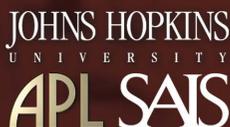


PROCEEDINGS ON STRATEGY,
ANALYSIS, AND TECHNOLOGY

UNRESTRICTED WARFARE SYMPOSIUM

20 - 21 MARCH 2007

SPONSORED BY:



OUSD(P)
ODPA&E



RONALD R. LUMAN, EXECUTIVE EDITOR

UNRESTRICTED WARFARE SYMPOSIUM 2007

PROCEEDINGS ON COMBATING THE UNRESTRICTED WARFARE THREAT:

INTEGRATING STRATEGY, ANALYSIS, AND TECHNOLOGY

20-21 MARCH 2007

SPONSORED BY:

JOHNS HOPKINS
UNIVERSITY

APL SAIS



RONALD R. LUMAN, EXECUTIVE EDITOR

ACKNOWLEDGMENTS

Executive Editor: Ronald Luman

Managing Editor: Ellen Wilkinson

Project Editors: Natalie Dickins

Judith Marcus

Daniel Portwood

Weeta White

Ellen Wilkinson

Art Directors: Catherine Peacock

Ian Courtney

Photo Credit: Department of Defense Image Library

Special thanks to our sponsors at: the Office of the Undersecretary of Defense for Policy [OUSD(P)]; the Office of the Director, Program Analysis and Evaluation (ODPA&E); the Defense Advanced Research Projects Agency (DARPA); and the National Intelligence Council (NIC).

A complete list of symposium contributors can be found at the symposium's website: www.jhuapl.edu/urw_symposium/

Copyright © 2007

By The Johns Hopkins University Applied Physics Laboratory

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher.

Requests for permission to make copies of any part of the work should be mailed to:

Dr. Ronald R. Luman,
Director, National Security Analysis Department
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, Maryland 20723

Printed in the United States of America.

Contents

Foreword – Welcome and Perspective on Unrestricted Warfare Ronald R. Luman	1
---	---

CHAPTER 1

FEATURED PAPERS

1.1 Warfighter Perspective on Integration of Strategy, Analysis, and Technology James Cartwright.....	13
1.2 “Know Your Enemy”—The Importance of Sun Tsu’s Admonition Bruce Hoffman	37
1.3 The Achilles’ Heel of Analysts Michael Bauman	41
1.4 Technology Policy Message: Adapting to URW Anthony Tether	57
1.5 Private Sector Viewpoint—Economic Infrastructure/ Systems Resiliency Alfred Berkeley.....	77
1.6 Intelligence Community Perspective on the Maturing URW Threat Mathew J. Burrows	97

CHAPTER 2

THE NATURE OF URW

2.1 Moderator’s Summary Thomas Keaney	107
2.2 Scenarios for Future Conflicts Michael O’Hanlon.....	111
2.3 Calibrating the WMD Threat Brad Roberts	121
2.4 The Jihadist Threat Mary Habeck.....	135
2.5 Questions and Answers Highlights Transcripts	143

CHAPTER 3

TAILORED DETERRENCE: WHAT WILL IT LOOK LIKE?

3.1 Tailored Deterrence: What Will It Look Like?
Thomas M^cNamara, Jr.161

3.2 Can Deterrence Be Tailored?
Charles Lutes163

3.3 Tailored Dissuasion and Deterrence?
Jasen Castillo173

3.4 Questions and Answers Highlights
Transcripts183

CHAPTER 4

ANALYTIC SUCCESSES AND APPLICABILITY TO URW

4.1 Moderator’s Summary
L. Dean Simmons191

4.2 Assessing Irregular Warfare
Timothy Bright197

4.3 Complex Adaptive Systems, Multiagent-Based
Models, and Some Heuristics Regarding Their
Applicability to URW
Andy Ilachinski205

4.4 Economic Analysis and Unrestricted Warfare
Gary M. Shiffman223

4.5 Questions and Answers Highlights
Transcripts237

CHAPTER 5

URW IN THE INFORMATION DOMAIN

5.1 Moderator’s Summary
Timothy Galpin251

5.2 The Digital Dimension
James Gosler255

5.3 Cyberspace ... the undeclared war!
Daniel Wolf269

5.4 Lead-Turning the 21st Century Fight: CYBERSPACE
Steven McPherson281

5.5 Questions and Answers Highlights
Transcripts297

CHAPTER 6

URW IN THE PHYSICAL DOMAIN

6.1 Moderator's Summary	
José Latimer	305

CHAPTER 7

SENIOR PERSPECTIVES

7.1 Eric Olson	313
7.2 Albert Calland	319
7.3 Nancy Brown	323
7.4 Thomas Mahnken	325
7.5 Philip Mudd	329
7.6 Questions and Answers Highlights	
Transcripts	335

AFTERTHOUGHTS

John McLaughlin	347
-----------------------	-----

APPENDIX A

Symposium Agenda	349
------------------------	-----

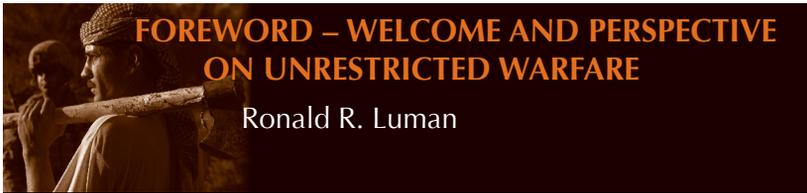
APPENDIX B

Acronyms and Abbreviations	353
----------------------------------	-----



FOREWORD

**WELCOME AND
PERSPECTIVE ON
UNRESTRICTED
WARFARE**



INTRODUCTION

On behalf of The Johns Hopkins University's Applied Physics Laboratory and its Paul H. Nitze School of Advanced International Studies, I welcome you to this 2007 symposium on Combating the Unrestricted Warfare (URW) Threat: Integrating Strategy, Analysis, and Technology.

This year, the symposium is co-sponsored by government leaders in the strategy, analysis, technology, and intelligence communities: the Office of the Undersecretary of Defense for Policy [OUSD(P)]; Office of the Director, Program Analysis and Evaluation (ODPA&E); the Defense Advanced Research Projects Agency (DARPA); and the National Intelligence Council (NIC). We have a unique opportunity to join an emerging community of experts that seeks to meet the unrestricted warfare threat by integrating strategy, analysis, and technology.

In addition to our scheduled keynote, luncheon, and dinner featured speakers, we have organized roundtables to address particular challenge areas and seek to integrate diverse perspectives to further develop an understanding of unrestricted warfare threats and strategies, explore approaches to analysis and assessment, and examine technological counters to threats

Dr. Ronald R. Luman is Head of the National Security Analysis Department at The Johns Hopkins University Applied Physics Laboratory. Dr. Luman has a broad base of technical experience in areas such as ballistic missile accuracy, unmanned undersea vehicles, countermine warfare, national missile defense, and intelligence, with particular emphasis on system of systems engineering.

in both the information and physical domains. Accordingly, we have five roundtables this year:

- Strategic Policy: The Nature of URW
- Analytic Successes and Applicability to URW
- URW in the Information Domain
- URW in the Physical Domain
- Strategic Policy: Tailored Deterrence

During the next 2 days, I encourage you to network and actively participate during breaks, to formulate new ideas, and to forge collaborative relationships with other participants. Seize opportunities to participate, inquire, and respond to the diverse topics presented using response cards, interactive tablet PCs, or handheld devices. Our common objective is to meet the URW challenge through an integrated approach.

We have produced summary papers from transcripts and presentations submitted by experts leading in the URW challenge. Content submitted in presentation graphics has not been altered in any way.

WHAT IS UNRESTRICTED WARFARE?

In 2006, the URW Symposium focused on exploring the diverse nature of unconventional warfare. This new threat, which has come to be known as “unrestricted warfare” (URW). Unfortunately, URW is another NOT word that we tend to use when we do not fully understand something. It joins unconventional, irregular, and asymmetric as terms in our conflict vocabulary; but it is broader than all of those. URW spans two of the four “security environments” the Department of Defense (DoD) identified for use in strategic planning, Irregular and Catastrophic, and may extend to the Disruptive (Figure 1).

Unrestricted warfare involves both state and nonstate actors seeking to gain advantage over stronger state opponents. These actors will employ a multitude of means, both military and nonmilitary, to strike out during times of real or perceived conflict.

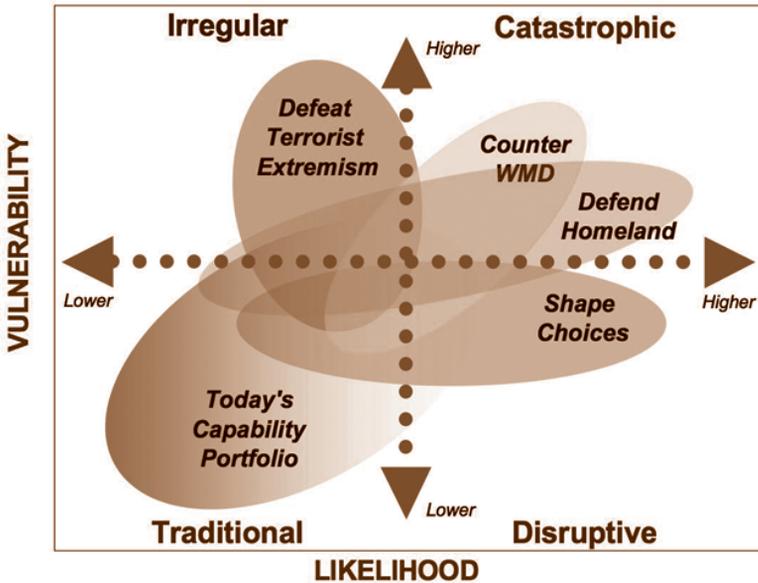


Figure 1 The DoD Security Environment Quadrant

The first rule of unrestricted warfare is that there are no rules; nothing is forbidden. Unrestricted warfare employs *surprise and deception* and uses both civilian technology and military weapons to break the opponent's will. The recent book by Qiao Liang and Wang Xiangsui offers an overview of unrestricted warfare, utilizing "*unrestricted employment of measures, but restricted to the accomplishment of limited objectives.*" Among the many means cited in their description of unrestricted warfare are *integrated attacks* exploiting diverse areas of vulnerability to produce a grand strategy:

- Cultural warfare by influencing or controlling cultural viewpoints within the adversary nation
- Drug warfare by targeting an adversary nation with illegal drugs
- Economic aid warfare by using aid dependency to control a targeted adversary
- Environmental warfare by despoiling the natural environment of the adversary nation

- Financial warfare by subverting the adversary's banking system and stock market
- International law warfare by subverting the policies of international or multinational organizations
- Media warfare by manipulating foreign news media
- Network warfare by dominating or subverting transnational information systems
- Psychological warfare by dominating the adversary nation's perception of its capabilities
- Resource warfare by controlling access to scarce natural resources or manipulating their market value
- Smuggling warfare by flooding an adversary's markets with illegal goods
- Technological warfare by gaining advantage or control of key civilian and military technologies
- Terrorism

URW CHARACTERISTICS

Unrestricted warfare demands “unrestricted employment of measures but restricted to the accomplishment of limited objectives.” It employs the elements of surprise and deception in asymmetric attacks. These attacks can be integrated to exploit diverse areas of vulnerability of a conventionally stronger opponent. Specifically, battlefields expand beyond the conventional physical domain to break the opponents' will in areas that are visible and have a tangible and threatening effect on the target nation's political base. For more than a decade, we have witnessed a surge of terrorist acts. Bruce Hoffman, in his book *Understanding Terrorism*, characterizes these acts as five processes designed to achieve key objectives:

1. *Attention.* Terrorists seek media attention to themselves and their cause through dramatic, violent acts.

2. *Acknowledgment.* Terrorists seek to translate their newfound notoriety in the states or international community into acknowledgment, sympathy, and support for their cause.
3. *Recognition.* Terrorists attempt to capitalize on the interest and acknowledgment that their violent acts have generated by obtaining recognition of their rights or acceptance of the justification for their cause and or their organization.
4. *Authority.* Terrorists seek the authority to effect the changes in government and society reflected in their movement's struggle. This may involve a change in government or in the state structure, redistribution of wealth, adjustment of geographical boundaries, assertion of minority rights, imposition of theocratic rule, or other transformation.
5. *Governance.* Terrorists seek to consolidate their direct and complete control over the state, its homeland, and its people.

ADVERSARIAL CHARACTERISTICS OF URW

Unconventional warfare employs small, well-organized units. These organizations are cell-structured, not organized as a hierarchical military force.

They are integrated within society, not apart from it; and they operate globally, using technology that broadens their reach beyond regions. State and nonstate actors may form ad hoc and unexpected alliances of convenience.

URW EFFECTS

Here, the few can impact the many with a global reach enabled by advanced information technology. The effect is that tactical level engagements can immediately affect strategic

security postures. Insurgents and terrorist groups spread like viral organisms, adapting and shifting command and control strategy and tactics. Their ability to adapt, change strategy, and persist serves to empower and shape generations of disenfranchised or radicalized activists, both here and abroad. This symposium provides disturbing insights into the dramatic shifts in traditional Islamist doctrine, the adoption of irregular warfare strategies by both state and nonstate adversaries, and the global spread of new warfare technologies that have the potential to increase the effectiveness of adversaries' attacks.

THE NATIONAL CRITICAL CHALLENGE

The United States must adapt its national security focus to fighting and defending itself against the radical Islamic insurgency and future adversaries who choose catastrophic terrorist attacks as their weapon of choice. This involves development of strategy, concepts, and capabilities appropriate to protracted conflicts of an unrestricted nature.

Unrestricted warfare will manifest itself across the full spectrum of political, social, economic, and military networks, blurring the distinction between war and peace and between combatants and bystanders. This type of war is not new, as noted by President John F. Kennedy in 1962. What is new and different today is the global reach of adversaries, enabled by advanced information technology.

“This is another type of war, new in its intensity, ancient in its origins—war by guerrillas, subversives, insurgents, assassins; war by ambush instead of by combat; by infiltration instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him . . . It requires in those situations where we must counter it . . . a whole new kind of strategy, a wholly different kind of force, and therefore a new and wholly different kind of military training.”

President John F. Kennedy

USMA Graduation Speech, 1962

STRATEGY, ANALYSIS, AND TECHNOLOGY INTEGRATION

We borrow Qiao and Wang's description of URW to acknowledge their perspective, but we seek our own assessment of what leading strategists, analysts, and technologists should consider viable future force capabilities and strategies.

We encourage your active participation, networking, and knowledge sharing to form a new, integrated community dedicated to countering our increasingly sophisticated adversaries. At this symposium, you have self-identified as being 40% strategists, 40% analysts, and about 20% technologists.

We are forming a multidisciplinary community with balanced perspectives and talents. Political scientists, historians, and international relations people tend to gravitate toward strategy. Naturally, scientists and engineers tend to gravitate toward technology; and analysts can come from a variety of backgrounds but are principally technically trained.

Figure 2 illustrates the integration of these distinct communities and what we need to draw from one another to form effective solutions to combating unconventional adversaries. It is imperative to tailor deterrence postures and courses of action (COA), Science and Technology (S&T), and Research Development Technology and Engineering (RDT&E).

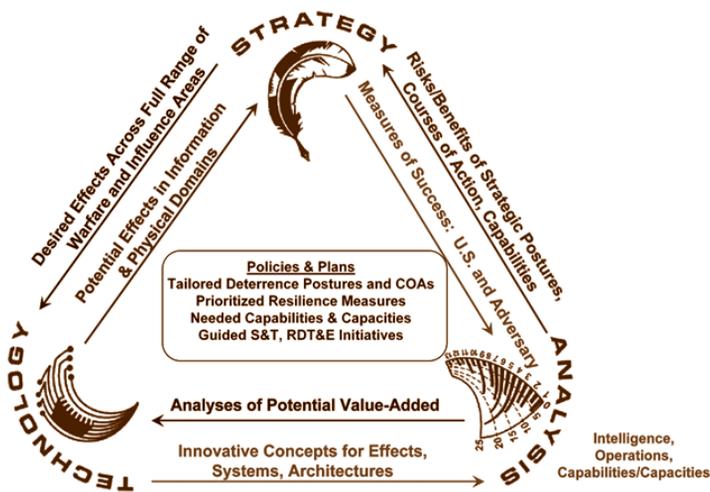


Figure 2 Integrated Strategy, Technology, and Analysis

WHAT STRATEGISTS, ANALYSTS, AND TECHNOLOGIST NEED FROM ONE ANOTHER

Specifically, the *strategy community* needs to understand the risks and benefits of various options for strategic postures, courses of action, and calls for additional capabilities. It needs insights from qualitative and quantitative analyses to guide the development of the full range of national security postures, which include tailored deterrence and adaptation of our offensive and defensive capabilities. The strategists should also understand what is technologically feasible with regard to potential effects in both the information and physical domains, and what strategy can be adapted from those domains.

The *analysis community* is unique in that it spans several domains, including intelligence, operations, and planning of new capabilities and capacities. Hence, the analysts cannot effectively work in a strategic or technological vacuum. Analysts need insights into U.S. and adversarial measures of overall success, not detailed measures of performance or evaluation but overall what each side values and what defines success. And, analysts need ideas and innovative concepts for effects, systems, and architectures to close areas of vulnerability.

The *technology community* needs to understand what effects are desired, operationally feasible, and potential innovative means to achieve those effects. For example, General James E. Cartwright is challenging the technology community with his Global Strike concept to reach out and touch any point on the earth in a short period of time. The analytic community can provide insights regarding the value-added of candidate technology. Especially useful are quantitative measures comparing new concepts to existing methods.

Together, we develop integrated policies and plans to enhance our effectiveness against adversaries employing URW. As illustrated in the center of Figure 2, we should:

1. address tailored deterrence postures and have the means to assess specific candidate courses of action;
2. develop prioritized resilience measures for homeland defense to enhance our own deterrence posture against URW threats;
3. develop integrated technical plans for needed capabilities and capacities across both the joint and interagency environments; and
4. provide focused guidance to our increasingly precious S&T and RDT&E initiatives to enhance the potential for transitioning technology to operational capability.

Our adversaries are increasingly sophisticated in integrating their efforts across the full spectrum of activity that constitutes unrestricted warfare. We will have to do the same to combat the threat.

Together, we need to understand what are the tailored deterrence postures that are founded in solid technology and understand the trade-offs.

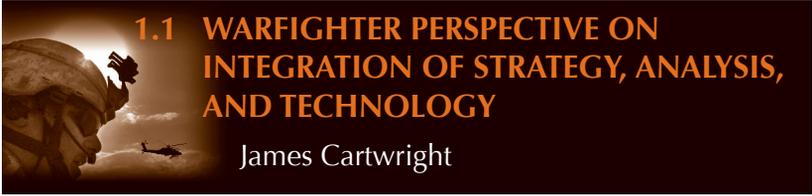
REFERENCES

1. *Unrestricted Warfare*, Col. Qiao Liang and Col. Wang Xiangsui, Panama City, Panama: Pan American Publishing Co., 2002.
2. *Understanding Terrorism*, Bruce Hoffman, New York: Columbia University Press, 1998.



CHAPTER 1

**FEATURED
PAPERS**



1.1 WARFIGHTER PERSPECTIVE ON INTEGRATION OF STRATEGY, ANALYSIS, AND TECHNOLOGY

James Cartwright

GENERAL CARTWRIGHT'S ADDRESS

We were getting up this morning in Nebraska to come to this symposium, and it was, as you can imagine, dark and cold with the north wind blowing on us—and we were making all the normal quips about the weather—such as, the only thing between us and Canada to slow the cold wind is barbed wire, and we had spent the last three months shoveling global warming... So it is a welcome change of climate to be here; it is good to have this opportunity. I applaud this conference and the agenda and the forum. And the warmer weather here.

My intent is to irritate you for at least 30 minutes. Then you can reverse the roles, and we will take the Q and A in any direction you want to go.

I think when you look at unrestricted warfare—when you look at warfare in the world that we live in today—a few things—at least from the military side of the equation and really for everybody—

General James E. Cartwright became Commander, United States Strategic Command (USSTRATCOM) in July 2004, responsible for the global command and control of U.S. strategic forces, providing strategic capabilities and options for the President and Secretary of Defense. Previously, he supported the Chairman of the Joint Chiefs of Staff in force structure requirements; studies, analyses, and assessments; and the evaluation of military forces, plans, programs, and strategies. He has served for more than 40 years with distinction in military operations and as a Naval Aviator. General Cartwright is a distinguished scholar, completing a fellowship with the Massachusetts Institute of Technology and an M.A. in National Security and Strategic Studies from the Naval War College.

should emerge. All of us here can justifiably assert that things really have changed in the world, but the pace of change in activity and the scale of that activity are truly phenomenal. When you think about the fall of the Berlin wall in 1989 and Operation Desert Storm in Iraq in 1991, and Afghanistan in October 2001, then back to Iraq in 2003—when you think about tsunamis and hurricanes and typhoons and volcanoes and earthquakes and two pandemics—and all of that occurring well within the short span of less than a single adult life, that should give you pause—because when you look back in history, that kind of activity is really unprecedented.

In the same context, consider the shift from the construct of the United States and Soviet Union as two monolithic powers engaged in a bipolar conflict, to a strategy requiring that the United States have the ability to conduct two regional wars or two major theater conflicts, focusing on four critical regions, as I believe Defense Planning Guidance (DPG) describes it: Northeast Asia, East Asian Littoral, Middle East/Southeast Asia, and Europe. That transition has happened in a very short period. Add to that the realization that the U.S. needs to think about its home territory, too.

Now we have to consider homeland protection, four critical regions, and two simultaneous wars—so the scope and the scale and the pace of the challenge have matured to the point where we have to find a way to put this in some sort of context. We have to look at how we are going to integrate this strategy, the way we analyze it, and the technology we need to manage it.

Much of the discussion about finding a perspective for the incredible pace of change and how to respond to it hinges on whether you approach it with concepts such as Thomas Friedman's flattening earth,¹ in which the playing field is being leveled, or you talk in terms of the globalization construct. The unprecedented access to technology, to information, to knowledge has fueled this activity in ways that we really are just now starting to understand.

1 Thomas L. Friedman, *The World Is Flat: A Brief History of the Twenty-first Century*, 1st edition, Farrar, Straus, Reese, and Giroux, 2005, ISBN 0-374-29288-4; "Updated and expanded," Farrar, Straus and Giroux, 2006, ISBN 0-374-29279-5

Even though we may find ways to explain it and understand it—what 21st century warfare and deterrence and assurance look like in that environment is a colossal challenge.

In 1999, a gent by the name of bin Laden moved from Saudi Arabia to Afghanistan to the caves of Afghanistan. What the heck are you going to do from a cave? Around the same time, in 1998, a guy by the name of Shawn Fanning—a college student—worked away at his computer writing code trying to figure out how to share music peer to peer; and within a few short months, he was able to capture—with a small organization that he put together called Napster—25% of the profit margins of the record industry. Likewise, a loosely knit alliance called Hamas took on a major regional nation state with credibility.

“When you think about the fall of the Berlin wall in 1989 and Operation Desert Storm in Iraq in 1991, and Afghanistan in October 2001, then back to Iraq in 2003—when you think about tsunamis and hurricanes and typhoons and volcanoes and earthquakes and two pandemics—and all of that occurring well within the short span of less than a single adult life, that should give you pause—because when you look back in history, that kind of activity is really unprecedented.”

What are the implications of all of this activity and how do you start to think about strategy? How do you think about an effective way to manage the constructs of governance in that kind of an environment? What kind of capabilities do you want to have? How is it going to affect culture? How is it going to affect the way we do business? How do you play in this sandbox?

When we started to work our way through these issues at STRATCOM—the new missions and the accelerated activities—trying to understand the model by which we could start to participate in a meaningful way in this environment, the challenge that was in front of us really had little to do with the the traditional approach to business, which had always been: “How can I build

this kingdom—how can I turn it from one castle into an empire?” All of the standard “Type A” things that we tend to do as leaders and people really were not going to get us any place.

The simple As and Bs and Cs were that we had a headquarters consisting of 5000 people, we now had five new missions, and we had to build a new structure for managing them—so the typical conclusion would be: “I guess I should be four or five times larger.” That did not work for Ma Bell, it didn’t work for IBM, and it was not going to work for STRATCOM. We now had a different environment that we had to work in, so we had to move forward in a different way. I will quickly step through a series of attributes to our approach with elevator speeches on each attribute, and I will be happy to let you pick them apart in the Q and A.

ATTRIBUTES OF THE NEW STRATCOM APPROACH

The first attribute I want to discuss is speed—and then I will examine cyberspace and scale. What is the definition of speed in the current environment? Is it going Mach Two in a fighter? Is it a tank that goes faster, jumps higher? Is that what we mean by speed?

