modern culture is like (where I can't close off my culture to preserve it). Globalization has escaped our old notion of

Americanization, it has also escaped the neo-liberalism – has already escaped all our definitions of it – "We recognize you as denizens of the post-modern world."

"Embourgeoisement" of the Middle East is an important development that has gotten little attention. Workshop participants were unaware of anyone having studied the rise of the middle class in non-western societies. A goal is to help people become middle class. Change rests on demographics and economics. In the Middle East, the median age is half of what it is in the West. The (Muslim) middle class is defined by prosperity and piety. We can support both (piety and the desire for prosperity) to develop to our advantage. The middle class are our natural allies. The Muslim middle class will develop in a moderate direction; middle classes always do.

On the other hand, Saudi Arabia has for ages encouraged the development of Salafist outlook at the expense of other sects. Saudi Arabia has used funding to build their religious control – do we have a chance to be an effective counterpoint?

There are unintended consequences to Salafist proselytizing, for many Muslims. There are two complications – it's Saudi state sponsorship and it's too "hot." There are more Muslims in India than in all the Arab countries.

There might be value in understanding how the Pentecostals gained footing in Brazil and in other Latin American countries, where the Catholic Church is residually state-sponsored.

Religions are great for communications. You can't stop religion and radical religions. (The spread of religion is) part of the quid pro quo of connectivity, everyone wants all the connectivity but not all the content. (This is not just true for religion, but for things like materialism and pornography. If connectivity is available, vested interests will seek to exploit it.) If you reach out to religions, you have to distinguish between the nations and super-nations. Globalization began in Europe with the rise of nation states, who expressed their power and exercised influence largely through colonial empires. Globalization via this colonial model was successful in North America, less so in Latin America. Hallmarking the gradual collapse of colonial model, North America emerged as a successor. The Far East was the next arena to arise thru the same model.

In the Middle East, who will be the agents of globalization? Most likely it will not be Europeans, nor Japanese, and while North Americans may seek to serve in this capacity, the potential for influence is limited due to the presence of the military as agents. In order to engage the Middle East and Africa in the globalized system, the agent of change will have to be capable of handling the tumultuous environment. Asia has profound demographic issues and has to deal with a far more rapid evolution to handle the transitions – they will be most in need of the job and resource markets in Africa. The Chinese and Indians will teach the Middle East and North Africa how to be Muslim and modern. The US can do only certain things with the military, some things with political and governance, but economics and infrastructure will come from India, China, and Malaysia.

Every culture has a concept of cosmos and chaos. Cyberspace and the Internet fit within this framework. Globalization defuses and cyberspace defuses. This is where some find their empowerment – particularly non-state actors who begin to try to wield power like states. When the leading edge comes into your area, the marginalized welcome it as power while national

entities tend to want to stop. Empowerment of the Internet is like this. As this edge spreads, we get more of the non-state actors – they see loosening of bonds – they don't necessarily want to live in chaos forever. The sense of chaos is universal, but has a curve to it.

The Internet gives rise to universalist visions – transnational visions. We need to understand the larger context of universalist vision – how can the Internet, in breaking down national barriers and erasing geographical limitations, empower non-state actors?

We can monitor Internet traffic and have a vast window into the leadership class thought process (recognizing that there is denial and deception)… "if I can find fundamental times and links, I can manipulate them."

Related matters and general thoughts

While the available tools can be used to gain tremendous insight into Internet power brokers, who they are and how they operate, caution must be exercised. Here's an example of how quantitative techniques for assessing power relationships through e-mail can yield inaccurate results. During a fleet exercise, patterns of email were gathered to figure out the most important people in the network, where they were and what their patterns of usage were. The most important were defined as those that had most emails and sent most emails. That turned out to be the Chaplain. So they pulled the chaplain. Then the most important person was the N1 who was coordinating personnel. Some of the email accounts are positional, that is they were used by different people as shifts changed. N3 and N5 emerged after long analysis. Some thought that you should not take chaplain and N1 off network – it's the best D&D available. Content networks don't map on communications networks.

We Americans typically don't want a relationship, we want a machine that handles our problem. The tool builders are all about the people they are dealing with via cyberspace.

I have voice, video and data that can span the world in seconds. Relationship to me is amorphous – so you need to teach me to use the tools. Cyberspace can be used.

Generation Y is populating the military. What are the implications of deterrence for the next generation – what are they inheriting?

Here's what you are going to be looking at – Apple will completely change the way the world works – every phone is going to be its own broadcasting unit. Direct and indirect communication will contribute to spheres of influence. Every phone is a TV station. Relationships can be built without collusion in transit, perhaps even without any organizational influences.

Instantaneous communications is going to change things – it can be used to build relationships. Consider not just broadcast to the whole world, but broadcast to a small world. Sociologically what emerges are small world networks – clusters with links to other clusters – maybe to religious scholars and their students. Recently, Islamists seem to have the edge in building their relationships, although US and Western youth seem equally adept.