Defining Speed

Where I generally face the biggest challenge in discussions about speed is in trying to bring it into a different dimension for intelligence, surveillance, and reconnaissance (ISR). When we entered into the new construct of two major theater wars with the added consideration of four critical regions, what has always been a limiting factor became even more important: How long does it take to swing intelligence, surveillance, and reconnaissance from one theater to the next?

We in the military start with the issues of getting assets into the new theater: “Okay, I’ve got to position the tankers so that I can get the aircraft, and I’ve got to build a bridge so that they can get from one theater to the next. How many days does it take to find the tankers? How many days does it take to move all of the

assets to the new theater—get them bedded down, get them ready to go?”

No matter what you do, that process is measured in days that are more than the fingers that I have on my hands (so as a Marine, it is beyond my comprehension). It simply takes a long time to position assets. But the reality is that from space, we are just dealing with a few minutes. In our system of joint military and government and intelligence agencies, there are at least 15 committees between me and those decisions, and each committee gets at least a day to debate it, and they all tend to use their “no” votes rather than “yes” votes. When you get to the theater, the objectives are: find, fix, and finish. So, if it takes me 10 or 15 days just to get the assets there to find—it is simply too slow. It is too slow when you are dealing with the weapon of choice today, which is a short- or medium-range ballistic missile that can pop out, shoot, finish its time of flight, and have an effect in something under 10 minutes easily. So, we are faced with some mismatches that generally stem from the bureaucracy—that conflict with our need for quick response in different theaters.

“How are you going to erect your defense in 300 milliseconds? How are you going to detect that you are under attack and do something about it in 300 milliseconds?”

The concept that we are pushing to any place on the face of the earth in less than an hour isn’t about hypersonics—although that kind of speed is certainly essential—it’s about how to find something, fix it, and finish it any place on the face of the earth in an hour. It’s not only about how fast you can make something fly or how fast you can find a target—it’s putting all of the pieces together in an hour. That’s the challenge. Technology can find things, get something that far, that quickly—technology can make it precise; but how do you put it all together inside the decision timelines of your adversary? That is at the heart of the issue in the new world with which we are now dealing. It is the decision timelines of the adversaries that we must beat; if we can stay inside

of those timelines, we have a reasonable chance of outthinking, outsmarting, and outmaneuvering them.

Cyberspace

Another aspect of how we define speed is a factor that I believe challenges the notion that we can continue to do what we have always done to conduct warfare by merely making it go a little faster—that factor is cyberspace, the “cyber world.” Decision cycles inside cyberspace are significantly different; committees do not do well in cyberspace. If an adversary wants to release a cyber virus from Baghdad—and he takes the long route and goes out to geosynchronous orbit and comes back down in Nebraska—he can do it in about 300 milliseconds.

How are you going to erect your defense in 300 milliseconds? How are you going to detect that you are under attack and do something about it in 300 milliseconds? That’s the speed that we’re dealing with in decision-making and in maneuvering and in command and control as we move through the 21st century. If you do not have a strategy to operate in that environment, if you do not have the technology, if you cannot assess what is happening to you—then you are going to be outmaneuvered.

A major challenge that the cyber environment brings is that it makes geography irrelevant. For the most part, our laws, our governance—the nation-state construct—is based on property—geography. The cyber world does not pay much attention to geographic definitions and constraints. How do you apply the constructs that we have today for governance to cyberspace?

So the issue of speed of decision-making, governance, and the ability to manage requires more than just adapting what we have today to work faster. If we do not understand that and make it a priority, then we will continue to build the next bombers and ships faster and faster, which is pretty much totally irrelevant.

Scale

The next attribute I want to discuss is scale. I tend to use a business analogy to explain the process of scaling for agility. If you

are dealing on a global basis, how do you achieve agility—that is, the ability to tailor your activity to an individual actor? That is hard to do strictly from within a single global construct.

STRATCOM has built a taxonomy that says that STRATCOM will be a global provider, but the regional combatant commanders will give us the agility for the transactions with the local actors; they can tailor the tools that STRATCOM can bring to them to the scale needed for that local area and activity. STRATCOM has to provide enough breadth and scalability in that toolset to be compelling.

Most of the transactions that occur between the global provider—STRATCOM—and the regional activity involve “finding the seams.” In business, the process most analogous to the STRATCOM strategy is called arbitrage. How do you find the seams, expand them, exploit the discrepancies, and scale your response to the problem quicker than your competitor or adversary can? STRATCOM provides the scale, finds the seams, and helps the regional commander tailor his response—but he provides the agility through individual judgment; he understands the adversary, he can do the lead-turning, he can put the pieces together to make his response effective against that particular adversary.

When STRATCOM dealt in a monolithic strategy called Mutual Assured Destruction, it had one tool. We simply cannot address the world that way anymore. The Quadrennial Defense Review (QDR) and the Nuclear Posture Review and other studies have all concluded that we have got to have a bigger toolset to counter a more diverse threat—a faster emerging threat, an agile threat. I believe that providing a broader set of tools to respond to an ever changing threat requires a critical construct: distributed attributes.

DISTRIBUTED ATTRIBUTES

This concept, I believe, is the least understood amongst us in the military. In business, many people define “distributed” as a strategy of buying up all of your competitors, so that once you

are established in many different locations, you are distributed. The military equivalent of that is: “I will use some Navy and some Army and some Air Force and I’ll have them moving around inside my theater, so now I have distributed attributes.” I do not think that is the essence—or the value—of being distributed. To me—and where STRATCOM has taken the command—distributed has more to do with leverage.

If you are a business, and you try to buy up everything to gain the advantage of being widely distributed, generally the oversight and management of your organization become so cumbersome and lethargic that your competitors can soon run circles around you. The same is true on the military side: Headquarters become huge, forces overlap so much that they interfere with one another, and the ability to be agile is lost.

“STRATCOM provides the scale, finds the seams, and helps the regional commander tailor his response—but he provides the agility through individual judgment; he understands the adversary, he can do the lead-turning, he can put the pieces together to make his response effective against that particular adversary.”

After talking with many people in the organization as I was coming into the job, we set an axiom at STRATCOM. We will not change a process unless we can improve whatever it is that we are changing by at least a factor of five. We apply our own version of the Disney Principle [the iterative process of dreaming, realizing, and criticizing]—if you cannot improve something fivefold, you are eliminated from the organization. Sounds brutal, but the objective is to prevent building big organizations that will become a hindrance. That is not what being distributed is about.

Let’s take the example of ISR. STRATCOM wanted to be able to build an ISR process second to none—global in nature, with the scale, pace, and agility that we needed to fulfill our new missions. We could have tried to build that kind of organization at Omaha. With 10,000 or 15,000 people in 10 or 15 years, we might have

come close, although I doubt it. It was much easier to take 200 people out of our headquarters, make them a component of the Defense Intelligence Agency (DIA), and tell them, “go!”—which is exactly what we did, and what we did in all of our functional areas.

Do not build it—distribute yourself, diversify, find a way to leverage off of existing excellence, and then drive it to a pace and a scale that is aligned with whatever your objectives are.

I can accomplish a lot more by tapping an established organization that is already 20,000 or 30,000 strong, already global in nature—by simply placing a couple hundred people in there to drive them crazy and to align them with what STRATCOM is trying to achieve. That is how STRATCOM has moved across all of its mission areas: The DIA has our ISR functionality; the National Security Agency has our cyber functionality; the Defense Threat Reduction Agency (DTRA) does nonproliferation/counter proliferation/consequence-management for us.

We do not send intelligence people into DIA—we take recovering F-16 pilots and warfighters and put them into the organization. A different culture—put it in there. Let them get in and amongst them. Tell them what it is we need—not what they want to give us. That is how STRATCOM is getting leverage. If that strategy results in anything less than a factor of five improvement on what we are doing, we are out of there. Unfortunately, in some cases, that has meant that we have had to tell some organizations: “Sorry, not interested.”

CHANGING THE ORGANIZATIONAL CULTURE

Trying to understand where we could gain value and changing the organizational construct to this kind of a model was easy verbally but difficult culturally. The words flow readily; everybody says: “The first thing we have got to do is be joint.” So we all sing kumbaya and hug and say: “We are joint. And the last war was the most joint conflict in the world. We’ve never seen better joint. Thank God there was a river to keep the Marines and the Army apart as they moved north. Thank God that the Army had enough

spare radios so they could give them to the Marines so they could talk to each other.”

That was our definition of joint. The reality is we are not terribly joint. Beyond that, we have the issue of what I will say is oftentimes more words than substance—integration with our allies in warfighting—really cumbersome, really poorly done. How do you build an organization that from the beginning integrates those two as a precept, and how do you put substance into it? It is one thing to put the idea of functional integration on your marquee, and altogether another thing actually to be able to do it.

STRATCOM is working its way through the issues of distributed attributes and integration, but the biggest challenge is not technology, it is culture. We have got to figure out a way to keep what is valuable in the existing culture and discard what is getting in the way.

Industry and Academia

There are two more pieces that we have endeavored to pull into this activity at STRATCOM that I would like to mention. If you look at history, at least for STRATCOM, I think that we have lost some aspects of our relationships with industry and academia.

The challenge we face is how to bring industry and academia to the table—not as an adjunct or an afterthought—but as integral players, to provide substance to the ideas of plug-n-play and integrated synchronized activities. A possible solution may consist of putting an American industry and an Allied military together to solve problems for which there is no clear authority or jurisdiction, but which might have a significant impact—such as, for example, the Proliferation Security Initiative (PSI), which is working with the international community to deter the spread and use of weapons of mass destruction and their delivery systems.

How do you start to mix and match capabilities for the problems you are really trying to solve; and how do you ensure that these capabilities drive you in the direction you want to go—not set you up for the fight you might not want to have? For issues like PSI, the question is, where do we really want to end up

in deterrence? What is the ultimate goal? The failure of deterrence is conflict. So if we are trying to deter, the tools we need in what we call Phase Zero and Phase One are often not battleships and airplanes. How do you start to bring that to the table for the nation so that you can broaden your toolset? The organizational construct is critical for that.

“Do not build it—distribute yourself, diversify, find a way to leverage off of existing excellence, and then drive it to a pace and a scale that is aligned with whatever your objectives are.”

I will tell you that we are not there by a long shot; but setting an objective and grading ourselves based on how well we are moving towards that objective helps the organization. STRATCOM is pushing hard on that, and I think that a lot of what we all will be discussing today will center on how to bring about fundamental change in the organizational construct.

Cultural Redux

The last piece I would like to reiterate—and then I will open the discussion to Q and A—is about culture, and how we manage our way through the cultural challenges and the dynamics of change.

We can attend these forums, and discuss these issues from the perspectives of being in the seats to being up here in front; and when we say we have got to change, we look around the room and see all the heads moving up and down. But when you really examine the issue, what you find out is that this change thing is great as long as it doesn't affect you.

How we manage the culture is a lot more about personal dynamics and human demographics and how we work together than it is about assessment of the technology. We are in a bit of a bind right now; and it took us—I go back to my green eyeshade past in the Department of Defense—it took us at least 15 years to go from the Planning, Programming, and Budgeting System

(PPBS) to Planning, Programming, Budgeting, and Execution (PPBE). It has simply revolutionized what we do.

We are stuck in fielding legacy equipment that is “legacy” before it ever hits IOC, and everybody calls it such. That kind of agility is just not going to service well. We must find the interface between the information age and the acquisition practices of the industrial age; and we must transition from the governance of the industrial age. How we do that is critical to whether or not we stay a competitor; and we are not very good at that yet.

Let’s consider some command and control acronyms. How do you outsmart your enemy? How do you stay inside their decision cycles? Well, you can build systems like the AFATDS [Advanced Field Artillery Tactical Data System] or the TBMCS [Theater Battle Management Core System]—each letter’s about a billion dollars; each letter’s at least a year just to change a line of code. What are our adversaries using?—Google, Yahoo, MSN—very agile, updated at least weekly, monthly—clearly effective. So from an acquisition standpoint, if you compare a command and control system built on an information-age model—with systems built on an industrial-acquisition construct that is significantly different culturally—the TBMCS, AFATDS—the standard packages that we have for command and control—who has the advantage?

“We have got to figure out a way to keep what is valuable in the existing culture and discard what is getting in the way.”

Assume that the adversaries know who we are, assume that they can tell us what we need to know—because we certainly cannot figure it out on our own. God forbid that when we step across the line of departure, they change things—because our response cannot change; we are locked into our response based on our information. Meanwhile, as the adversary is maneuvering on our flank, he has got perfect information.

How are we going to change that? I do not know what is going to happen when I step across the line of departure. I do

not know what the adversary is going to do. But I do know that the adversary is going to outmaneuver me if I don't change. He is going to be there to surprise me and he is going to work in my seams; and I am going to try to do the same to him—and that fight is going to be very dynamic. If my tools and my weapons are not equally dynamic, I lose.

If you sit on the firing line of a network attack activity, a slash is a whole new class of weapon. The warfight changes with a single slash. How are we doing to change the mindset and the culture to start to understand and be able to work in that environment?

Committees do not do well in milliseconds. A basic way of doing business today is: locate a problem, identify it, discuss it, come to some set of courses of action, brief that to at least four levels or echelons of bosses, issue a directive to gather the forces necessary, and then issue the authority to prosecute. The war is over before you have even started.

We are going to have to figure out how to operate in that environment, and it is going to stress the culture more than it is going to stress anything else.

Collaboration

I would like to leave you with a final thought on the issue of trying to move the culture of a large organization. It is an interesting, dynamic task. We at STRATCOM did this initially with collaboration: It is transformational—it just rolls off your tongue, and everybody uses it, and it justifies money, and you can say, “Oh, I collaborated on that. I'm in a distributed organization and I collaborated.” Okay, got it.

Rather than develop a multibillion dollar software package, we just took a cheap off-the-shelf commercial product and started to work collaboration processes. How do we define collaboration? If you ask someone my age what collaboration is, they will say it's the number of people that I called on the phone to discuss the issue. If you ask my daughter, it's how many chat rooms that she can run simultaneously. If you ask my grandson, who is three years old, he would say “It's the A key, grandpa. That's the one I

push to get automatic VTC with you at night to say good night." Collaboration means many different things to different people, so you have to consider the attributes of the different tools.

Chat rooms are very fast, they exchange information quickly between disparate groups, and you can make connections that give you huge leverage, but you all have to agree to be there simultaneously. The same with the phone. We started to acknowledge the fact that although it is convenient for me to conference at 2 o'clock in the afternoon, my forces in Diego Garcia or in Okinawa do not necessarily like to do daily routine activities at 2 o'clock in the morning. So we moved towards blocks because you do not have to all be there at the same time and you can follow the sun, so to speak, in your activities. Relatively simple. Unfortunately, it does not play well culturally in a military organization.

"We just do not need another 9/11 to compel us to start to compete in this environment. We cannot wait for that anymore. The proliferation of knowledge and access have allowed individual actors to have the throw-weight and the authority and the intellectual capital of nation states."

God forbid that I talk to Lance Corporal Cartwright as a four-star without at least 15 layers of command in between clearing whatever Cartwright said. That is the culture, and we had to find a way to work through the culture and command structure. After we started using the new collaboration channels, during the first six months, that is exactly what happened: An event would be posted with a blog space where you could talk about the event and experts could comment on it, so you could get input from all directions, to help you decide what you wanted to do.

All of that was good, but the inputs were very slow coming in. Why? Because the chain of command had become the chain of information, so everything had to be staffed before being said. Well, it didn't do much for our speed of execution.

So I had to threaten them with the fear of death, and things started to happen a little bit quicker. However, we found in the second six-month period—and it did tend to rotate on six-month periods—that we had a situation called “the tethered goat.” That is, Lance Corporal Cartwright would post the entry, but it had been staffed and given to him by the Colonel: “Okay, say this and use my name or use your name.”

“God forbid that when we step across the line of departure, they change things—because our response cannot change; we are locked into our response based on our information. Meanwhile, as the adversary is maneuvering on our flank, he has got perfect information.”

So, again, I had to use the fear of death: “You either stop that or I fire you,” which generally gets their attention. We started to move to collaboration. Collaboration in this flat environment really puts stress on middle management. Middle management owns the process. Their comfort zone and their power resides in their control over process. If you start one of these experiments—whether you are in business or you are in the government—you will come to that realization very quickly.

This little collaboration tool is marvelous; it has got incredible accountability, so you can tell what is happening anywhere in your organization—so you can check out Lance Corporal Cartwright in Shop X by typing his name into the tool and seeing everything that he has done/contributed to. Often, the list is long; sometimes the list is short. You put in Colonel Cartwright’s name and there is usually nothing there. Why not, you ask? “I’m managing people.” What is that doing for my bottom line? What are you really doing for my organization?

It puts a lot of stress—whether you are that overt about it or you are hopefully more subtle about it—it puts a hell of a lot of stress on middle management. Because they are the ones who will slow the decision down in order to enter into the process—and process gives them security. How you take that on in a large

organization—how you take that on in any large endeavor—is really at the heart of how you are going to move forward in this or not. It is a big challenge.

By nature, we do not generally like to change very much. If the world changes, we like to make sure it changes those around us—not us. We just do not need another 9/11 to compel us to start to compete in this environment. We cannot wait for that anymore. The proliferation of knowledge and access have allowed individual actors to have the throw-weight and the authority and the intellectual capital of nation states. That means they do not have to answer to voters, they do not have to answer to a congress, and they can have an incredible effect on you and me.

If we do not find a way to address that problem, we will be in dire straights. I'll leave it at that. The end statement here is that, if we are not willing to flatten out and get to these kind of decision speeds and execution capabilities and integrated agile organizations, then we will be the flattened—and that's just not where we want to end up. Okay? Appreciate it.

As I said, I am happy to let the Q and A go in any direction. I tried to bring up enough issues to irritate the majority of the audience here, so we can go in any direction you want to go.

Q & A SESSION WITH GENERAL CARTWRIGHT

Q: *Sir, could you talk a little bit about the Africa Command with an integrated State Department duty structure?*

Gen. James Cartwright—The question is about Africa Command and where we are headed in integrating State Department and DoD activities. What ideas are being proposed, how could the new command possibly follow a different model? One of the key things that STRATCOM has been trying to understand is the way DoD carves up the world versus the way State carves up the world. The boundaries are not the same. Is that good or bad? Some people think that's good; some people think it adds unnecessary challenge and keeps us from speaking with one voice.

If you have a regional combatant commander for an area and a group of ambassadors for that same area, how do you bring a coherent message, how do you work preconflict-type activities in that environment? We have had some dialogue about Africa Command—whether it will add value to integrate activities between State and DoD from the beginning, or whether it would unnecessarily impinge on checks and balances in the government. How do you approach this problem? My fear is that it will be like the Army and the Marines going north to Baghdad. Although we may have a common name, we might section ourselves off within the organization in a way that will not be value-additive.

The good aspect of this could be that if we integrate, we might find that the people in the State Department really do not all have just one eye in the middle of their forehead, and they do speak English, and we could actually find synergies where we could both add to the equation. The question is: how do you incentivize collaborative behavior?

Immediately, integrating goes against the process owners, so you will have to shift and balance power within the organization. You have to resolve internal conflicts such as who is in charge, when are they in charge, what issues State works on, what issues DoD works on—all of those things. The hope is that you can get them in the room together, close the door, and throw pizza under the door until they all start to behave—and that you will get something out of this that might add value in a way that we have not thought about. The opportunity in Africa is huge. If you can start to shape activities—absent conflict, preconflict—in a way that is coherent, you have a lot of potential there to move in a positive direction. It's an experiment.

It is going to take some senior leadership commitment to make everyone willing to accept new processes and modify existing processes in the name of devising better ways to conduct diplomatic and military activities. They will have to prove that they are more than just a demonstration to be accepted, and they will have to be able to interface in some way with all of the standard processes that will not change in the rest of the theaters.

So I think it has a huge challenge, but if senior leadership is absolutely committed to it—which is the only way that I think it's going to have any chance of succeeding—then it may well yield great rewards. I am hearing the conversations; I just have not seen the commitment yet to really move forcefully in that direction.

Q: *Can you elaborate on the topic of distributed attributes?*

Gen. James Cartwright – I think there are two dynamics to this discussion. There is value in a distributed organization that can move assets to a problem quickly on a global basis and have the appropriate scale associated with each problem; then there is the regional commander who can bring the context and the agility to match the right resource to the exact problem. How do you find the balance between the two? The unfortunate element that tends to muck up all of this is ownership. That is what people focus on: “What do I own? My worth is based on how many planes or sensors or whatever I own rather than what is happening.”

I have established a precept at STRATCOM that we adhere to before we approach any mission area: I do not really want to own any resources at STRATCOM. For example, I do not want to own the ISR platforms. What we bring to the table are efforts to understand globally what is out there, what is the problem set, what is the likelihood of matching a sensor to the problem and having some level of success, what is the probability of engagement success. Given that there are competing environments, multiple problems, and not enough sensors to cover every problem, how do you mix and match in a way that gives you the scale that you need to solve a particular problem? Not owning the assets unburdens STRATCOM significantly. Therefore, we stay mostly on the assessment and analysis and global force management side of the equation; we focus on applying these to the problems at the appropriate scale.

What we tend to find when we do this—and we do a lot of assessment activity—is that the ownership issue always surfaces. Here is one example that just drives me crazy that comes out of every single assessment we have done in every theater: A

combatant commander asks you for a Rivet Joint. He does not tell you why he wants it. He just wants the Rivet Joint, and he wants it for a period of time—not for an effect, but for a period of time—“I want it for six months.”

If you do not give him the Rivet Joint, he does not ask for something else. So, was it the target that he was trying to prosecute or was it the ownership of the asset? I have never had a combatant commander come back and ask for an alternative when we did not give them what they wanted. It bothers me. So, how do you change that? You ask (or tell) the commanders two things:

1. “Tell me what the desired effect is, and then let me offer you a range of solutions—because you are competing with other combatant commanders for the same assets. Let me offer you a range of solutions and a probability of engagement success associated with those, then you can pick and choose or argue or advocate for what you think your priority ought to be.”
2. “Define the problem we are trying to solve, and when we solve that problem, time’s up. You do not need to own the asset—I need to move it and move it quickly to the next problem.”

That is where we have to change the focus. It is less about ownership; but ownership is the prevailing culture. That is really at the heart of the problem. When physical ownership is a priority because it is a way that we gain stature and standing power, it can become self-limiting because you are more focused on the ownership and the management power of that activity than you are on the probability of engagement success and trying to understand what an asset is going to contribute rather than on owning the asset. Ownership is as prime a human attribute as they come, so trying to behave differently is a huge challenge.

Let me give you another example of the assessment role, and a tool we are using. We call them kill webs. Essentially, they are all of the different sets of command and control, sensors, and effects

or weapons that would be available to you as a commander. How do you string them together in different combinations to understand the probability of engagement success, match them up, and then solve more with a limited number of assets than you would have by just parsing them out one at a time. The system is not structured that way yet, but that is where we are trying to move it. We think these kill webs—on the output side—allow you to articulate to someone: “Here is the likelihood that this will solve your problem.”

When we look at the input side of this activity, we ask, “Where do I always hit a throughput node that causes me problems?” That is where I am going to start to advocate for additional new capability or more of what I already have. It gives you a way of looking at the problem that—analytically and from an assessment standpoint—allows you to articulate very quickly what the input equation ought to look like and what the output equation should yield.

That is the way we approach a problem, whether it is ISR or Strike or Net Warfare. We develop kill webs that allow us to understand the input side and the output side so that we can move quickly.

The problem is that at the end of it, the organization still tends to be more focused on ownership than it does on the product. That is the culture that we have got to try to break somehow. From my perspective, I do not want to own the assets and centralize ISR. STRATCOM is focused on what are the connections of opportunity, which ones take how long and what is the likelihood of engagement success. When I look at the enterprise, I am asking, “Where will I get the greatest leverage at my next acquisition?”

Q: *Do you have a problem in matching your goals to the culture of the Congress?*

Gen. James Cartwright – Oh, very much so. The problem is not in their acceptance of the methods—it lies in the committee structure, it is in the lack of agility, to move adaptively. Congress deals in one-year increments—that is a heck of a lot better than having to justify everything for five years at a time. When people

always point at the Congress as being the roadblock, my response is you ought to carry a mirror every time you accuse somebody of being a problem; because you are probably a major part of that problem. Because of the committee structure, they have had a heck of a time determining which committee STRATCOM should advise. The problem with the committee structure is trying to understand where the lines were between these disparate missions. A major part of my activity is shuttling between the intelligence committees, the standing committees, the armed services activities, energy, and water, all of which have oversight of the various mission areas. How do we reach consensus? How do we move something forward? If one committee goes left on you and the other one goes right—trying to square that is very difficult.

Congress is very aware of this challenge, and to their credit, they are working very hard to align across the committee structure. This year they have moved in a way to allow me to focus my consideration in three committee areas, down from nine last year. They have moved in a constructive, accommodating direction. They understand the opportunity and they're trying to reinforce the behavior and keep programs aligned so, for example, you actually have a delivery platform for a weapon or the other way around. They have moved much more aggressively than probably even the DoD has on trying to help with alignment issues.

Q: You talked quite eloquently about the value of speed in terms of added capability. Part of the fitting together that you talked about is making good decisions within an extreme timescale. In the past six years, what opportunities have we had to further develop that capability?

 **Gen. James Cartwright** – Opportunity is a double-edged sword. One of the things that we have worked very hard in missile defense and in prompt global strike is how do you—in the span of an hour or in the case of missile defense, in a six-minute decision timeline—how do you move to decision speeds in that timeline that are more than just the decision of yes or no weapons release or not? How do you actually get senior leadership to understand the gravity of the issue in those timelines and be able to add value?

It goes back to the collaboration discussions. I cannot guarantee you that the decision will be good, but let me give you a sense of what happens today versus where we would like to be. Today we would convene a conference on the phone and say, "Problem X—I am trying to get some place in an hour; I am trying to make a decision in four or five minutes." We spend the entire time in discovery, briefing somebody with PowerPoint or voice about what is happening—instead of spending that time asking if I do this what is the nuance, what are the second- and third-order effects, what assessment has been done that would give me a model to understand what I'm about to enter into? You cannot do that by voice—not in those timelines.

“. . . if we integrate, we might find that the people in the State Department really do not all have just one eye in the middle of their forehead, and they do speak English, and we could actually find synergies where we could both add to the equation.”

We are trying to move national command capabilities to provide tools that give you the situation awareness either with a picture—whatever makes an individual cognizant of what is going on—and to do discovery very, very quickly and spend the rest of the time understanding the implications and talking about that, rather than listening to somebody brief you about what is happening. That is a huge change in the way we do business.

Essentially, it means that the processes are running based on a rule-set and people are intervening by exception. When they intervene, it is giving them the time to think about alternative courses of action, second- and third-order effect-type activities instead of weapons release. It enables them to ask, "Am I in part of the envelope, am I not in part of the envelope. How many seconds have I got left to make a decision?"

Technically, it is relatively easy, but it is hard culturally to get decision-makers to work in that way, and it is hard to get forces to—in the missile defense example—it is hard to get all those

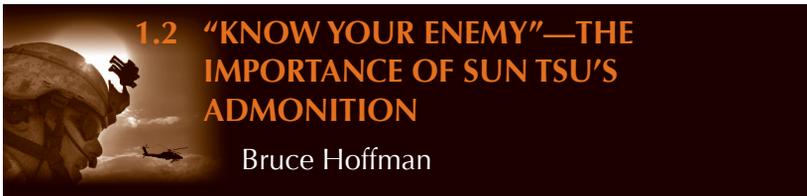
layers across nine time zones to not want to manage every sensor interaction, which would give you a stackup of time that would make the shot irrelevant, or the defense irrelevant—and instead have someone sitting there saying, “It looks good, I see no reason to intervene, and letting it pass through.”

The issue is not whether or not we can cause the effect and actually deliver something globally—we should focus on what are the implications of being able to do that and what are the regret factors of not being able to do that. Do I balance those and what are my other choices? We need to be able to think about it beforehand rather in the heat of conflict.

That is really the debate on prompt global strike. I think you want to have an alternative in prompt global strike to a nuclear only option. However, once you have this capability, what are the implications? Am I going to enter into conflict or incite or escalate in that activity unintentionally? How can I portray this capability and take me in the direction I want to go, which is to deescalate?

How do you start to understand? Because technology can give you some wonderful tools, but at the end of the day it still boils down to: what is the perception of your adversary, how are you trying to change that perception, and which direction do you want to change it in—and what is the likelihood you are going to be successful at doing that? These are huge, huge debates that ought to occur.

So, to the credit of the Congress and the Department and the Administration, in my mind—many of these debates are starting to be public, which I think is a good thing— including the nuclear debates. I think it is critical to start to get these things up on the table and let people talk about them. Without being able to do that, you are really challenged.



If there has been one consistent theme in both America’s war on terrorism and our melancholy involvement in Iraq it is a serial failure to fulfill the timeless admonition to “know your enemy.”

The war on terrorism has now lasted longer than World War II and our entanglement in Iraq for nearly as long. That we are still equally far from winning cries out for precisely the knowledge that we have instead neglected. “If you know the enemy and know yourself,” Sun Tsu famously advised centuries ago, “you need to fear the results of a hundred battles.” Yet, what remains missing five and half years into this struggle is a thorough, systematic, and empirical understanding of our enemy: encompassing motivation as well as mindset, decision-making processes, as well as command and control relationships; and ideological appeal as well as organizational dynamics.

Why is it so important to “know our enemy?” ... Simply, without knowing our enemy we cannot successfully penetrate their cells; we cannot knowledgeably sow discord and dissension in their ranks and thus weaken them from within; nor can we think like them in anticipation of how they may act in a variety of situations, aided by different resources; and, we cannot fulfill the most basic

Professor Bruce Hoffman is a tenured professor in the Security Studies Program at Georgetown University’s Edmund A. Walsh School of Foreign Service and former Corporate Chair of Counterterrorism and Counterinsurgency at the RAND Corporation. He also served at the Office of National Security Affairs, Coalition Professional Authority, Baghdad, Iraq, during the spring of 2004. He is the author of Inside Terrorism (Columbia University Press), May 2006.

requirements of either an effective counterterrorist strategy—preempting and preventing terrorist operations and deterring their attacks—or of an effective counterinsurgency strategy—gaining the support of the population and through the dismantling of the insurgent infrastructure. Until we recognize the importance of this vital prerequisite, America will remain perennially on the defensive: inherently reactive rather than proactive—deprived of the capacity to recognize, much less anticipate, important changes in our enemy’s modus operandi, recruitment, and targeting.

Forty-five years ago, the United States understood the importance of building this foundation to effectively counter an enigmatic, unseen enemy motivated by a powerful ideology who also used terrorism and insurgency to advance his cause and rally popular support. Although America encountered many frustrations during the Vietnam conflict, a lack of understanding of our adversary was not among them. Indeed, as early as 1965, the Pentagon had begun a program to analyze Vietcong morale and motivation based on detailed interviews conducted among thousands of guerrilla detainees. These voluminously detailed studies provided a road map of the ideological and psychological mindset of that enemy: clearly illuminating the critical need to win what was then often termed the “other war”—the ideological struggle for the hearts and minds of the Vietnamese people. Even if the fundamental changes required in U.S. military strategy to overcome the Vietcong’s appeal went ignored, tremendous effort and resources were devoted to understanding the enemy.

“Until we recognize the importance of this vital prerequisite, America will remain perennially on the defensive: inherently reactive rather than proactive—deprived of the capacity to recognize, much less anticipate, important changes in our enemy’s modus operandi, recruitment, and targeting.”

Today, Washington has no such program in the War on Terror in Iraq. Both America’s counterterrorism and counterinsurgency strategies appear predominately weighted towards a “kill or

capture" approach, targeting individual bad guys. This line of attack reflects a fundamentally conventional military's preoccupation with the "enemy centric" warfare it has long been accustomed to, trained for, and ineluctably prefers to fight rather than the "population centric" approach that is at the heart of countering terrorism as well as insurgency. It is also erroneously based on the assumption that America's contemporary enemies, be they al Qaeda or the insurgents in Iraq, have a traditional center of gravity, thus believing that these enemies simply need to be killed or imprisoned so that global terrorism and the Iraqi insurgency will both end.

1.3 THE ACHILLES' HEEL OF ANALYSTS

Michael Bauman

INTRODUCTION

TRADOC [U.S. Army Training and Doctrine Command] is working on three or four dozen studies and analyses at any one time, from tactical distributions systems and new trucks to convoy protection. We are finishing a study on the Joint Light Tactical Vehicle and making another annual run on Future Combat Systems. We just completed a Precision Munitions Mix Analysis, which won a Wilbur Payne Award, and the Unmanned Aerial System Mix Analysis. The most pressing analysis underway right now concerns the Army's Tactical Ground Network.

Our diverse body of work over the years has taught us that concepts are typically ambiguous, the data bases are miserable to work with, and the models are inadequate to the task. Furthermore, because of the compressed schedule of the work, we have to build methods and models in stride with the analysis and try to analyze data on the fly. It is a very tough business, and

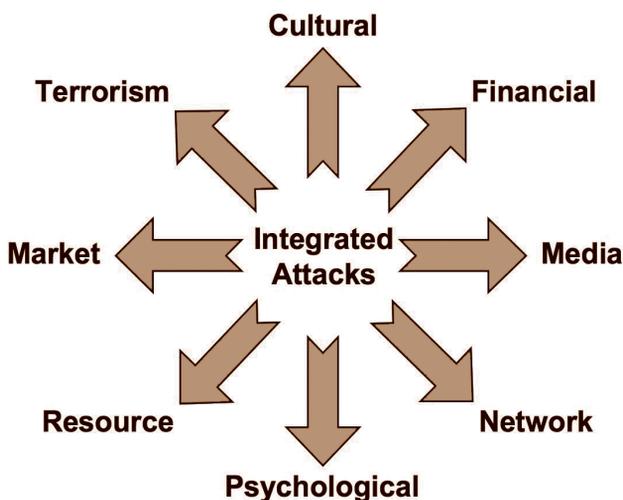
Mr. Bauman leads the analysis mission of the U.S. Army Training and Doctrine Command (TRADOC) and serves as the Director of the TRADOC Analysis Center (TRAC). Under his leadership, TRAC has been prized with thirty-six major DoD and Army awards for excellence in analysis. During the past two decades, his agency's analysis has enabled nearly every major Army force transformation and weapons acquisition. He received a Bachelor of Science in Aeronautical Engineering as a Beech Scholar and a Master's in Industrial Engineering (Operations Research) from Texas A&M University. Mr. Bauman has been recognized three times with the SES Presidential Rank Award and received the Army's Wilbur B. Payne Award for leading the Future Combat Systems Analysis of Alternatives.

it offers valuable insights to how we must analytically approach unrestricted warfare in the future.

A DIVERSE ENEMY

The CIA translation of *Unrestricted Warfare* by the two Chinese PLA colonels, Qiao and Wang, clearly reveals how unrestricted warfare is different from conventional warfare (Figure 1). The premise of their writing is that the militarily inferior can win against the militarily superior.

Unrestricted warfare attacks will be integrated and target the domains represented in the figure. That view has profound implications: the authors do not see a nation like China necessarily competing with us as peers or superiors militarily, and they do not believe they have to.



Col. Qiao Liang & Col. Wang Xiangsui, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, February 1999. English translation, Pan American Publishing Co., 2002.

Figure 1 Unrestricted Warfare

Soldiers are not the only ones that wage war—there are counterfeiters, hackers, black marketeers, and free trade violators. All these actors compose “the army” that is waging all aspects of unrestricted warfare. In fact, attacks are going on right now within

many of the domains represented in the figure. Are they coherent and integrated? Probably not. But various state and non-state actors are repeatedly probing in these domains. As Dr. Luman noted, there is only one rule in unrestricted warfare: there are no rules. However, the absence of rules doesn't mean we cannot perceive and analyze patterns in the behavior of those who are conducting these attacks.

IMPLICATIONS FOR ANALYSTS

The 2006 URW Symposium was excellent in its scholarly attention and exploration of what URW suggests for the community of modelers, analysts, and data gatherers. In his talk, entitled "Tailored Deterrence: New Challenges for the Analytical Agenda," Charles Lutes mentioned six key features of URW:

1. Nonlinear
2. Expanded time domain
3. Inherent dynamism within the system
4. Informational, cognitive, behavioral aspects
5. Immense diversity of targets and tactics
6. Contextually rational behavior of enemies (vice shared values and norms)

He concluded that the methods that an analyst uses to evaluate warfare are insufficient to evaluate unrestricted warfare.

One particularly interesting point is the contextually rational behavior of the enemy. In other words, we may not understand them to be rational; but within their own context, they are. If we do not understand that, we cannot treat the enemy properly in our body of work. Lutes also said that we need a renaissance of thinking and a new generation of luminaries. He talked about three steps for analyzing this kind of enemy: elucidate, estimate, and then evaluate as we move into this environment. Finally, he called for a shift in perspective that leads to new ways of connecting data and interpreting exhibited behavior.

The theme of this paper is data—interpreting, collecting, and connecting the data and interpreting and predicting the behaviors that we see in this new environment. At last year’s symposium, Blackett’s Circus was twice cited as an early example of the kind of operations research that URW demands. Blackett was the British astrophysicist during World War II, who led a multidisciplinary team in determining where to base the radar-guided guns for coastal defenses. Blackett’s success showed that, to understand an environment, we need to analyze the data to examine possible influences, explore relationships, and eventually mathematize them. In other words, if we are going to address URW, we have to understand what we are working with. We must observe, gather data, theorize, develop hypotheses, and test them against the data. Someone characterized this as “data intensive casework,” which is particularly apt. To paraphrase a paper from the 2006 URW Symposium, we have to manifest the value of information in our force-level work.

“ . . . to understand an environment, we need to analyze the data to examine possible influences, explore relationships, and eventually mathematize them.”

At TRAC, we have been able to model the layers of the network in excruciating detail at the force level, especially for brigade operations. We can generate and track discrete messages all the way through the system to the points where decisions are made using the information represented by these messages, and those decisions have traceable impacts on tactical and operational outcomes. It represents an Army modeling and analysis enterprise that few, if any, organizations have been able to duplicate. It requires very meticulous, very detailed work and very precise performance-level renderings of networks. But those networks are a manifestation of the physical world of warfare, and the outcomes are almost exclusively kinetic; they do not yet adequately account for the cognitive and behavioral aspects of military operations.

What has been done to date with new network concepts is enormously exhausting in terms of the intellectual work, the tedious business processes, and the complex modeling that have to be built-out and continually updated as the network changes. This set of challenges is but a glimpse of those facing analysts of URW.

COMPLEX ADAPTIVE SYSTEMS

Table 1 is a list of some of the features of complex adaptive systems, which apply to unrestricted warfare. These systems are difficult to work with and require a lot of data to achieve acceptable accuracy and predictability. I do not know of any cases in the Army where we have applied complex adaptive systems successfully. Complex adaptive systems have not yet been proven for the kind of problems we are facing—for example, where do we define the boundaries? If we keep trying to identify all the interrelationships, the cost keeps growing, and soon—to quote a familiar adage—we find ourselves trying to define the universe and present three examples.

Table 1 Complex Adaptive Systems

- Many interacting elements.
- Causality is complex and networked.
- Number of plausible options is vast.
- “Intelligent” context-appropriate behavior.
- System behavior is coherent (exhibits recurring patterns) but not fixed (the rules keep changing).
- Diverse, flexible responses towards any given end.
- Agility (rapidly change tact to be more effective).
- The system learns from experience.
- Predictability is reduced.

Holland, “Hidden Order: How Adaptation Builds Complexity,” 1995.
Grisogono, DSTO, Australia, 2006 C2 Research & Technology Symposium.

How do we define the problem and find the data needed to analyze it? The system behavior is coherent. The system can exhibit recurring patterns, but the rules keep changing. If there are enough data, a pattern can be discerned and analyzed even if it is shifting. The system is going to react to outside stimuli and try to find a way to always be successful despite barriers. It is going to learn, it is going to adapt, and it is going to keep changing. To use such a system in the work that we are doing, we have to have robust data and a very robust feedback loop built into the complex adaptive system that we are modeling so that we can keep up with the adaptations in the URW environment.

We are not adapting fast enough, but our adversaries are. The models that we build today are very difficult to change and very difficult to adapt. We need to search out new ways to represent this environment of unrestricted warfare. As Holland noted in *Hidden Order: How Adaptation Builds Complexity*, “an initially poor predictor will improve over time as feedback is used to refine the models . . . ” In other words, our URW model cannot be static. We have to design a model that will dynamically adapt as we tap the data base and understand what it is telling us. As we weigh how to analytically tackle the dimensions of URW, the use of complex adaptive systems deserves much more attention.

GROWTH IN DATA: AN OPPORTUNITY

Figure 2 shows the amount of digital data in billions of gigabytes that is expected to be generated worldwide by 2010. Leveraging this volume of data to our advantage is an enormous opportunity and, in my view, warrants a DARPA-type approach. There is already an enormous wealth of data freely available and readily accessible in many forms from a variety of sources. As a topical example, law enforcement agencies have begun monitoring YouTube for clues to crimes; and that is just one example of many. What are we doing to tap into these enormous data bases and use them to our advantage to ward off potential attacks on our nation?

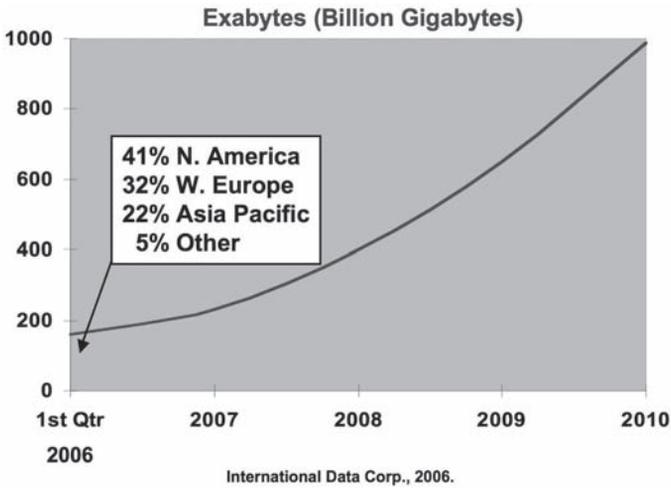


Figure 2 Digital Data Generated Worldwide: 2006–2010

BGI—Barclay’s Global Investors—is a classic data quantifying organization and an outstanding example of how to manage and exploit data successfully. It is America’s largest group of money managers, with \$1.6 trillion under management. Its original claim to fame was that it invented the index fund. Its goal is to systematically beat the market by harvesting the alphas—the gains above market return. In the past 5 years, it has generated \$20 billion in alpha. It is successful for several reasons:

- It employs over 100 PhD statisticians, who are credentialed in financial engineering, physics, applied math, and operations research.
- At any given moment, it is working on 50–60 new alpha theories, comprising scores of new statistical factors.
- Theories are tested against terabytes of historical data that are continuously updated.
- Techniques are derived from fuzzy logic, neural networks, Markov chains, and nonlinear probability models.
- It executes thousands of trades per day on more than 12,000 stocks and debt issues, based on continuous number crunching.

What is more important, creating wealth for your customers or defending the nation? Obviously, the litmus test for being a successful data manager and miner is creating “wealth” for your clients. Here is an example where the equities market has maintained, developed, managed, and made available in a matter of milliseconds enormous amounts of data to a wide variety of money managers so that they can create wealth for their customers.

We have nothing comparable in DoD. Yet, in the financial sector, there is a treasure of very valuable data accessible to everyone. These sector companies hire the best and brightest from the leading institutions and pay them very handsomely, but many of these financial specialists seek out those companies because they are at the cutting edge of research in their fields.

Barclay's is incredibly successful, in large part, because of its mining of data bases. Its leading experts posit theories about where they might be able to harvest alphas. They look for trends in the marketplace that offer potential gains above the market. Then, they vet and debate their hypotheses with their colleagues and test their theories based on historical evidence by tapping into BGI's terabytes of data. In other words, they seek compelling hypotheses and subject them to hard data. As a recent issue of *Business Week* reported about Barclay's, “*If a thing cannot be measured and factored into a hypothesis for testing against historical data, Barclay's has no use for it. They have essentially purged human fallibility from the system.*”

BGI is an excellent study of how a profit-motivated organization has prospered by tapping into a very rich data base even when those same data are available to its competitors. The last paragraph out of the article from *Business Week* makes a great analogy—it calls BGI:

. . . the Wall Street equivalent of one of those giant factory fish trawlers that have revolutionized commercial fishing. This superquant methodically cruises global markets, sucking alpha from the depths while everyone else drifts about in rowboats, corks bobbing pathetically atop waters that are nearly fished out.

That is a wonderful summary of what Barclay's is doing with data mining. There is only about \$30 billion of alpha out there for all of us, and Barclay's is reaping about \$5 billion of it—the direct result of an extraordinary data mining enterprise.

OIF DATA BASES

Now let's turn to our military's most ambitious operations data base, one that is relevant to URW, albeit in a far less grander scope and scale—the data being collected in-theater for Operation Iraqi Freedom (OIF). This evolving data enterprise is not nearly the scope or scale of BGI's, which should be of great concern to us given the hardships it already faces.

The OIF data are collected in a data base called the Combined Information Data Network Exchange or CIDNE. This data base collects three types of data: operational data; polling data, which have a kinetic focus; and assessments by subject matter experts (SMEs). The data are in raw form and are input by numerous parties, including the Coalition Forces (CF) and the Iraqi Security Forces (ISF). Those data are not integrated within CIDNE; they're entered separately and remain separate or non-relational. Little or no political, social, economic, or infrastructure data reside within CIDNE; and there is no strong data czar in total control, although Multinational Forces Iraq (MNFI) issued a memo recently that put a knowledge management (KM) officer in charge of the data base, albeit with limited real authority.

Each of the 150 or so fields in CIDNE is assigned to various offices in a lead or support role. To add new data fields to CIDNE, the Corps Commander sends out a fragmentary order (FRAGO) to input new data. However, when he did that recently, some summarily ignored it, for a variety of good reasons owing to the regimen of real operations.

What eventually make these data valuable are downstream data bases that are created by "cleansing" the CF and ISF data. For example, every Friday, a team from the Center for Army Analysis (CAA) updates the data from the two previous weeks. By noon on Saturday, any authorized person can tap into the network

and conduct analysis. The system is getting better thanks to the Herculean efforts of a few individuals, but it is still far from what we need to effectively wage war in a URW environment. Our OIF data base experience tests our patience and exposes weaknesses in how we collect, manage, and mine data in a complex environment resembling aspects of URW. Also, the data are largely kinetically focused. What about all of the other dimensions of unrestricted warfare? How do we get all those data in the data base? Who is going to be in charge? How do we manage security and classification issues when data with multiple classification levels are all in one data base? Who should have access so that the quants of our military can test their theories and make them available in defense of our nation?

“CIDNE collects three types of data: operational data; polling data, which have a kinetic focus; and assessments by subject matter experts . . . Little or no political, social, economic, or infrastructure data reside in CIDNE; and there is no strong data czar in total control.”

Another issue is trust among different government agencies. At present in Iraq, DoD cannot access the State Department network to download or upload data. The only way DoD can enter data in the State Department network is to key them in. This present day lack of coordination and connectivity offers a glimpse of future challenges in fully leveraging a comprehensive data base spanning multiple agencies and domains for purposes of analyzing URW.

SOLUTION: LEADERSHIP, INVESTMENT, DATA ENTERPRISE

Three resources are critical to solving this problem:

- Enlightened, take-action senior leaders.
- Money, lots of it.
- An unprecedented data enterprise.

It has been very difficult to convince senior leaders in the Army to invest in models, simulations, and data bases of emerging network-centric concepts. That experience is a harbinger of what to expect for URW. We need enlightened, take-action senior leaders who will understand the need for a whole new business enterprise associated with modeling and analysis.

In 1991, Paul Davis and Don Blumenthal of RAND wrote a paper, entitled “Base of Sand,” which criticized military models as woefully inadequate to represent the emerging concepts of that time. Davis followed up in 2001 with “Effects-Based Operations: A Grand Challenge for the Analyst,” which made the same point: the then-current methods of modeling and analysis were inadequate for effects-based operations, and new theories and methods and a new empirical base should be vigorously pursued. Today, we are hearing the same criticisms that we heard 15 years ago. Will we hear the same thing years from now when we are in the midst of unrestricted warfare?

Our leaders must be willing to provide sufficient funding for a new modeling and analysis enterprise. Otherwise, we have to scramble to keep up with the changing environment. It is unlikely that corporate DoD is going to make the kind of investments that are needed without enterprise-wide agreement. In 5 years, there will inevitably be some new criticism of modeling and analysis. Although there will also be some improvements, we will not be totally prepared to deal with what might arise in the future.

“It has been very difficult to convince senior leaders in the Army to invest in models, simulations and data bases of emerging network-centric concepts—a harbinger of what we face for unrestricted warfare.”