We can change aspects of behavior. Consider racism and sexism in the US – we haven't changed our culture, but over a couple of generations we have changed these aspects of our behavior. Can we hold people to that behavior even when unintentional by setting the conditions? Not going after extremists, but those who can influence those who can be extremists.

This conversation has two threads: deter someone from doing something with cyber, deter someone from using cyber as a threat – and they are different. The two are related. Deterrence is not always direct. But is the issue about using cyberspace to influence or is it about deterring something specific with respect to cyberspace itself?

One approach is to focus on specific acts that you want to prevent or stop. For example, deter a non-state actor from violence.

If we gave 1000 Airmen a video camera and told them to post what they wanted to on a webpage, would that influence a kid to be recruited by Jihadists?

How do you see the effect of the Madrassas and the education push as influencing the size of the pipeline for Jihad? They can push it, but can't create demand that isn't there.

Madrassas are not spreading terror – they tend to be very standards oriented, but adhere more to a local standard. Setting international standards of behavior requires that they teach math science and language – there has likely been over-focus on Madrassas in the hinterlands where they taught rote religion and how to fire a gun. Madrassas are competing with public schools. Perhaps the West can re-instill the legacy of the Middle East as a main keeper of some of the world's intellect and history as it did in the Dark Ages throughout the rest of Europe.

In terms of exerting influence and establishing relationships, the information age is different than previous eras because it is no longer hierarchical in a traditional sense. How states influence non-state actors is only one component of the interactive relationships inherent in the cyber realm. In reality we want non-state actors/ organizations to influence other non-state actors/ organizations – deterrence in the cyber age may mean energizing non-state actors to self-deter.

To practice deterrence in a cyber world, we have to understand the former old world restrictions on who wields power and influence and move away from that traditional hierarchy. For example, with non-governmental groups, self-policing occurs due to the reality that harm affects all NGOs.

In the connected world, indirect connections are more powerful in the collective than direct connections.

What are the means to successful deterrence in cyberspace? One participant stated: I have yet to hear how you can deter behavior in cyberspace. To which another responded: because you can't do it.

However, research is coming out now on how to influence in cyber world but it hasn't gotten into textbooks as yet. This subject is currently widely debated and in need of further exploration.

Deterring VNSA in Cyberspace

Wrap session

We've extended the definition of deterrence to include influence. We should also include actions like deflection and redirection. Look for (potential) allies in populations we want to affect, and those who have similar goals, and support their efforts. Don't just consider allies in a political sense, but all like-minded groups: NGOs, media, artists, pop culture (such as, for example, soap operas). The radicals have reached out; moderate groups should be supported in their out-reach efforts. Don't cede the field to the radicals. Oppose messages that support suicide bombers with messages that discourage suicide bombing. Such are the thoughts behind Deterrence 2.0!

We should be similarly expansive in identifying the forms of media to exploit: digital and analogue. Build sustainable deterrence using digital and analog media.

So is "deterrence" the right terminology? Some think it would be a disaster, because it carries the imprint of DoD and the baggage of the cold war. The application of deterrence in the cold war had all the components; deterrence is our aim at what we are doing. The basic calculation in deterrence is cost-benefit. But "deterrence" carries a strong implication of compellence and coercion.

There are different domains to be considered. We need to deter specific acts, including criminal acts. For much of the rest that we have been discussing, the issue is wider, like leveling the idea space.

A way ahead is by enabling, empowering, and allying ourselves with people who are in some ways like minded. However, a public and overt process may not work in this case – public association with US may not be helpful. What we want is to empower with less overt action.

Concepts of cold war deterrence are largely the same as those concepts currently being discussed. The difference is whether actions taken are direct or indirect. In cyber deterrence with non-state actors, actions will require more indirect actions. Our presence in the cyber world should be friendly, welcoming to relationships. Our cyber profile would benefit from a shift in public perceptions.

A small percentage are out to kill and it's that tiny minority that we are out to deal with and prevent the spread of their philosophy. There is an issue about whether we can influence a radical terrorist organization – less likely to change their mindset, but can still influence them, can influence that core element by influencing the sea in which they swim – although we believe they are winning, they are sure that we are winning because of the influence of globalization. You have to have redirection measures because the youth want to act – give them something constructive to do: a tiny hard core minority is viewed as glamorous by too many and dissuasion is critically important. Cyberspace gives us opportunity to get many alternative messages out.

If someone is violently bent, fundamentally fixated, we may not be able to deter them from their view—but influence, especially indirect, may still be possible. In addition, although de-radicalization may not be possible, the fence sitters and moderates may be susceptible to influence. The goal may be not to change the fence sitters way of thinking, rather to prevent the radicals from changing their views and swaying them to their side

This tiny radical group appears glamorous to the large group. There exist fault lines on the radical side that we can explore. We might be able to make them seem less glamorous. Occidentalism/Globalization is so influential—it is impossible to undo this influence—and this is why in the eyes of people such as Osama Bin Laden we have won the cultural war.