It is our responsibility to educate senior leaders about the importance of addressing these challenges. Whatever modest success we have had in representing the new networked concepts and operations has happened because we convinced a few key senior leaders that they need to invest in this area. Further progress

is going to take financial commitment. If we're serious about confronting unrestricted warfare with modeling and analysis to determine what capabilities to invest in, how to analyze operations in real time, predict what our adversaries are learning and will do next, adapting our strategies and tactics ahead of our enemies, then we need significant funding and talent—perhaps seeded by DARPA.

Finally, that commitment of resources and effort must result in an unprecedented data enterprise that will turn the DoD modeling and analysis community into the Barclay's of defense.

CONCLUSIONS

Huge quantities of diverse data are going to be readily accessible in the future that will cross over all the domains of unrestricted warfare. The sobering question is this: will we be the ones that most effectively exploit those data and do it first to our advantage, or will that prize belong to our adversaries?

Q & A SESSION WITH MR. BAUMAN

Q: *You mentioned the challenge of encountering thousands of exabytes of data on the Internet. The challenge versus, say, Barclay's is that there's no standard metric for what you're searching for. How do you decide what you want first?*

Mr. Michael Bauman – I agree with you. What is the strategy? What goals are our senior leaders establishing for how we conduct operations? What is a campaign in unrestricted warfare? What goals have we set so that we can establish those metrics? The goal at Barclay's is to make lots of money, but supporting that goal is a lot of subordinate metrics, like cash flow and pre-inventory levels, which sound very arcane to us.

What are our objectives here? What is our strategy? What are our goals: Containment? Deterrence? Defeat through attrition? Hearts and minds? Control of the information operations campaign? Our senior leaders have to provide that kind of direction at a national level.

I would like to follow upon what was said earlier. One of our problems with Information Operations (IO) at the strategic level is that different groups are all working independently on pieces of the same problem, and they don't coordinate well. But it's much more than that. The IO campaign has to go from the strategic level down to the tactical level. The relationships among activities at all levels have to be understood to wage an effective IO campaign. How do we build the processes and understand the patterns so that we can effectively do that?

Let me mention something that's going on in-theater right now. III Corps approached us and asked us to help them determine if they were collecting the right data and had the right measures to gauge whether they were achieving their campaign objectives. Over the course of many years, they had developed a lot of objectives, a lot of metrics, and a lot of data attributes that they were collecting. But nobody was checking to see if the measures actually told them if their actions were having the desired effect. There has to be feedback in the system that indicates whether or not a specific action will lead to the desired outcome. We're helping III Corps in-theater to understand which of those metrics are relevant to what they've established as desired effects.

What we haven't done is collect the data that are most relevant and then conduct statistical tests to establish how strongly those measures are correlated with desired outcomes. The units are rolling through the theater and back out; and every time one leaves, there are more measures left behind requiring more data to be collected. But the correlation is missing. We have to have that feedback in a system like this because we don't understand what's at work. It's not kinetic. It's very unusual for us as military analysts to deal in this environment. So we've got to first understand it. And you must have data to do that.

Q: You talked about various resources needed for this program. One of the things that I don't see is training of new, potential leaders. They're going to have to get smarter to do this stuff, particularly in the time involved.

 Mr. Michael Bauman – Do you mean military leaders?

Q: *The whole group of people who is responsible for decision-making in wartime.*

Mr. Michael Bauman – It's gratifying that General David H. Petraeus and General William S. Wallace are both leading a new generation of officers and Soldiers. Their influence is reflected in the Army's new manual on counterinsurgency, published by TRAC's parent command TRADOC. It addresses the behavioral aspects of the environment we're working in today, often referred to as the human dimension. In fact, some papers have been published within the last couple of weeks on the human dimension; and conferences are planned. A few years ago, General Wallace hosted a conference that assembled social scientists and anthropologists with warfighters to explore the kind of environment we're operating in today. On the military side, at least through the senior leader development programs that exist in the Army, we're educating a new generation of military leaders.

I can't speak to what's going on in the civilian sector. In DoD, many come from industry. Some kind of program is going to be needed to bring them onboard intellectually. There's a lot of ignorance about this problem even in my own organization as well as throughout DoD. It's going to take education and training to remedy.

At least in the Army, we're seeing a lot of traction in educating leaders. I think there will be a future generation of Army leaders that understands it much better.

Q: *What do you do about data overload?*

Mr. Michael Bauman – Do you mean in the sense of an analyst being data overloaded?

Q: *Yes.*

Mr. Michael Bauman – That's a real problem. But again, I believe we're going to have to turn to software to help us with that. Still, at the end of the day, somebody has to sit down and

look at what that software is telling us and figure out if it makes sense in explaining why things are the way they are.

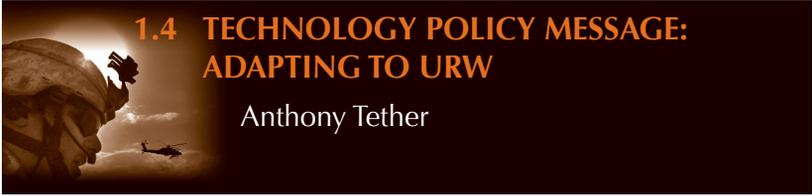
Barclay's challenge is that it still takes a human being, someone knowledgeable, to decide whether or not the product of the data mining, software tools, and the mathematization of the data makes sense. If it doesn't pass the so-what test, it's worthless. A marriage of software with human intelligence and skills can help with that problem.

However, if you're talking about overloading Commanders with data, that's a whole other problem that needs to be treated with much more sophisticated man-machine interfaces. I have joked that we ought to have Windows for Warfighters, enabling commanders to carry around their own portable, customized version of battle command software, tailored like Microsoft Office enables, to access data in the way that's most comfortable to them, adapting it as they grow throughout their professional careers.

Q: *Do you give the Commanders a one-paragraph executive summary?*

Mr. Michael Bauman – You're asking a question about the whole analysis business enterprise. I don't think it's possible to do that for the complex problems that TRAC most often analyzes. Our shortest executive summaries are typically several pages long. I haven't produced a one-paragraph executive summary in a long time.

I wouldn't take any executive summary to a senior leader if I didn't know what he'd ask in the first place and if I didn't have an answer to his question. My organization is not in the business of expanding the body of scientific knowledge, nor are we in the business of trying to defend the so-what of anything. TRAC is in the business of answering hard questions about complex problems posed by senior leaders. We try to do the analysis right and deliver the answer based on the evidence we have. The Commander wants to be confident you did the analysis right, and that takes more than one paragraph.



1.4 TECHNOLOGY POLICY MESSAGE: ADAPTING TO URW

Anthony Tether

INTRODUCTION

The following is a transcript of a speech given by the DARPA Director, Dr. Anthony Tether, at the 2007 URW Symposium. The transcript has only been lightly edited and should be read with that understanding.

DARPA is actually a very small organization, roughly 240 people comprising about 140 or 150 technical people. Only about 2% of our budget is used for agency operations; the remaining 98% goes to industry and universities. That means that we count on all of you for ideas.

What makes DARPA different than any other place in the world is that, by design, the program managers have been there for only a very short time—four to six years. They come from industry, universities, and government. If they are in the government, they

Dr. Anthony Tether founded and was CEO and President of the Sequoia Group, which provided program management and strategy development services to government and industry. From 1994 to 1996, he was CEO for Dynamics Technology, Inc. From 1992 to 1994, he was Vice President of Science Applications International Corporation's (SAIC's) Advanced Technology Sector and then Vice President and General Manager for Range Systems at SAIC. Before that, he was Vice President for Technology and Advanced Development at Ford Aerospace Corporation. Dr. Tether has served on Army and Defense Science Boards and the Office of National Drug Control Policy Research Committee. He received his Bachelor of Electrical Engineering from Rensselaer Polytechnic Institute. He earned his Masters and Ph.D. in Electrical Engineering from Stanford University.

have to give up their career status and become term employees. There are no careers at DARPA. We hire people for their ideas. They give up a lot; come to a place where they know they will not have a career; and sometimes, with the new ethics laws, are not sure they can get a job when they leave. But they all have one thing in common—they have an idea that they could not work on where they were. DARPA gives them that opportunity.

We have one organizing principle: if you put people with like interests together, after a while, they will start to like and trust one another. When that happens, you get a nonlinear effect in the generation of ideas. That is really what DARPA is about. If you want to know what is going on at DARPA, do not look at the titles of the offices; look at the topics under them. We try to create these offices with topics that are multidisciplinary. Even though the technical people might cluster around their own disciplines, they cannot help but meet people in associated disciplines.

THE DARPA MISSION: BRIDGING THE GAP

Where does DARPA fit in? The science and technology programs for the Armed Services tend to be near- to mid-term programs. This is great science and technology but it typically deals with known systems and concepts—making radars more sensitive, jet engines more efficient, and so forth. That should not be a surprise—people tend to put today’s problems at the top of a list rather than future problems. So when the funding line is drawn, what usually survives is on the near to mid end.

But there are folks on the far end who will say, “We can move atoms around. Tell me what you want, and I will create the material for it.” For them to be funded, they have to be like an electron and tunnel their way across this gap. President Eisenhower created DARPA nearly 50 years ago for one purpose: to bridge that gap (Figure 1).

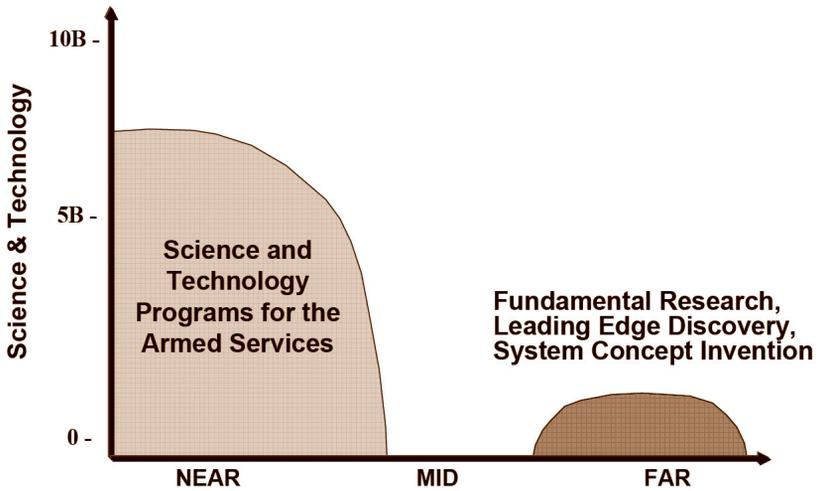


Figure 1 DARPA's Role in Science and Technology

When the Russians beat us into space, it was an embarrassment for this country, especially because it was the geophysical year, when we were supposed to go to space. When President Eisenhower asked how that happened, he found that it just wasn't high enough priority. But there were plenty of people out here on the far end who said, "If you wanted to go to space, we could have done it. But you had to give us the money." So DARPA was specifically created to never let that happen again and was chartered to mine the far side, find those ideas and concepts that could be taken from the far side to the near side, and then pass them on for development.

50 YEARS OF ACCOMPLISHMENTS

What have we done in 50 years? Figure 2 shows some of the programs that DARPA brought from the far side to practical development. They range from Saturn to Global Hawk and Predator. What will DARPA do in the future? I am going to highlight just a few of the ones that are most relevant to this symposium's theme of unrestricted warfare.



Figure 2 DARPA Accomplishments

SUPPORTING THE WARFIGHTER

The next few figures describe some of the DARPA programs that are supporting our warfighters in Iraq today.

DEFENSIVE SYSTEMS

The Bar Armor Counter RPG System (Figure 3) prevents an RPG [rocket-propelled grenade] from forming its jet when it pierces a vehicle. It is not 100% effective, but it does it well enough that the enemy in Iraq no longer fires RPGs at strikers with the bar armor.

Boomerang is a system that detects hostile fire. When DARPA developed it in the 90s, the Army said that there wasn't a requirement to know that they are being shot at while on the move. In 2002, General Alexander called me and said, "I've got guys coming back, their vehicles are all shot up, and they don't even know they're being shot at. Can you help?" And we did. BBN resurrected Boomerang and produced the units, and they are now deployed in Iraq. They are inexpensive—on the order of

\$8,000 to \$10,000 each. The word is out among our adversaries: “Don’t shoot at the vehicles that have that thing on them because they’ll shoot back.”

Future Icons

- Networks – Self-forming, Robust, Self-defending
- Sensors to detect and precisely identify elusive targets
- Real-time language translation to replace linguists (Defense Language Institute, III – IV)
- Air Vehicles – Fast Access, long loiter for military operations
- Space capabilities to enable global military operations

Core Technologies

- High-productivity computing system – peta scale computer
- Prosthetics to enable return to units without loss of capability
- Quantum Information Science for new computational capabilities
- Low-cost titanium to enable routine use (3.5/lb military grade alloy)
- High Energy Liquid Laser Area Defense System as a penetration aid to replace stealth

Figure 3 DARPA Programs Supporting the Warfighter

RAPID-REACTION SUPPORT NETWORKS

We are in a revolution today. Back in the old days, our targets were not moving. We could take our time disabling them, but our enemies quickly learned that a fixed target was a dead target against the United States. They learned how to become mobile

and to fractionate themselves into small groups. We can no longer tolerate the time gap between finding the target and taking care of it. To prevail in the battles of the future, we have to be able to respond quickly. That is one of the reasons for Predator and Hellfire.

What do we have to do to defeat the enemies of the future? Everything will have to be integrated (Figure 4). Assets used to find targets will be used to destroy targets. The battles of the future will probably not be force on force. Tanks are still important, but they are going to be used differently. In the battle scene of the future, the network integrating everything becomes the weapon of the future and has to be reliable and dependable. It has to be self-forming as the forces flow in because the network now is as important as the platforms, maybe even more so.

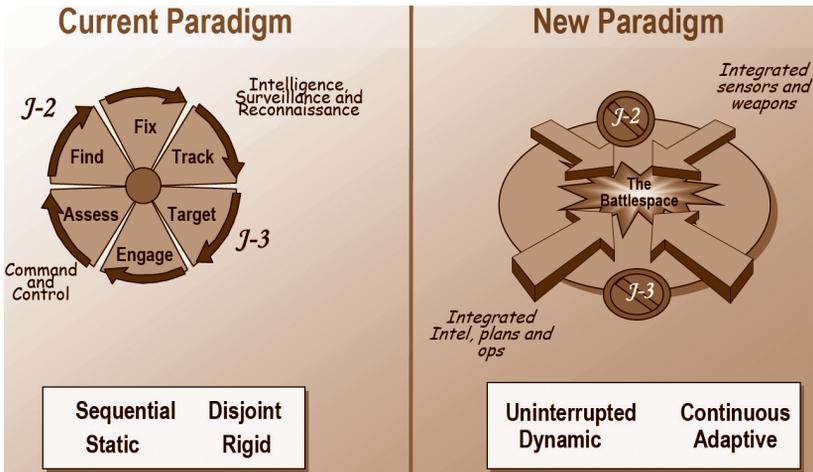


Figure 4 Network-Enabled Shift

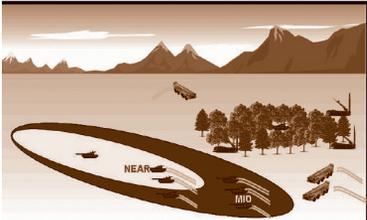
NETWORK-CENTRIC STRUCTURE

At DARPA, we have broken the problem down into two parts with a gap between them (Figure 5). First, there is the network-centric enterprise, the strategic level, the back echelons. These are the people with high clearances and typically great fiber bandwidth. They do all the planning.

Network Centric Enterprise
***Strategic and operational
 level of deployment and
 warfare***



Bridge the Gap



Network Centric Warfare
***Tactical level of
 deployment and warfare***

Figure 5 Military Operations Network-Centric Structure

Down at the tactical level, all connections are wireless. Here, the network cannot rely on infrastructure because the infrastructure is too easily disabled. The infrastructure has to be part of the flow into the system. The people at this level do not have clearances; some are coalition partners. It is a nasty environment, with a lower bandwidth. These people have to be connected so that they can exchange information that is not readily available, know what is going on, and resupply any lax areas. That is part of how to bridge the gap between these two organizations.

As nodes come and go at the tactical level, the network has to recognize and accommodate it—take the node out, put the node back in, etc. And it all has to happen automatically. That is a tall order; but several years ago, DARPA proved it could be done. We built prototype radios and showed that dismounted warfighters could not only be connected, they could know where one another was. The Army took the prototype over and developed it into the compact Soldier Radio Waveform.

NETWORKING FOR SITUATIONAL AWARENESS

We went even further. We created a program to interconnect all the platforms (Figure 6). If a platform went out of line of sight, we developed techniques for holding the information going to it until it was back on the net.

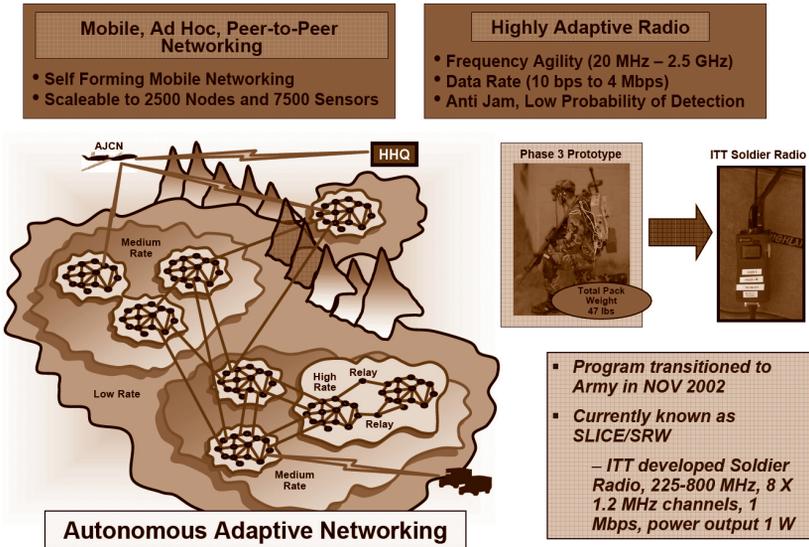


Figure 6 Small-Unit Operations Situational Awareness System

Everyone wanted that common radio. But it was very expensive, and we had a lot of legacy radios. Further, we did not really know how people were going to use a common radio because we had not been able to give them a network-centric capability.

We asked ourselves if we could network those legacy radios to the point of true network-centric warfare, which is what we needed to be able to respond to the current and future enemy.

SELF-FORMING NETWORKS

The result was the Future Combat Systems-Communications (FCS-C) gateway architecture, which could seamlessly connect each of the radio systems, whether on a vehicle, airborne, or carried by an individual Soldier (Figure 7). If people in the First

Battalion using the PRC-119 wanted to talk to a Company, the gateway would automatically change the protocol. A similar gateway is what allows a user with a Global System for Mobile Communications (GSM) cell phone to talk to someone with a Code Division Multiple Access (CDMA) cell phone. The difference is that the FCS-C does not need towers or infrastructure.

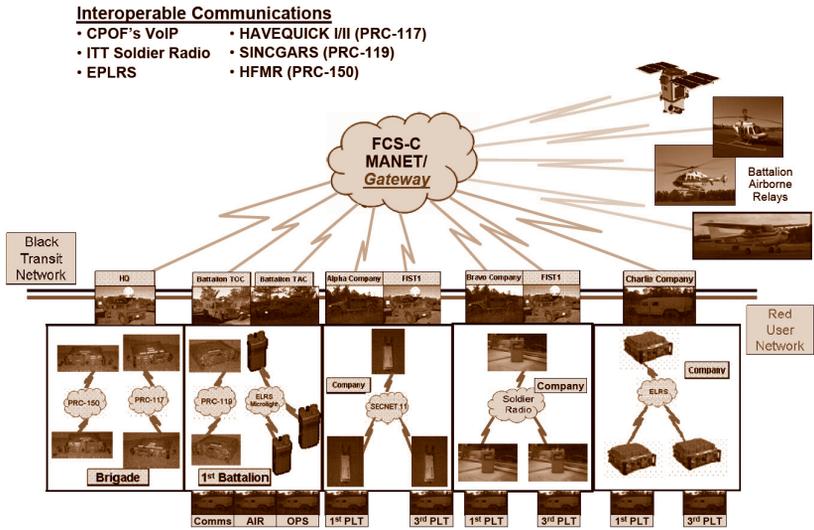
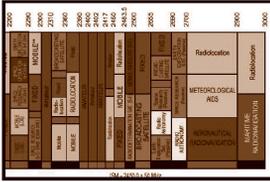


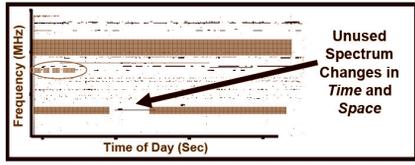
Figure 7 FCS-C Network Centricity Demonstration

We overcame the problem of finding the local radio spectrum by having the radios themselves find the spectrum and create the network based on the spectrum at the time. Even though the spectrum was 100% allocated, we found that only 5% to 10% was actually being used at any instant in time. The result was the neXt Generation (XG) communications technology, which was demonstrated last summer (Figure 8). When the radios come in to form the network, they listen to the spectrum, find the part that is not being used, and go to that part. Everybody on the network tunes to that part. If there is interference, the network recognizes it and goes to another part of the spectrum. We also showed that the network can stay ahead of a jamming system that constantly goes to the part of the spectrum in use.

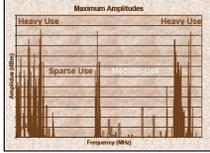
TODAY: Spectrum statically allocated



OBJECTIVE: Dynamically allocating spectrum in frequency, space, and time

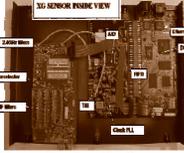


Collected RF Environment: FY02



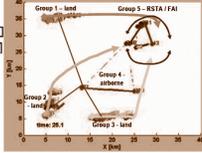
Spectrum Occupancy

First Version of Sensor: FY04



Spectrum Sensing

3 Designs Validated: FY04



Operational Modeling

6-Node Network Field Demo: MAR-JUN 2006



Potential 10X better utilization of spectrum

Figure 8 neXt Generation (XG) Communications

CHIP-SCALE ATOMIC CLOCK

The problem is that we need the spectrum to network the weapon, and the enemy knows it. It is going to try to take the network down with the same kinds of commercial networks it is using now for situational awareness, calling down fire, etc. One of the easy ways to disable a self-forming network is to jam its GPS [Global Positioning System] so that it cannot get a time signal. One of our program managers proposed putting a low-power chip-scale atomic clock in every radio that would provide precise time for several days (Figure 9). Our goal now is to reduce the size of that chip package to 1 cubic centimeter. We are well on our way to enabling a soldier to continue to talk with a Single-Channel Ground and Airborne Radio System (SINCGARS) for several days without a GPS.

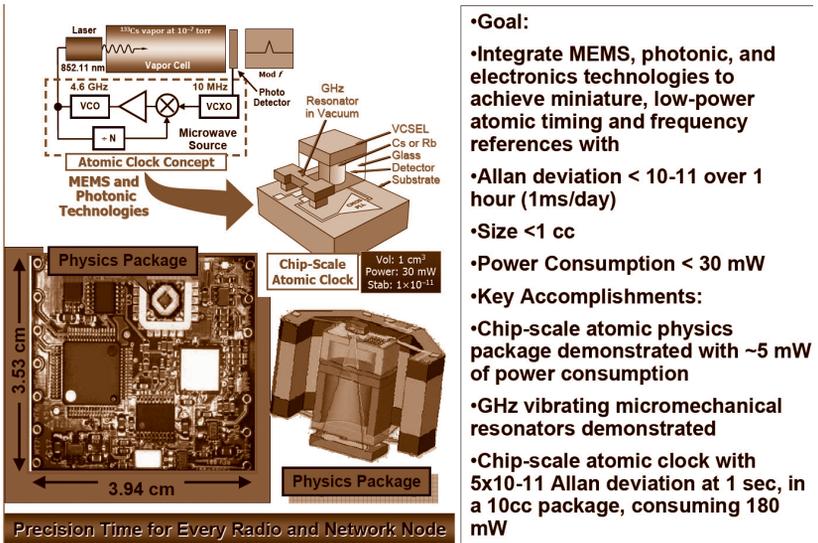


Figure 9 Chip-Scale Atomic Clock

ORCLE

Another system we are developing is the Optical and Radio Frequency Combined Link Experiment (ORCLE) (Figure 10). ORCLE combines a high-data-rate laser and a colocated radio frequency (RF) link. The idea here is that, no matter where you are around the world, sooner or later, you will find a fiberhead. If one airplane is connected to a fiberhead and the rest to ground units, you can communicate around the world over that fiber. When the Transformation Communications Satellite (TSAT) is deployed, ORCLE is designed to connect to that fiber for a virtual fiber linkup in the sky. The RF link helps the lasers link up and self-form the network and also ensures conductivity if clouds are obscuring the laser beams. The result will be a system that always allows low-bandwidth, high-priority messages to get through.

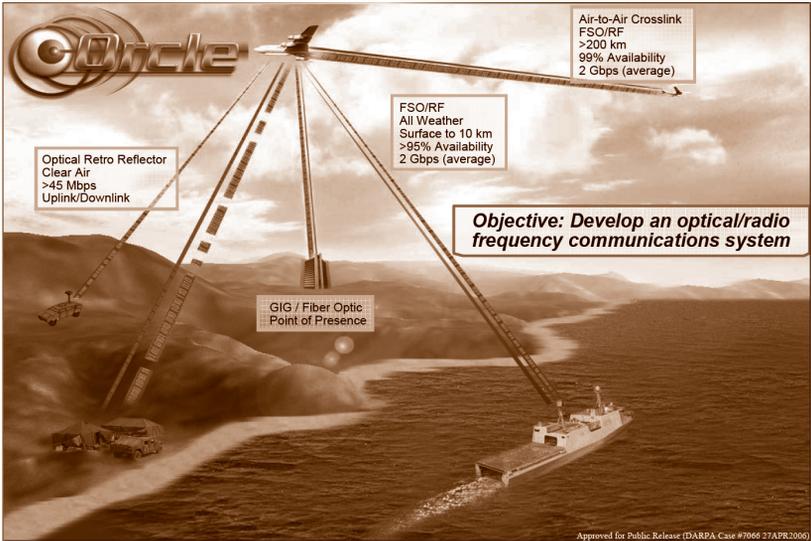


Figure 10 Optical and RF Combined Link Experiment (ORCLE)

OPTICAL MEMORY

DARPA is also building the next-generation core optical network, an all-optical Internet that will self-form and immediately repair itself if the fiber breaks (Figure 11). The network will allow people in the military anywhere to transfer large quantities of data and imagery through the ORCLE network. One problem we had to overcome was how to store optical communications in an all-optical router if they could not be sent immediately. So, we developed optical memories. We can slow light down enough so that it can remain where it is locally while the router figures the next route.

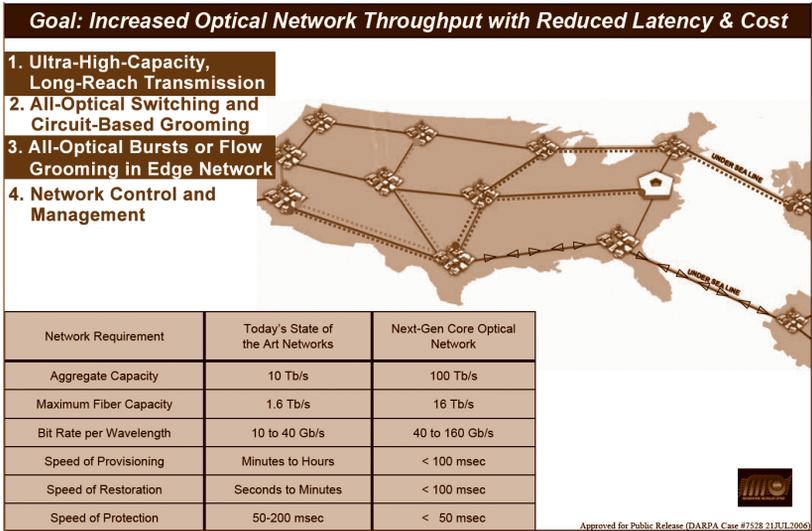


Figure 11 Next-Generation Core Optical Networks

That technology is what we are going to need to adapt to unrestricted warfare. We need one person with situational awareness to be able to communicate that situational awareness to anyone and call for fire without needing the tank along side.

TARGET DETECTION AND IDENTIFICATION

We are also working on target detection and identification. The objective of one program, called Foliage Penetration Reconnaissance, Surveillance, Tracking, and Engagement Radar (FORESTER), is to find people under foliage (Figure 12). Very High Frequency/Ultra High Frequency (VHF/UHF) radars can find vehicles; but we want to find dismounted troops out of their vehicles, which is very difficult in a forested area. FORESTER, mounted on an A160 autonomous Predator-class helicopter, can detect people walking among trees. The aircraft has a range of a couple of thousand miles and can stay up for a day. To identify a possible target, we are developing a synthetic-aperture laser radar or ladar that will let us take a photograph of that target from an airplane and unleash a weapon on it (Figure 13).

Detect dismounted troops under foliage



Program Objectives

- Wide-area surveillance capability
 - > 600 km² coverage area
 - 20 - 30 km standoff range
- Affordable (< \$1.9M) sensor cost
- Rapid technology insertion

Concept: Develop a persistent surveillance capability that can detect and track targets moving slowly through dense foliage



Dist. C - Subject to limitations on title page

Figure 12 FORESTER

Objective: Demonstrate the first long-range, high-resolution 3-D Synthetic Aperture Ladar

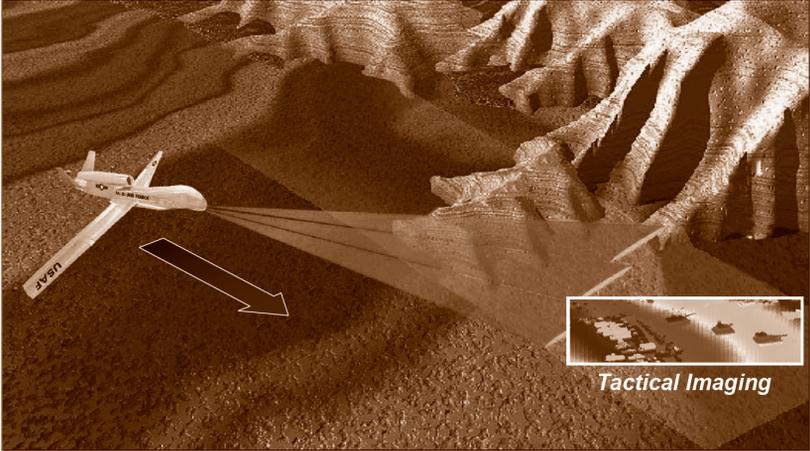


Figure 13 Synthetic-Aperture Ladar for Tactical Imaging (SALTl)

LANGUAGE TRANSLATION

Unrestricted warfare means that we may be fighting battles all over the world. That means we will need to know what is going on all over the world—we will need to talk to people; we will need to understand what the radio, TV, and the newspapers are saying. We are developing technology that translates foreign language broadcasts with a 5-minute delay. We are actually using it in Iraq today instead of linguists for translating TV stations like Al Jazeera. It is not perfect, but it is good enough to give someone the gist of a story so that they can decide if they want to have the rest translated (Figure 14). Our intent is to develop this capability to the point where the warfighter no longer needs a linguist to translate. We are aiming for 90% accuracy, which is roughly equivalent to a Defense Language Institute (DLI) level four linguist. We believe that we will be able to go directly from speech to a translated text by 2009 or 2010.

• Program Goal

- Fully automated and highly accurate language translation
- Current foreign language focus:
 - Arabic
 - Chinese

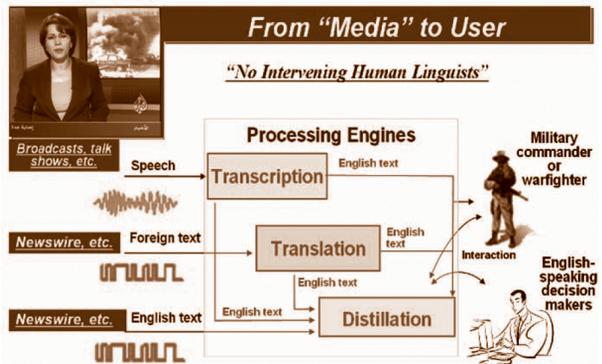


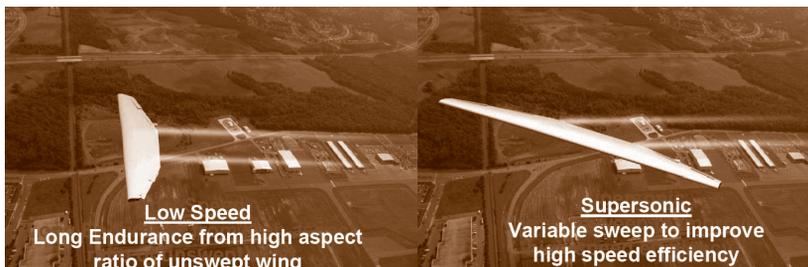
Figure 14 Language Translation

AIR VEHICLES

We are working on a lot of ideas for air vehicles. The Wasp has revolutionized the situational awareness process for the Marines in Fallujah and Ramadi. It looks like a bird so the enemy usually ignores it.

OBLIQUE FLYING WING

Another program is developing the OFW (Oblique Flying Wing) (Figure 15). Like an airplane, it takes off normally with the wings perpendicular to the direction of flight. It cannot go very fast in that configuration but is very efficient. When it needs to go fast, it can turn the wings—as if the engine were on a lazy susan—and go supersonic. If it penetrates any defenses, it can turn itself back into the efficient configuration and loiter for a long time.



Supersonic, tail-less, variable sweep

DARPA Program:

- Define, develop, and mature key oblique flying wing technologies
- Conduct preliminary design of X-Plane demonstrator in Phase I
- Design, build and fly OFW X-Plane in Phase II

Figure 15 Oblique Flying Wing

AUTONOMOUS REFUELING

We have developed an F-18 Unmanned Aerial Vehicle (UAV) surrogate that refuels autonomously. It will attach itself to a tanker hands off. This capability is a total paradigm shift because the UAV does not wear itself out from landings and takeoffs. Because

the limiting factor on endurance is oil, we will have to learn to pass oil as well as fuel. Autonomous refueling will change the way we operate—we will be able to deploy Global Hawk-like aircraft that will stay up for months and years. The tanker itself could be autonomous—an autonomous tanker could fuel an autonomous aircraft. Our whole fleet could stand constant watch over an area, each of them with a Hellfire or two ready to go.

ORBITAL EXPRESS

We are also working on space programs. Last week, we launched the Orbital Express, which is an on-orbit servicing system with autonomous refueling capabilities in space (Figure 16). A satellite will hook up with it, mate to it, and receive fluids from it. It will also be able to reach out an arm and change out electronics. It is now going through checkout.

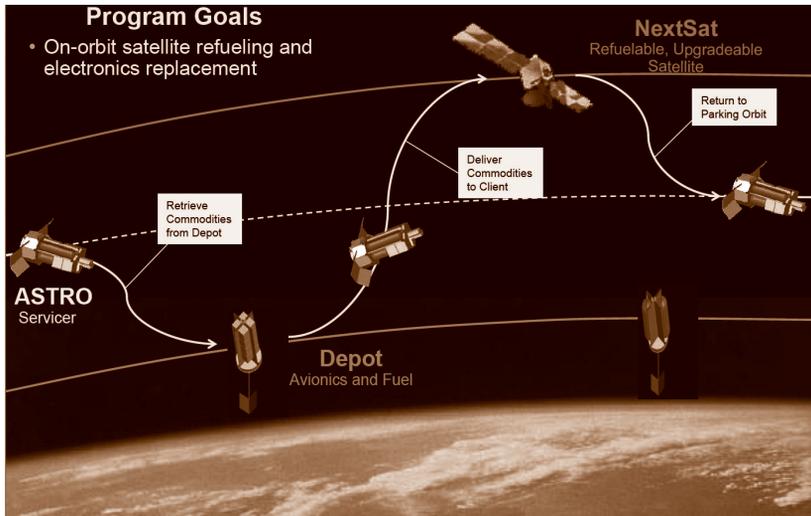


Figure 16 Orbital Express: On-Orbit Servicing System

HIGH-PRODUCTIVITY COMPUTER

Unrestricted warfare means we are going to have to respond quickly to threats. We have to do a lot of building and testing today because our computers are not fast enough to be able to do it virtually. We are on the verge of building a high-productivity

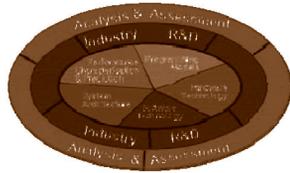
pedaflop computer that performs 1015 instructions per second (Figure 17) or 1 billion MIPS. This is a high-productivity system, not a high-performance system. The reason is that we placed two constraints on the contractor: the machine had to operate in the pedaflop range, and it had to be easily programmable. To meet the terms of the contract, the contractor has to prove that the machine operates as a pedaflop and can be programmed 25 to 100 times faster than a MIPS machine. It will be operational by 2010 and will give us a big advantage in terms of unrestricted warfare.

Develop a new generation of **economically viable** high-productivity computing systems for the national security and industrial user community

• **High-Productivity Computing is Critical to National Security**

Impact:

- **Performance** (time-to-solution): speedup critical national security applications by a factor of **10X to 40X**
- **Programmability** (idea-to-first-solution): reduce cost and time of developing application solutions
- **Portability** (transparency): insulate research and operational application software from system
- **Robustness** (reliability): apply all known techniques to **protect against outside attacks**, hardware faults, & programming errors



HPCS Program Focus Areas



Fill the Critical DoD Need for:
 Intelligence/surveillance/reconnaissance, cryptanalysis, weapons design and analysis, airborne contaminant modeling and biotechnology

Figure 17 High-Productivity Computing System

PROSTHETICS

We have an exciting program in prosthetics (Figure 18). It started with a monkey at Duke University. We put microelectronic implants into her brain, taught her to bring two balls together with a joystick to get a treat, and then used the signals from her brain to manipulate a mechanical arm. The signals from her brain went to the Internet and then to MIT where the arm was located. When she moved her arm to operate the joystick, the mechanical arm at MIT would move just like it. Then, we took the joystick away. She knew she had to bring those two balls together to get the treat.

She moved her arm as if she were still operating the joystick, and the arm at MIT also moved. We thought we had captured the motor signal, but we had actually tapped into her thought. After a while, she learned that she did not have to move her arm to move the balls. She just had to think it, and her brain pulled the balls together.

Then we did something fantastic. We connected an artificial arm to her brain with wires. When she was offered a piece of food, she used thought to make the arm reach out, take the food with its fingers, and bring it to her mouth. We think we can build an artificial arm with all the degrees of freedom and articulation of a real arm. The arm itself is an engineering marvel, but the revolutionary part is that it will be controlled by the wearer's brain. We will run fiber optics through the nerve in the feedback path that brings the impulses back to the brain so the brain knows where that arm is. And this is all happening here at Johns Hopkins. Dean Kamen is also working on an arm, but Johns Hopkins is giving it neural control. We have cases now where people have actually regained feeling. Imagine what else can be done with this capability.

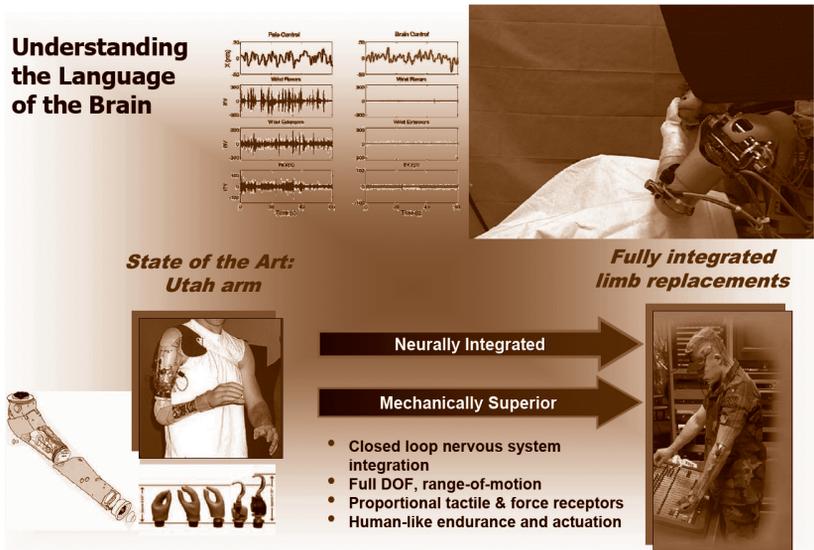
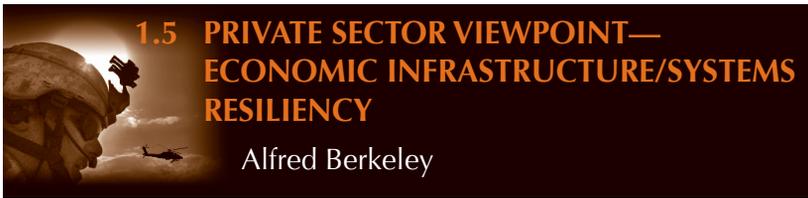


Figure 18 Revolutionizing Prosthetics

CONCLUSIONS

DARPA is always interested in innovative ideas and people with good ideas. Get to know our program managers—they are the ones who really run the place.



The National Infrastructure Advisory Council (NIAC) was created by Executive Order in the wake of the September 11 terrorist attacks. The NIAC provides the President with recommendations on policy changes to improve America's critical infrastructure security. Since its inception, the Council has developed a homeland security policy that helps define how the Federal government and private sector can collaborate to protect the public good. The Council strongly promotes the view that the private sector must play an integral role in developing these policies. To date, the NIAC has completed 13 reports, all of which address the following topics:

- Clarification of roles and responsibilities between public and private sectors
- Risk assessment and management
- Information sharing
- Protective strategies

INTRODUCTION

We've been talking today about defining, adapting to, and combating URW with analysis, strategy, and technology. I'm going

Mr. Alfred Berkeley is chairman and CEO of Pipeline Trading Systems. He has over 25 years of experience as a former president and vice chairman of the NASDAQ Stock Market, Inc. He earned an MBA from the Wharton School of Finance of the University of Pennsylvania and a BA from the University of Virginia. He has been an officer in the United States Air Force and is a trustee of The Johns Hopkins University.

to discuss the same issues but from the perspective of the business community. I specifically want to discuss the lessons that the business community has learned from 9/11 and the work that I've been doing since October of 2001 with the National Infrastructure Advisory Council. I am speaking as an individual citizen and am not representing the views of the National Infrastructure Advisory Council.

THE NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

The NIAC was created to bring a business perspective to many of the issues associated with URW. I was asked to participate because the NASDAQ was the target of daily, sophisticated hacking attacks, particularly from central Europe and Asia. We had developed a very close working relationship with the FBI; the National Security Agency; the Pentagon; the White House; and the New York Stock Exchange, whose websites and operations were also being hacked.

Executive Orders 13286 and 13231 led to the establishment of the NIAC shortly after 9/11, specifically to address cyber security. The scope was subsequently expanded to include other infrastructures such as water systems, railroads, and finance. Since then, it has expanded considerably to include 17 industrial sectors. With the creation of the Department of Homeland Security (DHS), administrative support for the NIAC shifted from the National Security Council to DHS.

The Council consists of no more than 30 people who represent many diverse sectors of the economy. The NIAC makes policy recommendations to the President to improve America's critical infrastructure security. The NIAC is more than an advisory council because it addresses process and does substantive work.

Current and former members include Chairman Erle Nye from TXU and former Vice Chairman John Chambers from Cisco. Others include: Craig Barrett from Intel; Margaret Grayson, a cyber expert; Ray Kelly, the Commissioner of Police in New York; Martha Marsh, head of Stanford University's Hospital;

Tom Noonan, General Manager of IBM's Internet Security Group; Bruce Rohde, Chairman and CEO emeritus of ConAgra Foods; Dr. Linwood Rose, President of James Madison University; and John Thompson from Symantec, which produces security software for PCs. Past members have included Don Carty, CEO emeritus of American Airlines, who brought an aviation perspective; Archie Dunham, Chairman of Conoco Phillips; Chuck Holliday, CEO emeritus of Dupont; and Marty McGuinn, who ran Mellon Financial, a very large commercial banking operation. Marilyn Ware, Chairwoman of American Water Works, highlighted an important infrastructure issue: water is particularly vulnerable, we all need water, and many water systems can't detect what's in them. Another former member was Tom Weidemeyer, Chief Operating Officer of United Parcel Service, which has the most feet on the street of any business. United Parcel Service provides a particularly interesting view into the economy because it carries packages that could potentially hold dangerous items and it has people everywhere every day.

THE BUSINESS COMMUNITY PERSPECTIVE

The NIAC has met with the President about four times in six years; each meeting lasting long enough to engage him in discussions and find out what he thought was relevant and interesting.

The business community view on URW that I've gleaned from 5 or 6 years on the Council may counterpoint some of what you've heard today and reinforce other expressed views.

So our first project was to spend about 6 or 7 months getting a firm grounding in the existing laws and understanding what information the government needed—how much, what was relevant—and how that information might be used. When we investigated, we found that business was so nervous about FOIA—the Freedom of Information Act—the Plaintiff's Bar, competitors, shareholder suits, etc., that no company wanted to come forward with any information about weaknesses in its operations.

Partially on our recommendation, Congress passed a law exempting from FOIA information provided to the federal government expressly for the purpose of infrastructure protection.

We thought we had solved that problem; but a year and a half later, only a few companies had come forward with any information. So we went back out into the field and found out that businesses were still reluctant because the law had never been tried in court and wasn't guaranteed to be bulletproof.

"... we found that business was so nervous about FOIA—the Freedom of Information Act—the Plaintiff's Bar, competitors, shareholder suits, etc., that no company wanted to come forward with any information about weaknesses in its operations."

In the course of those discussions, we'd hear comments like, "Well, I'll tell you my problems, but it cannot go to my regulator because the only thing a regulator's going to do is come back and say, fix it." Some of these problems were so expensive to fix, they raised the question of whether we were building resilience or a fortress. There are many of these cases where it seems to make sense to report a situation—this little problem with the water supply, or this little problem with the railroad, or this little problem with a bridge—but then you find yourself saddled with an immediate requirement to spend more than your net worth to fix it—clearly, a non-starter.

We stumbled upon a lot of these tradeoffs during that very first project. We still do not have a case in the courts testing the law, and we do not have anyone coming forward with information that could be sensibly used by sensible people in the government with a sympathetic view to this balancing act. If the view toward these tradeoffs isn't sympathetic, if there is no effort to determine what amount is reasonable to spend—not to protect ourselves from every contingency but from risk-based contingencies—no information will be forthcoming. These are matters of trust, in

the grey areas of the law. Figuring out the right balance between information and secrecy and what information goes where in the government and who gets to use it is not easy.

RISK-BASED ASSESSMENT

Our second theme running through many of our activities was to answer the question: how much should the U.S. spend on infrastructure protection? In theory, you can never spend enough. We had an enlightening comment from one of our members about the interest in Des Moines, Iowa, in protecting its skyscraper. It's unlikely that Osama bin Laden really cares about that skyscraper in Des Moines, Iowa; and yet it's the center of the universe for the people who live there. You heard Secretary Chertoff talk about allocating federal funds on the basis of risk. Part of that assessment was the result of work the Council did. We recommended spending the money on the most likely targets and the most significant targets in terms of consequences. This is a significant shift away from allocating funds politically.

It will take a while for risk-based spending policies to take hold. Last week, there was an article in one of the Baltimore papers inviting community-based nonprofits—soup kitchens, projects for elderly, etc.—to apply for \$635,000 in grant money to add bulletproof glass and chain link fencing to their facilities. That's the direct opposite of risk-based. Even with our emphasis on risk-basing, even with Secretary Chertoff's recognition of the value of risk-basing, and even with the efforts of local politicians to protect their communities, we haven't succeeded if we're spending over a half a million dollars to add bulletproof glass to community-based nonprofit facilities.

We must spend sensibly. There's a feeling in the business community that Osama wins if we start spending our growth capital on defensive protection that doesn't benefit us competitively.

Where do skyscrapers in Des Moines and soup kitchens in Baltimore rank versus the Capitol and Grand Central Station? How do we think about that? Part of the risk-based program was what we call the common vulnerability scoring system (CVSS).

When we began to solicit ideas on what was important to protect, everyone had a different idea depending on his breadth of vision, global awareness, and institutional pressures. We developed the CVSS to promote understanding of vulnerabilities and their impacts and to apply limited resources to the most critical vulnerabilities. The system is currently used by the Department of Homeland Security and is the basis for the allocation of funding requested from Congress, i.e., more emphasis on high-vulnerability port cities and less on the smaller cities in the heartland.

CYBER SECURITY

Another NIAC project, headed by George Conrades, CEO of Akamai, developed strategies for hardening the Internet. Mr. Conrades organized a group of Internet experts to determine what can sensibly be done to protect it. The recommendations have been distributed to the software houses that are developing software that can be used at these hardening points. Akamai and Symantec are leading this effort, along with others on the NIAC who have influence with people in the industry.