Several participants pointed out that globalization has been changing the international environment in a way that the radicals don't like. Open news sources are an engine of that: BBC, al-Jazeera. We may view al-Jazeera as providing a Muslim point of view, but the radicals see it as spreading information that undermines their cause. Radio Free Europe satisfied a similar demand during the cold war. (That model should be extended into the globalized cyberworld.)

Today there is a demand for identity in a rapidly changing world. A central principle is (could be): core American values of professionalism, economic upward mobility, with a dose of piety. We might encourage piety through non-violent Muslim clerics, support those who share values with us and oppose the radicals. Encourage economic upward mobility indirectly through our partners who have what the youth need – trade. Discover how to educate for professionalism and need partners to employ the newly created professionals (currently émigrés because of lack of opportunity).

An unconventional warfare campaign contains the exertion of influence at local levels— go right through the local establishments as the ones who receive support and use it directly – as opposed to going through a federal government.

Micro-targeting is not a new concept– but the tools are new, visibility on the Internet is ability to find and work with presences on line.

We could do things like find the websites that are most popular with Arab or Iranian youth (who speak English, or who are living in the US), and make those websites available in local languages. There is a huge expansion in the Arab language on the web and a huge lack of content in Arab language. We have to be careful to take into consideration the huge diversity in the Islamic world.

We need the open playing field of a relatively unconstrained Internet environment. How do we keep the Internet free and open? Promotion of open cyberism ***is*** a deterrence strategy. However, doing so means that from time to time you will have a small group that uses the net to enable them to blow up a subway – we may have to tolerate the occasional violent act. We need the openness to mine the openness, we also need to solve our own stability and continuity - we have to have resiliency and continuity; this points to the need to have the appropriate network security – it will get worse on a case by case basis and the cyber security industry is in a hole and fighting an uphill battle.

We do better when everybody does better and it should be in our national strategy to provide it and defend the cyber world. One participant suggested that we could advocate a UN or some other international body to govern it.

Perhaps we can put this in some form of a query framework

1. how are our adversaries using the Internet and cyber media in general

2. what do we do about that
3. how do we go beyond that

We should have a better understanding of how we can use cyber tools to understand our environment on a persistent basis. In order to gain such insights, we need to look at the socialization process, forming of communities and effect of that type of organization and empowerment.

Appendix C: Acronyms

ASAM	Adaptive Safety Analysis and Monitoring (U. Conn. tool)
ATDS	Advanced Terror Detection System (model from Ben-Gurion University)
BN	Bayesian Network
CASOS	Computational Analysis of Social and Organizational Systems (CMU group)
CMU	Carnegie Mellon University
CNN	Cable News Network
COA	Course of Action
CPU	Central Processing Unit
DBN	Dynamic Bayesian Network
DIME	Diplomacy, Information, Military, and Economic
DIMEFIL	Diplomacy, Information, Military, Economic, Financial, Intelligence and Law Enforcement
DMU	Data Marshalling Unit
DNA	Dynamic Network Analysis (CMU approach)
DoS	Denial of Service
DWAS	Dark Web Attribute System
FTP	File Transfer Protocol
GISC	Global Innovation and Strategy Center (STRATCOM)
GMM	Gaussian Mixture Models (analysis algorithm)
HMM	Hidden Markov Model
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
IDA	Institute for Defense Analyses
IMC	Intelligent Memory Core
IMF	International Monetary Fund
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
KNN	K-nearest neighbor (analysis algorithm)
MDS	multidimensional scaling (analysis algorithm)

MRSA	Methicillin-resistant Staphylococcus aureus
NEMESIS	Network Modeling Environment for Structural Intervention Strategies
NGO	Non-Government Organization
NSA	Non-State Actor
NSI	National Security Innovations
NYPD	New York Police Department
ODL	Organizational Descriptive Language
ORA	Organizational Risk Analysis (tool from Carnegie Mellon University)
OSD	Office of Secretary of Defense
PCA	Principle Component Analysis (analysis algorithm)
PNN	Probabilistic Neural Networks (analysis algorithm)
SMA	Strategic Multi-layer Assessment
SOA	Service Oriented Architecture
SOI	Spheres of Influence
SPAWAR	Space and Naval Warfare Systems Command (US Navy)
SRC	Syracuse Research Corporation
STRATCOM	Strategic Command
SUNY	State University of New York
SVM	Support Vector Machines (analysis algorithm)
TB	Terabyte = 2^{40} bytes, approximately 10^{12} bytes
USG	US Government
VNSA	Violent Non-State Actor