You might ask: “When you design a new feature or a new function or when you move to Internet 2, why not design out the old vulnerabilities and design in the new, more robust processes?” That’s a very interesting idea. There’s not a lot of money involved—it’s a matter of asking people to think about these issues as they design new products, and I’m told that it’s working pretty well.

PRIVATE–PUBLIC SECTOR COORDINATION

Another of our projects was to recommend ways to involve the private sector in infrastructure protection projects of concern to the government. What we found is that one size does not fit all — not all industries are alike. For example, the railroad industry is highly organized at the industry level. It has a national control center run by the American Association of Railroads that is primarily safety-oriented and traffic-oriented. The railroads compete with one another; but because they’re regional, they don’t compete head to head the way technology companies do—

say Dell versus Gateway or Microsoft versus Oracle. Rather, they coordinate because they have many interconnecting standards like the gage of the rail, the interchange of railcars, etc.

At the other extreme is the apartment industry. A terrorist can cause extensive destruction in a metropolitan area by renting an apartment, turning on the gas, and setting a fuse to light a match after he leaves. The apartment industry is essentially owned by large REITs [real estate investment trusts] or small apartment owners.

“Last week, there was an article in one of the Baltimore papers inviting community-based nonprofits—soup kitchens, projects for elderly, etc.—to apply for \$635,000 in grant money to add bulletproof glass and chain link fencing to their facilities.”

So, on the one hand, we have a highly coordinated rail industry and, on the other, a completely uncoordinated apartment building industry. The question is: what’s the right level of public–private cooperation and information sharing at those two extremes and for all of the other industries in between? We realized that one-size-fits-all federal laws and regulations would not work. Some industries—the highly regulated businesses such as the telecommunications industry, the airline industry, the nuclear power plant industry—already have highly cooperative interchanges of information with the federal government.

We developed a model, which has been approved and adopted, that defines 17 different sectors. Our recommendations, which have largely been adopted, set an expectation at the federal level that each industry will be dealt with slightly differently, reflecting the reality of how well organized the industry is naturally. In some of those sectors, the industry people meet with government people every day. Some of the industries invite government people to sit in their control centers and be quick-reaction interfaces. Others just have periodic meetings and discussions.

This cooperative process is a major accomplishment because the original instinct was to enact laws and regulations that dictated public–private coordination one particular way. We were very pleased to be able to convince them that they had to recognize the realities of each of these different industries.

AVIAN FLU PANDEMIC PLANNING

The avian flu pandemic is an example of how the NIAC works. Typically, the President or his staff ask us a question; we assemble volunteers from the Council; and each person is allowed to have a technical assistant. One person is appointed chairperson. The group meets once a week for 1 hour and interviews as many witnesses as needed via conference calls until all possible issues are explored. Then, they write reports; and the entire NIAC vets them. We’ve had no trouble getting some of the most knowledgeable and interesting people from industry, academia, government, and Nongovernmental Organizations (NGOs) to participate because all they have to do is pick up the phone for an hour; and everything is off the record. We have a lot of good give and take. We have a scribe and, with Secretary Chertoff’s support, a staff at DHS that digests all the material so we can turn out the reports quickly and efficiently.

“The NASDAQ has tremendous redundancy built in—doubly redundant electrical, doubly redundant circuits—because in 1991 or ‘92, a squirrel caused a short circuit that brought the NASDAQ down for 2 hours and 45 minutes.”

The most recent issue was how to deal with the possibility of pandemic avian flu. Health and Human Services (HHS) and the Centers for Disease Control (CDC) had recommended to the President that our limited supply of avian flu vaccine go where it would save the most lives—children and old people. The President asked us to evaluate that recommendation. After about 6 or 8 months of interviews and research, we completely retooled the recommendation.

We asked the 16 (now 17) industry sectors from the earlier study to identify their critical workers. Even though the Public Health Service says it expects a 10–15% mortality rate from avian flu, the mortality rate worldwide has been about 55%. We didn't want to bet that modern medicine was going to reduce 55% down to 10%. So, we used war games with different sectors to determine how to keep the economy going with a large mortality rate.

“Their wives and husbands won't let them come to work. There won't be any trading. And, by the way, you just posited to us that there was going to be about a 4-month decline in economic activity, a little rebound, and then another 4-month wave of avian flu.”

I had previously participated in a game run by the Federal Reserve in New York, along with one or two other financial services people and representatives from the electricity industry, the telecommunications industry, and the commuter rail industry. The electrical sector didn't foresee a problem even if 30% of its people were out sick. If they eliminated new installations, they would be able to reduce their field capacity by about 30% and make up the deficit. The telephone reps said essentially the same thing. The commuter rail people said they weren't sure their workers would come to work; but if they did, they'd sit in the front of the train away from the passengers and would probably be able to get people to work.

Then, I asked, “How many people in this room have been in a trading room and seen people sit shoulder to shoulder? Their wives and husbands won't let them come to work. There won't be any trading. And, by the way, you just posited to us that there was going to be about a 4-month decline in economic activity, a little rebound, then another 4-month wave of avian flu, and more economic decline. So, as a rational man, I am going to wait to buy later; I'm certainly not going to go into work and wait.

There are not going to be any buyers." Well, planners didn't want to hear that, but I think that's the actual human reaction.

LESSONS OF 9/11—NEED FOR RESILIENCE

We learned some lessons from 9/11. A high ranking person at NASDAQ was in the control center with me on 9/11 when the plane flew into the Pentagon. She said, "I'm going to get my child from his nursery school in Alexandria." She bolted. And she had her priorities right. I recounted that story to participants in the war game on the Financial Services Industry and pandemic and said, "That's going to happen thousands of times because people are not going to stay at work if their families are at risk."

I want to talk about a couple of lessons from 9/11 that tie all the NIAC work together. I happened to be in Washington on 9/11. When the second plane hit, I was actually on the phone with Richard Grasso [President of the New York Stock Exchange], who had called to ask me to delay the opening of the NASDAQ. He said "There's some problem up at the World Trade Center and a lot of my people aren't here yet." Then we saw the plane hit. We agreed to talk to each other every hour to see what we could do to help each other.

"That's going to happen thousands of times because people are not going to stay at work if their families are at risk."

As many of you know, the NASDAQ is a highly distributed network. The data centers are in Trumble, Connecticut, and Rockville, Maryland. The NASDAQ has tremendous redundancy built in—doubly redundant electrical, doubly redundant circuits—because in 1991 or '92, a squirrel caused a short circuit that brought the NASDAQ down for 2 hours and 45 minutes. The redundancy was tested on 9/11. We lost a couple of points of presence on Wall Street, specifically at Goldman Sachs and in the Merrill Lynch building, but otherwise, the NASDAQ was functioning.

The phone calls with Grasso expanded with each hour as more and more people conferenced in. At the 1 o'clock call, we had the heads of all the markets, the White House, FEMA [Federal Emergency Management Agency], and the Treasury on. The Treasury is the federal agency that actually controls policy for the markets. The question was asked, "New York, when are you going to open your backup center?" It turned out that the New York Stock Exchange (NYSE) had been joking about having a backup center; they had no backup center.

We decided that we would do whatever was necessary to get the NYSE up as fast as possible. Telephone people from all over the country flew in and laid cables down the middle of the street to get the New York Stock Exchange back up by Monday.

The point is that the industry had not prepared to be resilient. The real heroine of 9/11 is a woman named Jill Considine. Until a week or so ago, Jill Considine was President and CEO of the Depository Trust Company. The Depository Trust Company is a nonprofit jointly owned by all the banks and brokerages that handle, manage, and physically hold all the stock certificates in the United States. Jill locked her people in the building and had the National Guard bring in food and water. They processed that day's settlements, which had been traded 3 days before; they processed the next day's settlements, which had been traded 2 days before; and they processed the third day's settlements. They had a couple of days off when there were no trades; and then, they resumed business.

"The NIAC heard one recommendation to install chain link fencing on both sides of all railroad tracks—even across Kansas!"

The Federal Reserve Board also kept the country going financially immediately after 9/11. The New York Fed couldn't clear checks because checks were moved around by planes, which were no longer flying. If checks couldn't be validated, bad checks would be treated as good. We knew statistically how

many checks would be invalid, but the Fed ignored it and kept the system working.

Between Jill Considine, the Depository Trust, and the Fed, our financial markets kept functioning as we struggled to get the NYSE back up in operation. I'm telling you this to demonstrate the importance of resilience—getting back in action rather than worrying about not being put out of action. Being put out of action may be a huge political problem, but it's not necessarily a big economic problem. Getting back in business is the key.

What happened in New York had economic impacts because the market crashed. But the British experience with the Irish Republican Army (IRA) over the years has shown that the financial markets respond less to each attack—the markets become more resilient. There has to be a balance between investing to protect institutions ahead of time and being able to be extremely resilient after the fact. For example, we can't afford to build a fortress around every mile of railroad. The NIAC heard one recommendation to install chain link fencing on both sides of all railroad tracks—even across Kansas! I'd much rather send a fast-reaction team to fix the blown track than spend money that should be used for growth to defend 100,000 or 200,000 miles of track. The beauty of resilience is that it will help you deal with all sorts of disasters from natural to terrorist-related. The business view on the NIAC is to always consider investments in resilience in planning for the infinite number of possible threats.

Q: Your talk was fascinating. Recently, I attended a seminar in Alexandria, where Dr. Tara O'Toole, the Executive Director of the Center for Biosecurity [University of Pittsburgh Medical Center], talked pretty eloquently and rather forcefully over the fact that you spend a lot of money preparing to prevent bioterrorist acts, but our [health care system] is broken.

And if we have an attack here, here's the analogy I thought of: we're putting up fencing for biodefense but we're not prepared to have a rapid-response team. Could you talk about that aspect?

Mr. Alfred Berkeley – We have not looked at that explicitly, but I certainly agree with you. If you look at it from my point of

view and that of the financial services industry, in industry after industry, we've wound our businesses up so tight to the margin—cut out hospital rooms, centralized x-ray machines, outsourced recordkeeping to India—we're not providing cushions, shock absorbers. In health care, it's a matter of government policy. In most businesses, it's a matter of international competition to lower the cost of labor. We've got this enormous global wage deflation going on, where very bright, very attractive, very well-educated people in other parts of the world are willing to do the same work for a fifth or a third or less of the wages we pay. You're exactly right: we've applied our super-shrewd, short term, MBA mentality to take all the fat out of the system. With the fat goes margins of safety.

The problem is exacerbated by the financial services industry, where there's an enormous focus on leverage of short-term returns. It will throw out a CEO out who builds extra hospital beds if it's a for-profit hospital or adds an extra anything. Because moving from investment to investment is essentially friction-free in the United States, predatory investors milk existing businesses and move on if they fail. For an investor to move from one investment to another, it costs a cent a share: It could be a \$100 stock; it could be a \$500 stock; it could be a \$5,000 stock. It's a cent for any of them... it's friction-free. The punishing unintended consequence for our country is that CEOs who are living quarter to quarter can't afford to build the extra hospital beds or the extra generators or extra whatever. I don't know how to solve that problem other than through the tax code, and that's not going to happen. I don't know if that answers your question or not, but you hit a hot button for me.

Q: *Do you think there should be more coordination between business and the intelligence agencies?*

Mr. Alfred Berkeley – Well, it's an interesting question. One of the projects that I worked on for the NIAC was to interview the CEOs of a number of very large companies about whether and under what circumstances they would work a little more closely with the Central Intelligence Agency and National Security

Agency. I had long conversations with quite a number of people from different sectors, all of whom you would recognize.

Two kinds of responses came from the very large multinationals—be they drug companies, technology companies, or financial services companies. Some said, “I’ve been dealing with these kinds of threats all over the world. The U.S. government people are focused on it now, since 9/11. They’re hard working, they’re smart, and they’re doing a good job, but they just discovered the world. I’ve been dealing with bombings; I’ve been dealing with crooks; I’ve been dealing with industrial espionage all over the world for my entire career. I don’t think that Osama bin Laden is that big a deal to my company. I don’t operate in Afghanistan; I haven’t been able to operate in Iraq for the last 40 years; but before that, we did.” Global CEOs treat terrorism as just another problem. That conversation often led to the resilience discussion: “Don’t order me to protect every door and every plant I’m in or I’ll just put my plant somewhere else because I can’t bear those costs, selling in a global market.”

“But I want all those people to have something to lose; if they’ve got something to lose, they are not going to join Osama, and they’re not going to want to come over here and fight. Democracies don’t fight with each other, basically.”

The other really interesting comment was: “You want me to cooperate more with the CIA and the NSA, but what do I tell the 91 other countries’ intelligence services when they knock on my door?” There’s this divergence in the interests of the home nation and the interests of a global company. The global company is a little less national than you think. It has a different set of objectives, which is a complicating overlay to issues where we say: “I want to talk to you about working a little closer with the intelligence community in the United States.” They’re saying, “I’ve got 91 other intelligence agencies to deal with, too. If you’ve got an incident or an issue, I’m pleased to be as helpful as I can, but it has to be legal, the regulating part of the federal government can’t

have anything to do with it—can't know anything about it, and, by the way, stop sending people from 15 different federal agencies to talk to me about the same issue. And, by the way again, when you send somebody in, please let them know something about my business." These are just the realities of dealing with these companies.

I don't have any easy answer for you. I think the right answer is diversification, and I think it's helping these other countries get rule of law. Probably the right answer is to get at the root cause of the terrorism, probably through those economic arguments we heard today.

"We have to fix the underlying causes of terrorism, which, in my opinion, are people not having enough to feel secure about themselves, their families, and their future. The way to do that is to help with economic reform and ownership."

I can tell you that a lot of the business community people that I deal with say it's perfectly okay to capture and kill a bunch of thugs, but don't aggrandize them so that they're presented as more than thugs—i.e., martyrs. They exist because people are genuinely unhappy, so let's figure out what that unhappiness is.

I think the best thing that could possibly have happened to this country was to have two or three billion people move from command economies to free markets in Russia and China, but we're going through a 50- or 100-year adjustment phase that's going to be really painful for us. But I want all those people to have something to lose; if they've got something to lose, they are not going to join Osama, and they're not going to want to come over here and fight.

The most brilliant legislation we've ever had in this country is something you and I never think about anymore. It's the legislation that allowed us to have a civil society in the face of massive influxes of people who had nothing. It was the Homestead Act. It reflected a brilliant public policy in the 1850s, '60s, '70s and, '80s when there were 13 different waves of European immigration, all

triggered by different causes, like the potato famine or a war in some country. You can see these 13 different ethnic communities in every Atlantic port city. It's because my forefathers and probably yours came looking for opportunity and arrived with almost nothing. The idea behind the brilliant Homestead Act was to give them something to lose. Let them work a plot of land, a sufficient amount of land to support their family for 5 years, and then they own it.

Sounds a lot like a stock option, doesn't it? Stock options are the modern equivalent of the Homestead Act. Wages and tax laws are basically stacked against most American workers. They will never have enough money to live on in the additional years that medical progress has given after they leave the workforce. They have to have savings. The right way to have savings is in the productive assets of the economy—i.e., equities. That's exactly what we want other countries to do: give ownership of the productive assets of their economies to their people. In Islamic law, there are two fundamental biases against that system: no-interest savings (which they work around) and the way property is divided when someone dies. It gets smaller and smaller and smaller and smaller. It's suboptimal for earning a living. France had the same problem until World War II. We have to fix the underlying causes of terrorism, which, in my opinion, are people not having enough to feel secure about themselves, their families, and their future. The way to do that is to help with economic reform and ownership.

A great man named Hernando de Soto—a descendant, I gather, of the explorer Hernando de Soto—has written a book about what economies need to get started. He says that you need really good ownership law so that you're sure of what you own. In India, there's a gentleman at the World Bank, Srivatsa Krishna, who was the "mayor" of Hyderabad when he was in the Indian Administrative Service. He did for the Hyderabad what Thomas Jefferson did for this country in 1815: order land surveys and establish firm ownership and land registries. It meant pushing a lot of squatters off the land and making sure that productive

enterprises could actually own the land under their plant. With clear titles established, Hyderabad boomed.

So, some people in India are getting a shot at a real title to land, which allows them to use it as collateral for a loan. They have a recognized bankruptcy law, a recognized uniform commercial code, and contract law, so they're beginning to have the kinds of certainties that we take for granted here but are the basis for families being able to own their own resources.

Q: *How long do you think the war in Iraq will last?*

Mr. Alfred Berkeley – This is a marathon, not a sprint. It's probably a multi-generational marathon. You can look at it from the thuggery side. Hitler started in a small town in Germany with two thug associates, and the whole Gestapo grew out of two guys who figured out how to harass and frighten and then kill and frighten people.

I had a conversation with Charlie Allen at DHS about this. What expectation should we have for the length of this conflict? He stressed to me the need for the American public to understand that this is a marathon, not a sprint.

I do think you can deal with the thuggery side of it by capture and kill; but I don't think that's sufficient. I think you have to address the fact that half the population of Iraq is under 20, and they have nothing. On television, they see us wasting more than they'll ever have in their entire lives. I'm not talking about issues of globalization and north/south divide and that sort of stuff. I'm just saying we need to promote the same kind of economic opportunity in these countries with these huge population increases that we promoted successfully in Germany and Japan and many other places in the world. Until we fix those root causes—which may take 50 to 100 years—we'll have a problem.

It really amounts to giving the other guy an opportunity to be in a win-win relationship with us rather than forcing him into a win-lose relationship. So it's not an easy answer. We could do a lot by speaking out about the long-term nature of the problem

and its economic roots as opposed to short-term victories and defeats reported in the media.

Q: *Exploring a little more the tradeoff between prevention and resiliency, resiliency doesn't help much if the problem is large numbers of people being killed in an attack. You can't bring them back to life. Even if it doesn't show in the GNP, a lot of people dead is a lot of people dead. Based on the work you've been doing in trying to prioritize threats, do you think that proper attention is being given to prevention of the kinds of threats where large numbers of lives might be vulnerable to a single attack?*

▬ **Mr. Alfred Berkeley** – Well, that would be a chemical or biological/radiological attack.

Q: *Or a bad underground fire in a big city.*

▬ **Mr. Alfred Berkeley** – I think we spend a lot of time on the highly visible, and much less time on the harder to visualize. I think that's human nature. For example, I think that we need to ask people in construction to give an alarm when gas valves are putting out a lot more gas than they should. It's a complex issue. I think we could do a lot more by working with the people who are building and maintaining infrastructure rather than issuing an order for everybody to change their gas meters. I don't think that'll happen—I don't think it's realistic. But I also think that if we just began doing this, we'd get an awful lot of infrastructure fixed. The gas meter is an interesting specific example.

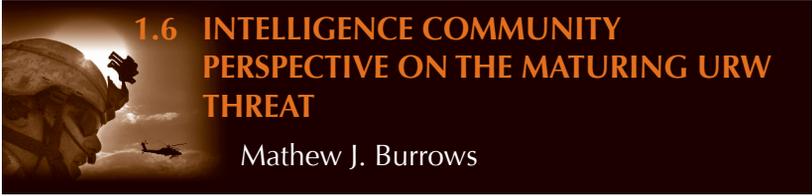
Q: *I'm going to ask one that gets you to extrapolate from your marketing discussion. I was intrigued some years ago by the Chicago Board of Trade trading in catastrophe derivatives. So is there a future for catastrophe insurance in the following case? All the contingencies that you so eloquently explained all involve stable rational expectations. There is a market in expectations that it continues to function. But let me ask you to address the question of catastrophe or something similar where that assumption doesn't hold—where you have a declaration of national emergency, marshal law is in effect, and there are no business owners because the government owns the businesses. Now what?*

—Mr. Alfred Berkeley – We actually have begun looking at this issue in a slightly different way. Remember I said the Depository Trust Company kept going and the Fed honored your checks right after 9/11? Something else happened in Dubai at the same time: Lloyds of London cancelled all its insurance on ships. One of these Sheiks in Dubai said he would underwrite those potential losses personally.

John Chambers, who is at Cisco, and I met with the Deputy Secretary for Homeland Security and asked DHS to begin to compile a list of all the kinds of things like insurance that we might want some enabling legislation in place for, laws that would become effective when an emergency is declared. The Fed made a wonderful interpretation and the right one, but they probably should have had a little clearer authority to do it. There are many other areas in the economy that require a little bit of forethought.

Catastrophe insurance is sold every day—it's called reinsurance. But, there are unintended consequences. The Louisiana Attorney General is saying: the insurance companies should pay for flood damage even though it was specifically excluded from homeowners' policies. Some insurance companies are not allowed to write insurance in New Orleans because they refuse to pay money out for losses they never underwrote to begin with. So, the law is always in a state of flux there.

I think that the ultimate answer is to get as many individual Americans to think about what they would do in a natural disaster and prepare for it, and then they would be prepared for an unnatural disaster. Prevention, resilience, and insurance all knit together to create preparedness.



1.6 INTELLIGENCE COMMUNITY PERSPECTIVE ON THE MATURING URW THREAT

Mathew J. Burrows

INTRODUCTION

I would like to discuss with you today my perspective on the changing character of warfare, including foreign development of so-called “unrestricted warfare” strategies, and the issues this raises for how analysts assess emerging threats to U.S. military operations and security interests.

In the face of U.S. superiority in conventional, high-technology warfare, potential adversaries are developing strategies designed to counter or circumvent vital U.S. operational capabilities and to undermine strategic political and public support for military action. Interest in unrestricted warfare strategies reflects this trend as both potential state and non-state adversaries seek new opportunities and new domains in which to exploit perceived U.S. political and military vulnerabilities.

Foreign unrestricted warfare concepts advocate attacking an enemy’s finances, resources, and networks and the use of media and psychological warfare and terrorism—rather than seeking to defeat military forces on the battlefield—as the means to achieve political objectives and undercut an enemy’s national resolve. If such concepts are employed in the future, we should expect a shift

Dr. Mathew J. Burrows is the Director, Analysis and Production Staff, National Intelligence Council. He is a member of the Directorate of Intelligence (DI) Senior Analyst Service, and has served the CIA in Western Europe, including the development of institutions such as the European Union. Formerly, he was the Intelligence Community Fellow at the Council on Foreign Relations, and special assistant to the U.S. UN Ambassador, Richard Holbrooke. Dr. Burrows served as Deputy National Security Advisor to Treasury Secretary Paul O’Neill.

in the focus of an adversary's attacks—away from confronting the U.S. military directly through force-on-force engagements and towards targeting key elements supporting the U.S. way of war at both the operational and strategic levels. In the future, such attacks could target capabilities perceived to be critical to U.S. military operations such as communications networks, intelligence and surveillance systems, and logistics. In addition, adversaries might seek to undermine U.S. and allied national will by imposing untenable costs, manipulating public opinion, upsetting vital political alliances, and targeting critical U.S. infrastructures.

THE ADVERSARIES' APPROACH TO WARFARE

We should not think of unrestricted warfare as only the tactic of terrorists and insurgent groups. The term unrestricted warfare was recently coined by two Chinese Colonels, Qiao Liang and Wang Xiangsui, to describe how both state militaries and non-state groups could strike out against an enemy with a superior military force in times of conflict. How adversaries will implement such strategies in the future, however, will depend upon their strategic objectives and technical capabilities. In general, I would expect the following:

- *Military powers* with advanced technical capabilities will likely seek to deter U.S. military intervention by acquiring counters to specific military capabilities perceived as critical to U.S. military operations.
- Conversely, *terrorist groups, insurgents, militias, and less advanced militaries* will likely focus on irregular warfare operations, terrorism, and information campaigns to undercut U.S. political and public support for ongoing military operations.
- *Rising military powers* will likely straddle both approaches, seeking some advanced military capabilities—such as air defenses and antiship weapons—while also developing capabilities to impose costs and undermine U.S. resolve through irregular warfare, terrorism, and attacks against U.S. allies and key infrastructures.

What does this shift in how our adversaries approach warfare and the potential employment of unrestricted warfare strategies mean for the character of future conflicts and the types of threats we will face? The implementation of such strategies, especially if they are enhanced by the emergence of new technologies, will likely present new challenges to U.S. policymakers and defense planners. Let me mention a few that I can foresee:

Containing the escalation and expansion of future crises will likely become more problematic in the future. The inability to compete directly with U.S. conventional forces will continue to drive some adversaries to attempt to expand and escalate conflicts beyond the traditional battlefield. Some adversaries, for example, might target the U.S. mainland and territories and those of its key allies in an attempt to distract U.S. strategic attention, compel the redeployment of military forces to the homeland, and undercut resolve for continuing military operations. In addition, both state and non-state adversaries might view the intentional escalation of a conflict—by imposing or threatening to impose significant costs in response to U.S. military operations—as a way to disrupt ongoing U.S. operations, seize the initiative, and redefine the conflict on their own terms.

Advances in biotechnologies and information technologies are creating new opportunities for adversaries to expand a conflict and create widespread disruption. The globalization of biotechnology industries is spreading expertise and capabilities and increasing the accessibility to biological agents that may be suitable for a disruptive biological attack as part of an adversary's unrestricted warfare strategy. Also, foreign perceptions of increasing U.S. military and economic dependence on information systems could lead future adversaries to consider attacks against U.S. networks and communication capabilities.

The recent conflicts in Iraq and Lebanon will likely foster interest by both state militaries and non-state groups in adopting irregular warfare strategies as their primary warfighting approach for countering superior military forces. The elevation of the importance of irregular warfare in the perception of potential U.S. adversaries will likely lead to new challenges to U.S. ground

forces and peacekeeping operations. Furthermore, advances in information, communication, sensor, and man-portable weapon technologies have the potential to increase the effectiveness of future foreign irregular warfare operations. Such capabilities might also be exported by states to proxies along with other modern weapon systems to increase their effectiveness against U.S. or allied military forces as part of an unrestricted warfare strategy.

Changing international attitudes towards war and the use of military power are likely to be exploited by adversaries pursuing an unrestricted warfare campaign. “Media warfare” is likely to become an increasingly important element in future wars as adversaries seek to exploit advances in mass communications and other electronic media to manipulate public opinion and organize local and widespread opposition to U.S. forces and interests. In addition, some experts have argued that changing attitudes towards war might lead to an “asymmetry of brutality” in future conflicts. The United States and its allies will seek to restrict the level of violence and destruction in future conflicts because of adherence to moral and legal standards and through the employment of precision weapons. However, potential adversaries pursuing unrestricted warfare strategies might see advantages to raising the level of violence and brutality to undermine U.S. resolve, influence public opinion, and provoke a U.S. response that would be supportive to their cause.

“The Intelligence Community is particularly vulnerable to surprise by rapidly changing and readily available emerging technologies whose use by state and non-state actors, in yet unanticipated ways, may result in serious and unexpected threats.”

Emerging unrestricted warfare capabilities will pose new defense challenges for the United States and its allies. Increasing threats from long-range weapons, cyber attacks, and terrorism will affect the security interests of the United States and its allies alike. Mutual development of defensive strategies and capabilities

to deal with these threats will be critical in countering future adversary attempts to coerce using an unrestricted approach to warfare.

A COLLABORATIVE INTELLIGENCE COMMUNITY

How well are analysts positioned to assess and warn about emerging strategic challenges such as those posed by foreign unrestricted warfare concepts? In its 2005 report to the President, the Robb-Silberman Weapons of Mass Destruction (WMD) Commission examined the capabilities of the Intelligence Community in the aftermath of the Iraq WMD; and estimates noted deficiencies in long-term research and strategic thinking in the Intelligence Community. The Commission found that the drive to fill “current intelligence” requirements had crowded out work on strategic military issues by the Intelligence Community. Furthermore, the Commission’s report stated that the Intelligence Community was particularly vulnerable to surprise by “rapidly changing and readily available emerging technologies whose use by state and non-state actors, in yet unanticipated ways, may result in serious and unexpected threats.”

Since the publication of the WMD Commission’s report, the Intelligence Community, under the direction of the Director of National Intelligence, has taken steps to address the imbalance of intelligence analysis towards “current intelligence” by promoting analysis that is both “wide”—cutting across traditional analytical accounts—and “deep”—having a long time horizon. Of particular note is the establishment within the National Intelligence Council of the Long Range Analysis unit. The purpose of this unit is to focus on long-term, strategic analysis and to alert policymakers to strategic trends that are evolving in such a way as to potentially threaten U.S. interests. In particular, this unit seeks to promote collaboration between the Intelligence Community and nongovernmental experts in understanding and assessing issues and trends that may have gone unnoticed or underappreciated if our focus was strictly on current developments. The Long Range Analysis unit, for example, just published an assessment

on the changing character of warfare that summarized the findings of a collaborative effort among intelligence analysts and nongovernmental experts to assess emerging threats to the U.S. way of war.

CONCLUSION

Let me conclude by citing six recommendations for how the Intelligence Community can continue to position itself to best understand and warn against new foreign approaches to warfare and emerging threats to U.S. strategic interests:

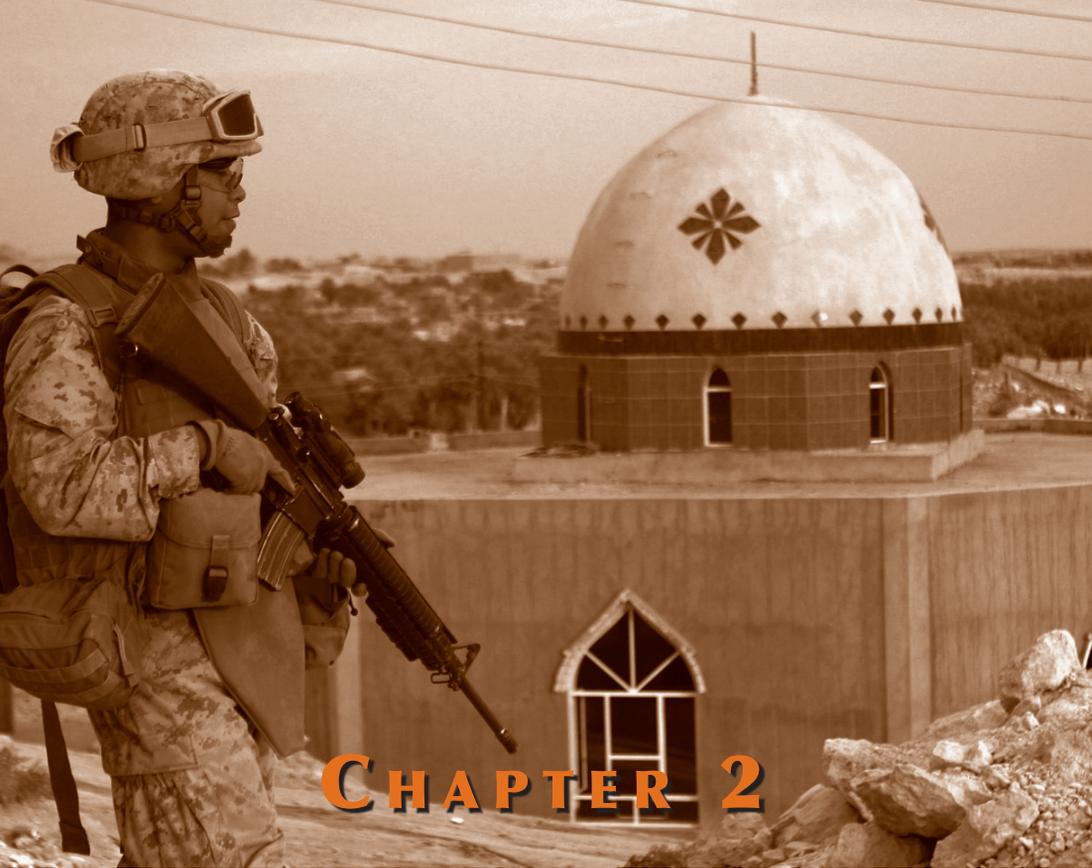
- 1. Understanding the implications of emerging adversary capabilities and strategies requires a holistic approach to analysis.** By this, I mean that it is not sufficient to assess technology developments alone in identifying future threats. Rather, analysts should examine the synergy between technology developments, emerging foreign capabilities and concepts for future war, and geostrategic political and security dynamics. Analysis that is organized into separate functional and regional areas will be ill-suited to addressing complex interdisciplinary issues such as the challenges posed by unrestricted warfare strategies. Such issues require strong integration among the analytic, technology, and strategy communities—which, I am pleased to see, is a major theme and goal of this symposium.
- 2. Red teaming and exploratory analysis are useful tools in understanding new foreign approaches to warfare.** Traditional evidence-based, linear, deductive analysis is often insufficient to address complex problems such as emerging unrestricted warfare strategies that can challenge prevailing assumptions and linear trend projections. Red teaming of future foreign warfare strategies that takes into account foreign threat perceptions, military culture, leadership dynamics,

technological acuity, and societal norms can be useful in identifying potential doctrinal and technological developments that could be disruptive to U.S. security interests. Such analytical techniques are especially important where there is a dearth of current information on the capabilities and strategies of a potential future adversary because those technologies help determine which indicators might reveal the emergence of a new threat.

- 3. Understanding foreign motivations, intentions, and perceptions of U.S. military capabilities, objectives, and vulnerabilities is key to warning of emerging threats to U.S. interests.** Understanding when an adversary perceives it has the necessary capabilities to deter or disrupt U.S. military operations is as important as knowing the technical characteristics of those capabilities. Failure to understand foreign perceptions could lead to the United States being surprised by preemptive or escalatory actions taken by an adversary convinced of its ability to disrupt U.S. military operations or undermine U.S. political resolve.
- 4. Analysts should be cognizant of potential foreign attempts to use mass media to influence and manipulate perceptions.** Foreign media warfare and other influence activities are likely to be a part of a future unrestricted warfare strategy; therefore, analysts need to be prepared to recognize and warn of such efforts.
- 5. Analysts should also examine potential future events that can be disruptive.** Global epidemics and widespread environmental disasters are examples of events that could significantly impact international security dynamics and future U.S. military operations. Our adversaries might seek to

exploit such events for their own benefit. Scenario-based analysis can be helpful in anticipating such strategic changes, assessing their potential implications for U.S. interests, and assisting analysts in identifying important dynamics that would otherwise be missed in a narrower analytic approach.

- 6. The analytic community needs to ensure that analysts remain properly trained, organized, and rewarded for addressing complex, multidisciplinary, strategic, and long-range issues.** This is critical to ensuring that the analytic community maintains a sustained effort to collect, examine, and warn against emerging strategic issues such as the foreign development of unrestricted warfare strategies and capabilities. Failing to do so risks a return of the imbalance in analysis towards current developments that the WMD Commission identified.



CHAPTER 2

STRATEGIC POLICY ROUNDTABLE

THE NATURE OF URW



A familiar aphorism among military planners holds that getting the strategy correct can bring success in spite of many tactical errors, but excellent tactics applied to an incoherent strategy will lead nowhere. Such a principle also applies to addressing the nature of URW. Thus, an examination of needed methods of analysis and technologies should begin with some understanding of the strategic circumstances in which they must operate. Hence, this session makes projections on the nature of the threat, the strategic context, and options for dealing with URW.

While it examines possible contingencies, this session makes no claim to project a future U.S. policy or strategy. Instead, the presentations set forth some of the dimensions that a strategy must consider. Needless to say, no one panel session can encompass the range of factors involved; but addressing some of the key factors and projected international developments sets a valuable context for later discussions. With that caveat and an awareness of how little we can know of the future, these presentations look at likely scenarios for U.S. military involvement and provide more specific examinations of the possible roles of WMD in warfare.

Professor Thomas Keane of the Paul Nitze School of International Studies at The Johns Hopkins University is also the executive director of the Foreign Policy Institute, the Merrill Center for Strategic Studies, and senior adjunct professor of Strategic Studies at SAIS. He is a former professor of military strategy at the National War College, Air Force Academy; planner on the Air Staff, Forward Air Controller in Vietnam; and B-52 Squadron Commander.

Despite current and intense U.S. involvement in counterinsurgency operations in Afghanistan and Iraq, this panel will not explicitly address those countries or counterinsurgency in general. As Dr. Ron Luman mentioned earlier, at the first symposium on URW, held last year, the focus was heavily on counterinsurgency operations in those countries and on the Global War on Terror in general. This symposium should be seen as a complement to last year's event, with the two together providing a broad-based assessment of the future strategic landscape.

In the first presentation, Michael O'Hanlon looks at regions in Asia in which conflict could motivate large-scale U.S. involvement. Rather than just a listing of possible conflicts, his analysis of the region delivers more substantial judgments. First, he presents the relative plausibility of each scenario and the likelihood of U.S. involvement. Then, he estimates the kinds of military forces or capabilities that might be required. Finally, he discusses the probable objectives of the combatants involved, setting in proper context the stakes of U.S. force involvement. While areas outside Asia have the potential for deadly conflict involving the United States, possible scenarios involving states ranging from North Korea to Pakistan to Iran encompass some of the world's most critical and most dangerous situations that planners must consider.

The Asia Pacific region offers not only potentially the most serious battlegrounds but also includes countries identified now as most active in the acquisition and proliferation of WMD. The possession of WMD by states such as North Korea or Iran or by non-state actors poses particular problems. In addition, the long-standing enmity between India and Pakistan, two nuclear states, raises the possibility of use of nuclear weapons. It is with these dangers in mind that the remaining two presentations of the panel focus on WMD and their potential use.

Dr. Brad Roberts lays out a framework for evaluating the WMD threat. Far more than just an estimate of weapons' capabilities, Dr. Roberts proceeds through an analysis of why WMD has not yet been used in the post-Cold War setting, differentiating between the motivations of states and non-state

actors and between the various conditions that might encourage or discourage the use of these weapons. His explanations of why states have not used WMD not only provides a corrective to much of what passes for fear-mongering on the possible use of these weapons, it also invites consideration of what happens when or if past impediments no longer apply. Most importantly, Dr. Roberts sets the discussion of WMD in the strategic context of the circumstances in which WMD might be used and the types of weapons that would have most or least utility. Finally, his analysis of WMD considers both basic elements of a threat: its capability and intent.

Building on the presentation of Dr. Roberts, Prof. Mary Habeck deals specifically with how radical Islamists—she uses the term jihadists—view the possible use of WMD and how those perspectives may be changing. Her presentation looks closely at the history of Islamic teaching on the treatment of non-combatants, warfare with non-Muslims, and the rules of war in which Islamic forces are engaged. Dealing specifically with the issue of the barriers to WMD included in Dr. Roberts' presentation, Prof. Habeck outlines how in recent years jihadist proclamations have declared previous restrictions in the conduct of warfare no longer valid. Her conclusions indicate a serious and immediate threat of WMD use against U.S. forces and the United States itself.

These three presentations introduce important perspectives on the nature of the threat and areas of possible involvement for U.S. forces. Together with last year's addressal of the threat environment, they provide an essential framework for establishing priorities of needed analysis and technological developments that will be discussed at this year's URW symposium.



2.2 SCENARIOS FOR FUTURE CONFLICTS

Michael O'Hanlon

This article discusses five places in the Asian littoral where the United States must be prepared for future conflicts. Although wars in these areas cannot be predicted with any kind of definitive likelihood, the scenarios are plausible enough that the U.S. has to prepare. This kind of exercise helps us frame the broad discussion about U.S. strategy, defense budget choices, the kinds of technological capabilities we must develop to meet these challenges, and the kinds of asymmetric threats with which we must be most concerned.

INTRODUCTION

Forgive me for beginning this with a golf joke, but it has a relevant moral. The joke is partially based in reality—the time that Tiger Woods and Bill Clinton played golf together. Clinton teed off first and sliced the drive badly, and it went into the woods. Since this was the first hole and he was playing the best golfer in the world, President Clinton did not feel it was too unreasonable to give himself a mulligan. So Clinton hit the next drive, and this

Michael E. O'Hanlon is a senior fellow in Foreign Policy Studies at the Brookings Institution, where he specializes in U.S. defense strategy and budgeting, homeland security, Northeast Asian security, and humanitarian intervention. He is also adjunct professor at the Public Policy School of Columbia University, a visiting lecturer at Princeton University, and a member of the International Institute for Strategic Studies and the Council on Foreign Relations. He is a frequent op-ed contributor and television speaker and has written a book on defense strategy for the post-Saddam era; another on the use of the military for humanitarian intervention; and most notably, one on protecting the homeland.

one hooked way left. It is somewhat inappropriate to take two mulligans on the same hole, but the weather is cold and Clinton is in his 50s—he needs a little time to loosen up—and he’s playing Tiger, so he takes a second mulligan. He hits his next drive straight down the fairway—except it goes into a pond. He gives himself a drop and hits his next shot onto the green. Tiger, meanwhile, plays a fairly uneventful hole and pars it with a couple of putts. Clinton’s shot from behind the pond lands about eight feet from the pin, so Clinton picks up his ball and says, “Tiger, I just beat ya. I had a three on that hole.” That’s the Bill Clinton part of the story, and that part is (mostly) true.

The next part, which is also true—at least in terms of how the North Korean press reported this particular outing—is that Kim Jong Il recently played his first round of golf. According to the Korean press reports, of the 18 holes he played, he had a hole-in-one on eight of the holes. The North Korean press did not give the detailed scoring on the other nine, but I think we can safely assume his overall 18-hole score was somewhere in the range of 30 to 35 based on this initial assessment of the holes-in-one. That story tells us a little bit about the North Korean regime and the nature of who we might have to face there.

Finally, even though we all love the Chinese—and, in fact, this story is a little bit complimentary—Hu Jintao played his first round of golf. Instead of bothering with any kind of fabricated story, the Chinese had Hu Jintao go out into a forest and hit 18 balls, and in the next 4 hours, they built a golf course around those 18 shots to make sure that his balls wound up in the right place. That story reminds us about the nature of whom we are potentially dealing with in this world, their capabilities and their strengths, and how they sometimes have certain asymmetric advantages over us.

POTENTIAL FOR CONFLICT IN THE ASIAN LITTORAL

I will begin with two scenarios that I do not propose we plan against—I will not address each and every scenario I can possibly contemplate. I just want you to imagine the different scenarios around the world in which we could possibly fight. My criteria

for assessing the plausibility of the scenarios are likelihood of the initial conflict, likelihood of sufficient U.S. strategic engagement or interest to get us involved, and whether we get involved directly to reverse whatever aggression or operation is at issue or take a more indirect approach. I want to start with two that do not meet these criteria.

UNLIKELY SCENARIOS

The two unlikely scenarios are a possible Russian attack on the Baltic States and a future Chinese threat to the Korean peninsula. A Russian attack on the Baltic States used to be in Paul Wolfowitz's list of possible scenarios when he was Undersecretary of Defense for Policy in the first Bush administration. The defense planning guidance that was leaked to the newspapers at that time had six or seven scenarios. That guidance was the genesis of the whole two-war framework, and it was ultimately concluded that the North Korea/Iraq simultaneous scenario was the most demanding. One of the other scenarios on that list was a Russian threat to Latvia, Lithuania, or Estonia; and we can all remember the argument about why this kind of scenario was plausible.

Now, of course, those three countries are members of NATO. So in one sense, we have an even more direct obligation to worry about their potential for being attacked and our potential for having to respond. Vladimir Putin, despite today's news about his willingness to be a little tougher with Iran, has not been a great friend of the United States recently, as evidenced by his engagement with U.S. Defense Secretary Robert Gates a few weeks ago in Europe.

You could say the Russian scenario is very real and serious, and one we should plan against. Even though we have an Article V commitment to the Baltic states, if this scenario ever did transpire, my argument would be that the military disadvantages of responding in that particular setting in a direct, symmetrical way would simply be too great to be worth the trouble and strategic risk. The United States would be much better off organizing a Cold War-like economic squeeze of Russia than trying to respond directly with ground forces.

For any Russians in the audience, I apologize for starting with this kind of a scenario—I do not mean to sound Russia-phobic. In this business, when we think about scenarios, we have to be a little bit imaginative and think through the what-ifs. Who would have thought 10 years ago that the U.S. would be fighting in Afghanistan? I am using these examples to broaden the scope of imagination far enough to be prudent.

I submit to you that the Baltic State scenario is a) unlikely, and b) even if it occurred, a much better strategy would be to respond indirectly. So I will take that scenario off my list and move to Korea—one Korean scenario I think we do have to worry about—but I will get to that next. The scenario that I would submit we do not have to worry about in direct military terms is a future Chinese threat to the Korean peninsula. I am sure that the experts at this URW symposium who study Korean issues are well aware from Chinese writings and political discourse, that Chinese claims to portions of the Korean peninsula date back to kingdoms that existed over a millennium ago. How do we confidently project that China, with its growing population, its thirst for resources, and its historical claims, would never threaten either Siberia or Korea? I would submit that:

1. China has too much of a real interest in staying engaged in the world economy to bother with that kind of limited territorial acquisition, which all of China's major economic partners would consider unjustifiable.
2. Getting into another land war with China on the Asian landmass would not play to our strategic strengths.

If this unlikely scenario were ever to happen, the proper American strategic response should be to organize a combination of naval and economic sanctions that would penalize China until it reversed its aggression. If necessary, we could be patient and wait many years for the situation to play out. This is not a major scenario—certainly not for ground force planning.

LIKELY SCENARIOS

North Korea Nuclear Facilities

Now, I will propose some scenarios that I think we do have to worry about. All of us in the community of defense specialists have thought about these issues. Nobody here is naïve about Korea, and many of you know a good deal more about it than I do. The point I want to make is that a Korean conflict is still plausible, although I hope it is somewhat less plausible now because of the recent negotiations and progress towards putting the North Korean Yongbyon nuclear facility under wraps and, ultimately, I hope, dismantling it. If that agreement falls apart, or if the North Koreans make progress on their underground uranium enrichment program, we may feel that we have to destroy that fissile material production capability to keep North Korea from becoming a “nuclear Wal-Mart.” Under that scenario, I do not think it is plausible that the U.S. would simply invade North Korea.

However, under certain circumstances, I think it is plausible that the U.S. would decide to launch a surgical strike against North Korea’s nuclear capabilities using air power and maybe even Special Forces. It is unlikely the U.S. will ever find Korea’s existing weapons and be able to target them in this kind of a raid, but we could target their fissile material production capability and likely would consider doing so. You may remember that Secretary Bill Perry basically threatened this kind of strike in 1994 at the very moment when the Clinton administration was having troubles being tough even in Somalia and Rwanda and Bosnia; yet, Perry threatened a far more capable potential enemy when he said on national TV, “We will not let the North Koreans develop a nuclear arsenal.” Jimmy Carter offered Kim Il-sung the carrot of direct dialogue with the United States in exchange for North Korea’s cessation of its nuclear program, and he wound up with a pretty nice carrot-stick policy that helped lead to the agreed framework.

If Perry could make that threat then, it is plausible that a future Secretary of Defense would do the same thing. In fact, I am

surprised the Bush administration has not done something similar in the last 5 years—obviously, the focus on Iraq made it harder to use a similar kind of coercive diplomacy against North Korea. I hope very much that the new deal that Assistant Secretary of State Christopher Hill has negotiated will make this threat unnecessary in the future. However, if North Korea ever resumes construction on these big reactors, a war could get started. If the U.S. were to strike those reactors, no one knows what the North Koreans would do next. That is why we have to keep Korea on the planning horizon.

Taiwan Strait

Another scenario that I think we still also have to keep in the portfolio of possible contingencies for U.S. military planning is the Taiwan Strait. That contingency has been on our national list one way or another for more than 50 years, going back to the days of Eisenhower and the nuclear threats towards China in the 1950s over Taiwan. This issue was of acute concern in the mid-1990s after the Chinese missile strikes led to beefed-up American carrier deployment in the Taiwan Strait vicinity.

“I had not fully appreciated the nuance of sovereignty versus independence until Richard and I did this book; many Taiwan leaders see pursuing more sovereignty as totally legitimate.”

Since that time, things have cooled off a little bit. However, I would like to present a scenario that is informed by historical conflicts discussed in a book I coauthored with my colleague, Richard Bush, who is a Taiwan expert and has been studying the intricacies of Taiwan domestic politics.¹ A real possibility exists, just as we have seen with President Chen Shui-bian, that some future Taiwan leader will decide to push the independence issue far enough to provoke China. Richard, who is a huge supporter of

¹ Richard Bush and Michael O’Hanlon, *A War Like No Other: The Truth About China’s Challenge to America*, Hoboken, New Jersey, John Wiley & Sons Inc., 2007.

Taiwan, has helped me appreciate some of the ways in which this scenario could come about.

The leaders of Taiwan see their role in the world as being inappropriately curtailed by China. Even if they are prepared to say they do not want independence right now, they want more sovereignty, more independent decision-making capability, and more standing in various international organizations even if they are technically not considered to be a nation state by the international community. I had not fully appreciated the nuance of sovereignty versus independence until Richard and I did this book; many Taiwan leaders see pursuing more sovereignty as totally legitimate.

Many U.S. officials also see Taiwan's pursuit of sovereignty as entirely reasonable. However, U.S. policy is to keep the Taiwanese from pursuing outright independence. That is a very fine line to walk: "You can go ahead and get more sovereignty but not more independence." Let's hope these two words translate well into Chinese and that the Chinese always make the same distinction that we do between the two and understand what the Taiwan leaders are doing for domestic political reasons versus for international reasons. The Taiwan Strait issue is not over yet.

My contribution to *A War Like No Other* was to think through the dynamics of crises and conflict decision-making and escalation as we potentially get into a shooting war with China over Taiwan, especially in the event of what I call a "leaky blockade," where China is smart enough not to try to invade but simply tries to curtail commercial traffic in and out of Taiwan through the use of the occasional submarine hit-and-run patrol. What does the U.S. do in response? If we deploy more naval assets to the region, the Chinese may back down for a while, or they may try to sneak one submarine through and shoot out a ship or even try to hit a carrier—or make us worry that they could. Certainly, they would keep the pressure on the Taiwan economy. No one knows how this situation will play out. If it takes several months or years to play out, it is not clear that we will be able to sustain this kind of a naval presence in the western Pacific to guarantee access for ships in and out of Taiwan. China may find that it has the upper

hand. It is not clear who would then escalate to a higher level of conflict—would the United States want to start attacking Chinese submarines in their ports as a way to prevent them from continuing this blockade? If the U.S. did so, how would the Chinese respond once the U.S. had hit at PRC territory? The potential for escalation is high, and the U.S. would face many challenges in the ASW, anticruise missile, and antiballistic missile realms as well as broader strategic questions.

THREE MORE SCENARIOS

I will now briefly present three different scenarios. The scenarios I have discussed so far play to U.S. naval capabilities and air power. In the case of Korea, the scenarios involve U.S. ground forces as well. In South Korea, the U.S. is fortunate to have an ally that has developed good ground forces over the years. Therefore, one could make the argument that, in east Asia, the U.S. can ratchet back its focus on ground forces once the Iraq operation is concluded and possibly realize Donald Rumsfeld's transformation vision after all—in which the U.S. relies more on its air power, high-technology, and naval strengths and less on its ground forces. However, I do not think that is going to happen—and south Asia is one of the main reasons why.

The two scenarios regarding south Asia involve the collapse of Pakistan and an Indo-Pakistani war over Kashmir. I will begin with Kashmir.

Kashmir Scenario

India does not want any other nations to intercede or even discuss Kashmir—it does not want any help diplomatically. The U.S. would never forcibly intervene to stop the kind of war that an Indo-Pakistani war over Kashmir represents. The U.S. is not going to become involved in the business of deciding who should rule Kashmir or whether it should be independent, trying to insert a million-person-strong ground force into Kashmir, or forming a NATO coalition to make sure that it is liberated. If the Indians and the Pakistanis begin another conflict over Kashmir and, this time,

they do not ratchet down the confrontation quickly, the possibility of nuclear escalation exists.

If the possibility of nuclear escalation increases or nuclear weapons are used, what does the world do? Do we really stand by and let India and Pakistan kill 100 million people in South Asia and say that we are going to stay out of this conflict because we have no formal strategic commitment to either country? I do not think so, especially because any scenario involving Pakistan's basic cohesion as a nation and the future security of its nuclear arsenal are of intense strategic concern to us. I will say more about that in a second. I think it is highly possible that, if an Indo-Pakistani war escalated to the point where use of nuclear weapons was likely, the international community would get extremely involved.

What we would say to India and Pakistan—and they may even be saying this to us quietly at that point—is: “We are prepared to offer trusteeship for Kashmir, robust international monitoring of Kashmir's borders to keep infiltrators and terrorists out, and, in 10 or 20 years, some kind of a referendum process for Kashmiris to determine their own future. India, you will not like this, and Pakistan, you will not like this that well; but if the alternative is nuclear war, maybe you will like it better than you used to.” That means that, all of a sudden, NATO is deploying a couple hundred thousand forces to Kashmir and sustaining them for many years. I think that is a distinct possibility. Let's hope the Indians and Pakistanis are on the way towards solving Kashmir—or at least realizing they cannot afford military escalation to resolve the problem, but I am not confident. Like my other scenarios, I think there is at least a 5% to 10% chance that this could go the wrong way in the next decade or two.

Pakistan Collapse

None of these scenarios is meant to be overly fear-mongering. I do not think any of them are super likely. I can see a 5% to 10% chance of most of these scenarios happening and potentially involving U.S. forces in the next couple of decades. If the Pakistan state collapses suddenly, it is too late. The U.S. cannot get enough forces there to make any difference. If Pakistan begins to fray

over time and the state asks for international help to shore up stability, it is implausible that the U.S. would say no. Because of its nuclear arsenal and the potential for it to get into the hands of Islamic radicals, a collapsing Pakistan is just as great a threat to our security as a Soviet invasion of Europe would have been in the post-World War II/Cold War era.

Iran

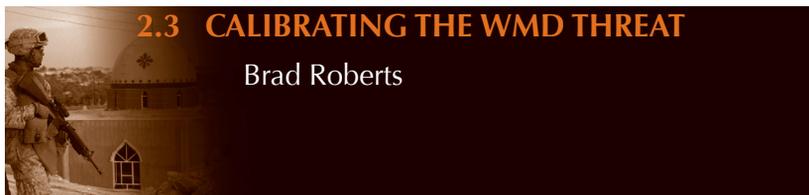
I only have one scenario left—Iran. Similar to the situation with North Korea, if we bomb Iran’s nuclear facilities, no one knows what will happen next. I do not think the Iran scenario is likely to lead to all-out invasion and regime overthrow. However, I think there is a distinct possibility of a much more engaged, longstanding Persian Gulf-kind of conflict, with Iranians using cruise missiles, antiship missiles, torpedoes, and sea mines against U.S. forces and those of our allies in the region. We would essentially have another “war of the tankers” in response to a U.S. strike on Iranian nuclear facilities. I am not trying to suggest this is likely, but there is enough of a possibility that I think we have to plan for that too.

CONCLUSION

There are many possible scenarios besides the ones I have discussed here. We all know in this business that unpredictable things happen. When I applied my criteria for assessing the plausibility of major conflicts, I came up with five or six big candidates—not even counting Latin America and Africa—just looking at the Eurasian littoral, where I think the U.S. has to create and sustain a broad range of capabilities to be reliable custodians of our future security.

2.3 CALIBRATING THE WMD THREAT

Brad Roberts



INTRODUCTION

Most American experts who worry about the problem of unrestricted warfare have a fairly clear view of the nature of the WMD threat: It's a given. We Americans tend to view weapons of mass destruction as the quintessential tools of asymmetric warfare. Our national concern about WMD has grown steadily more pronounced over the last two decades as the Cold War receded and new problems emerged associated with both state and non-state adversaries that could not face the United States in symmetric military terms and expect to win—or even to survive. As many experts and policymakers have argued, “It’s not a matter of if but when.”

But this fairly clear view must be squared with actual experience. In the period since the end of the Cold War, the U.S. military has been heavily engaged overseas; but not a single state adversary has chosen to employ WMD against U.S. forces or other interests. Even in those wars where the United States sought to remove a regime (Milosevic, the Taliban, and Saddam), the WMD threat did not materialize. Non-state actors too have not met U.S. expectations in this regard. In the many thousands of terrorist

*Dr. Brad Roberts is a member of the research staff at the Institute of Defense Analyses in Alexandria, VA. He is also a member of DoD's Threat Reduction Advisory Committee and an advisor to the STRATCOM Strategic Advisory Group. His recent publications include *Deterrence and WMD Terrorism: Calibrating its Potential Contributions to Risk Reduction* (IDA, 2007).*

incidents in the last two decades, only a very small handful have involved the use of chemical, biological, radiological, or nuclear materials. Moreover, none sought to exploit their full lethal potential.

I invite you to recall the words of Sherlock Holmes, in a Sir Conan Doyle short story entitled “*Silver Blaze*.”

Inspector Gregory: “Is there any point to which you wish to draw my attention?”

Sherlock Holmes: “To the curious incident of the dog in the night-time.”

Gregory: “The dog did nothing in the night-time.”

Holmes: “That was the curious incident.”

I am interested in the dog that did not bark. Why hasn’t this dog barked, and what do we do about that? How should we understand this stark contrast between expectation and reality? Have our fears been exaggerated? Or is it simply that, so far, U.S. adversaries have simply been incompetent in their attempts to employ these capabilities? To explore these questions, I will explore first the interests of terrorists in WMD and then rogue states.

“I am interested in the dog that did not bark. Why hasn’t this dog barked, and what do we do about that?”

Answers to these questions are helpful to calibrating the WMD threat. It is important to do so because this offers a contrast to the polar extremes of fear-mongering coming from some segments of the counterterrorism community and the complete complacency that grips other parts of this community.

TERRORISTS AND WMD

Decades ago, Brian Jenkins, terrorism expert and advisor to the RAND Corporation and the National Commission on Terrorism, expressed a key insight into terrorist objectives:

“Simply killing a lot of people has seldom been a terrorist objective. Terrorists want a lot of people watching, not a lot of people dead. Terrorists operate on the principle of the minimum force necessary. They find it unnecessary to kill many, as long as killing a few suffices for their purposes.”

Terrorists motivated as described by Jenkins accordingly had little interest in weapons of mass destruction. They cranked up the volume of violence loud enough to get attention to their cause and also to win concessions. But they had to worry about the problem of killing too many—of alienating key sponsors and enablers, of offending those whom they purported to represent, of turning internal opponents into police informers.

But in the 1990s, this form of terrorism seemed to wane and something more sinister to take its place. The bombings of the World Trade Center and then the federal building in Oklahoma City; Aum Shinrikyo chemical attacks in Japan; and al Qaeda’s unfolding actions in Africa, the Middle East, and elsewhere signaled a radical shift in terrorist ideology and objectives. Private constituencies and radical religious ideologies overshadowed public constituencies. Ambitions became revolutionary in the broadest sense, and the terrorist innovators became motivated by a desire to kill in much larger numbers. This has led one commentator on Jenkins’ work to argue as follows:

“In today’s world, marked as it is by groups such as al Qaeda, it is no longer true that terrorist groups don’t want a lot of people dead. It is, however, still very much the case that they want a lot of people watching.”¹

1 hsgac.senate.gov/_files/050307Doran.pdf: Statement of Michael S. Doran, Deputy Assistant Secretary of Defense Support to Public Diplomacy before the Committee on Homeland Security and Governmental Affairs, United States Senate, 3 May 2007.

In our national discussion about terrorism, the focus typically is on how much traditional terrorism has been replaced by new forms of transnational and religiously inspired terrorism. We should not forget that some of the old faces of terrorism remain. These include terrorist loners, national separatists, and even the occasional right wing militia group. Moreover, many al Qaeda affiliates fit Brian Jenkins' aphorism very well. They are after governance, territory, and legitimacy; and this thrust constrains their interest in mass casualty attacks.

But what about the "new faces" of terrorism? What purposes guide their thinking about the differences between killing enough and killing too many? It is helpful to distinguish between apocalyptic, catalytic, and instrumental purposes.

Apocalyptic – To destroy Western society. Supporting evidence is psychological gratification of mass casualties and motivation of "holy duty" to acquire WMD. However, the 9/11 attackers did not kill "as many as possible." They killed enough to make us fearful where we had felt safe and to damage powerful societal symbols.

Catalytic – To unleash pent-up resistance to Westernized and corrupt regimes, to induce U.S. overreactions that would discredit it, and thereby to change the regional status quo.

Instrumental – To generate fear in America to induce military disengagement from the Islamic world.

In my view, within the militant Islamic extremist movement, each of these purposes is at play, albeit at different times and in different ways. This uncertainty does not make it very easy for us to calibrate how much incentive and restraint they have when it comes to mass casualty attacks. Accordingly, very many different opinions have crept into our national debate about how to explain the gap between our expectations of WMD terrorism from Islamic extremists and our experience—so far, of course. Collected in Figure 1 are some of those opinions.

Various Propositions in the Debate:

1. The al Qaeda leadership core is scattered or destroyed and thus incapable of strategic guidance to the campaign or of sustaining the special programs for “terrorist spectaculars.”
2. The rank and file are less energetic, competent, and capable of innovation than the leadership would have hoped.
3. State sponsors have pulled back their support for fear of going the way of the Taliban and now Saddam.
4. Usama bin Laden (UBL) does not need a game-changer now because:
 - a. This is an epochal struggle, and his focus is now the Near Enemy.
 - b. He sees things unraveling in the Umma in ways that serve his interests.
 - c. It took a decade to crush the USSR, and the Iraqi outcome looks promising.
5. Like Saddam in 1991, UBL went to war without ready WMD.
6. The use of WMD does not fit the jihadist theory of victory.
7. The phase of war has not yet arrived for which al Qaeda leaders conceive and prepare the use of WMD—in defense of the restored Caliphate.
8. Exploitation of the full lethal potential of WMD requires mastering and combining various skill sets. Although this is not insurmountable, it requires a culture of

Figure 1 Why Has WMD Not Been Used So Far in a Decade of War?

Let me offer a few comments on some of these hypotheses.

If Proposition Number 2 is valid, the leadership of al Qaeda must be hugely frustrated. The attacks of 9/11 were evidently intended in part to inspire young Muslims to take up jihad and attack vulnerable enemies, both near and far, and to act without central direction or support from al Qaeda. So far at least, the degree of innovation has been unimpressive; there have been very few activities by jihadists that are not in the playbooks used in the training programs in the camps in Afghanistan. So far at least, they seem not capable of conceiving, planning, and executing WMD attacks.

“Calibrating the threat offers a contrast to the polar extremes of fear-mongering coming from some segments of the counterterrorism community and the complete complacency that grips other parts of this community.”

Proposition Number 4 in Figure 1 suggests that Osama bin Laden is not interested now in using WMD, but he might be interested later. By this way of thinking, he is not interested now because global jihad is generally taking history in his preferred direction; and he does not need a game-changer now. Indeed, the game-changer might be counter-productive.

Proposition Number 5 definitely has some validity. Recall that Saddam went to war without WMD twice. It may be that al Qaeda made the same choice.

Proposition Number 7 highlights the possibility that al Qaeda leaders are waiting for the next phase of the war to develop their WMD capability and strategy. That phase would come when they succeed in restoring a functioning Islamic Caliphate. Recall what bin Laden said when asked if al Qaeda was pursuing nuclear weapons: “Of course we should want to have them. It is a holy duty to acquire them.” He did not use the word “deterrence,” but the notion reflected in his comment seemed to be that, if the West can do damage to Muslims with these weapons, al Qaeda must have them too to prevent such damage. It may be that this image

of deterrence is associated with the time when the Caliphate has been restored. By this logic, al Qaeda would not use nuclear weapons in the early revolutionary period; it would save them to use as coins of power to shape the presumably hostile environment around the restored Caliphate.

“The most capable of conducting WMD attacks may lack the motivation.”

Proposition Number 8 in Figure 1 raises a key point about innovation. Innovation has proven to be extremely difficult for many types of organizations. Is this also true for terrorist organizations? Such innovation is essential to bringing together the needed expertise and skills to create and employ WMD. Scientists and engineers from laboratories such as the Applied Physics Laboratory well understand the need to nurture a systematic and experimental mindset in the laboratory environment. Experimentation requires a culture in which failure is rewarded because such failure is the shortest route to needed learning. Failure is not highly prized in terrorist movements. Some of the al Qaeda leadership seems to tolerate a fair amount of it but not a lot.

AL QAEDA’S WMD INCENTIVES AND RESTRAINTS

Let me return to my main question: why have terrorists not so far embraced WMD? The preceding discussion suggests that their intentions may not be well formed or their capabilities not well developed. Let me now pose a more specific question: why have the myriad elements in the al Qaeda network not so far embraced WMD? The following graphic (Figure 2) sketches out a way of thinking about this question. It builds on the observation that the al Qaeda network is, in fact, a network of disparate elements, each with its own incentives and restraints.

Node or Group	Characteristics
Jihadists	<ul style="list-style-type: none"> • Most are motivated by a desire to wage jihad, not mass murder. • Untrained jihadists are very unlikely to successfully exploit CBRN. • Trained jihadists know CB training module and see CBW as unproven.
Affiliate Groups	<ul style="list-style-type: none"> • They often have the “interests” of traditional groups—and they compete for legitimacy. • The professionals described below train most.
Professionals	<ul style="list-style-type: none"> • Practice a proven art and weigh alternatives against known means. • Dedicated to the profession, not necessarily the cause. • Show no interest in putting ties to states at risk.
Leaders	<ul style="list-style-type: none"> • Motivated to conduct highly impressive terrorist “spectaculars.” • Seek legitimizing context of fatwas. • Concern themselves with the long-term viability of the movement and thus the interests of their “coalition” members.

Figure 2 WMD Restraint at the Top Versus in the Network

This suggests a couple of important insights. First, the most motivated may lack some of the essential capabilities. Second, to conduct WMD attacks that reap the full lethal potential of WMD, essentially, all of these elements would have to cooperate to a high degree to conceive, plan, prepare, and execute such attacks. There are important barriers to their success in doing so as this chart suggests.

This line of investigation casts doubt on the conventional wisdom that “we know that terrorists are motivated to use WMD.” In fact, we can imagine a range of intentions, from simply exploring the possibility of acquiring or using WMD, through the intention to create such weapons and threaten their use, and up to an intent to reap their full lethal potential. In historical experience, only a relatively few groups have formed the first of these intentions; and far fewer have developed the higher-end ones. This fact is represented in Figure 3. Only Aum Shinrikyo has so far been committed—and evidently not deeply committed because it was not successful in reaping the full lethal potential of WMD. That should be encouraging to us.



Figure 3 “We Know Their Intentions,” Really?

ROGUE STATES AND WMD

What about state actors? Why have not state adversaries so far resorted to the use of WMD in the decades since the end of the Cold War? Especially in U.S. wars of regime removal, why have they not threatened or used such weapons to safeguard the regime’s grip on power?

A variety of opinions has formed in answer to these questions, just as they did in answer to the question about why terrorists have not used WMD. These include the following hypotheses:

1. **Deterrence.** In only two cases was regime survival at risk. In those cases, deterrence worked against political leaders or military decision-makers at various levels.
2. **Preemptive Operations.** In the two Iraq wars, early, decisive operations denied adversaries the operational ability to employ WMD.
3. **Passive Defenses.** Effective passive defenses took adversary cheap CBW shots off the table and left them operational options that would have been catastrophic for their interests.
4. **Conflict Maturity.** The U.S. did not reach the phase of conflict for which state adversaries prepared and deployed WMD.
5. **Low-Key Methods.** Weaker states can beat the U.S. without recourse to highly risky means. Asymmetric conflict against the U.S. involves fighting in ways that do not legitimize the full use of the force available to it. Use of WMD would unleash full U.S. power.
6. **Avoidance of High-Risk Tactics.** Terrorist delivery means may seem appealing but are too risky for leaders who doubt their grip on power.

Obviously, some of these ideas are contradictory. Each seems to have been embraced without a great deal of detailed analysis.

In exploring the possible incentives of non-state actors to acquire and employ WMD, we began with Brian Jenkins' famous characterization of their purposes. What are the analogous purposes of state actors? Especially when they face the possibility of war against a far militarily superior United States, what incentives

and interests shape their strategic choices? In my view, such state actors have a series of strategic priorities in such a circumstance. I summarize these below as a series of imperatives. These are to:

1. **Dissuade.** Dissuade formation of a coalition under U.S. leadership and thereby isolate the U.S. in the hope that this will be militarily or politically crippling to U.S. power projection.
2. **Deter.** If Imperative 1 fails, deter the coalition from taking military action and thereby secure the aggression.
3. **Achieve *fait accompli*.** If Imperative 2 fails, achieve a militarily decisive *fait accompli* prior to outside intervention, reversible only at high cost to the intervening parties.
4. **Cripple.** If Imperative 3 fails, cripple the intervention in its early phases to prevent the coalition from exploiting its full military potential, thus creating a prolonged stalemate and a basis upon which to negotiate an outcome that protects some or all of the aggression's gains—or at least regime survival.
5. **Defeat Conventionally.** If Imperative 4 fails, inflict operational defeat on in-theater coalition forces by conventional means alone.
6. **Survive.** If Imperative 5 fails, prevent a battlefield defeat from becoming a strategic defeat that might include dismemberment of its military, occupation of its country, and/or removal of the aggressor regime—and do so without legitimizing a nuclear reply.
7. **Intimidate.** If the original aggression is reversed, the military is hobbled, the country loses some measure of sovereignty, but the regime escapes

the war intact, the imperative is to prevent a consolidation of regional forces detrimental to its interests.

- 8. **Exact Revenge.** Exact revenge against those who fought against it—whether individuals, groups, or societies. A weak, collapsing regime might be particularly motivated to exact such revenge. (An imperative?)

Obviously, this is a rough sketch and not applicable in every respect vis-à-vis every potential U.S. asymmetric adversary. But it is a useful way to think about how they think about the problems of confrontation with the United States. Where does WMD fit in achieving these objectives?

In service of these imperatives, asymmetric state adversaries of the United States have a somewhat diverse toolkit. These tools are represented across the top of Figure 4. The remaining content of the figure constitutes my best effort to assess, from the state adversary’s perspective, the utility of each of these tools in service of the varied imperatives repeated again down the left-hand side of the figure.

Strategic imperative	<div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px;"> 0 = little to no utility 1 = modest utility 2 = high potential utility </div>				
	conventional	missiles with conventional warheads	nuclear weapons	chemical weapons	biological weapons
dissuade	1	1	?	1	(-/+)*
deter	0	1	?	1	2
achieve fait accompli	1	0	0	2	(-/+)*
cripple	0	0	1	2	2
defeat conventionally	0	0	na	na	na
survive	2	1	2	1	2
intimidate	1	0	1	2	2
revenge	1	1	0	0	2

* function of agent type

Figure 4 Weighting the Tools in the Adversary’s Toolkit

Of course, specific ratings in Figure 4 are arguable. But they do point to some interesting insights. Biological weapons might be highly rated by potential state adversaries because they provide high potential utility across a broad spectrum of imperatives, particularly if nonlethal types could be used early in a conflict. As the question marks indicate, much ambiguity exists about the utility of nuclear weapons for state adversaries.

“We have seen very few activities by jihadists that are not in the playbooks used in the training programs in the camps in Afghanistan. The lack of competency and ability to innovate amongst the rank and file is not what we expected, and it seems that it is not what the leadership of al Qaeda expected.”

ALTERNATIVE HYPOTHESES

So how do we understand the dog that has not so far barked? Recall the opening hypothesis, expressed as current conventional wisdom: “It’s not a matter of if but when.” In light of the preceding discussion, let us consider some alternative hypotheses:

1. Terrorist interest in CBRNE is rising, but how far and how fast are uncertain.
2. Terrorist intentions to exploit the full lethal potential of WMD are not well demonstrated.
3. The intentions of rogue state leaders to threaten or employ WMD are unclear.
4. Although the intent to use WMD may be secret or merely uncertain, we can infer a partial picture of the intentions adversaries might have in a conflict by understanding those conflicts from their perspective.

Are dogs that do not bark permitted in our vision of the future of warfare? Is adversary restraint consistent with the understanding of unrestricted warfare? I found it useful to return to the Chinese godfathers of unrestricted warfare: Qiao Liang and Wang Xiangsui. As they argue in their famous book, “the concept of exceeding limits . . . does not mean that the most extreme means must be selected always and everywhere.” So far at least, U.S. adversaries have not seen it as necessary or possible or wise to select the extreme means of WMD to advance or safeguard their interests in war against the United States. Of course, this cannot disprove the notion that “it’s not a matter of if but when.” What it does is raise a fundamental question about how well we understand our adversaries’ concepts of war against us.

- **“The concept of exceeding limits . . . does not mean that the most extreme means must be selected always and everywhere.”**
- **“The trend is toward unrestricted employment of measures but restricted to the accomplishment of limited objectives.”**
- **“Victory is certainly not in the bag just because a side adheres to the principles [of warfare in an age of globalization], but violating them no doubt leads to defeat.”**
- **On nuclear weapons: “How do we avoid warfare that results in ruin for all?”**

Figure 5 Conan Doyle Meets Qiao Liang and Wang Xiangsui: Is WMD Restraint Inconsistent with the Theory of Unrestricted Warfare?



INTRODUCTION

To develop an effective strategic policy and an understanding of the nature of URW, it is paramount to have a keen awareness of what radical jihadis think and say about weapons of mass destruction (WMD) and how these differ from traditional Islamic beliefs on the use of these weapons. Jihadist statements reveal that their interest and intention levels towards WMD are shifting away from traditional Islamic thought over the past 6 years. These statements cannot be taken at face value, because, obviously, they are not telling us everything they can do with regard to capabilities; but their interest and intent are quite clear and represent a significant threat.

To illustrate the change in jihadist thinking on this issue, let us begin with three statements made by al Qaeda and affiliated groups over the last 5 years about WMD. In November 2001, almost precisely 2 months after the attacks of September 11, bin Laden gave an interview with a Pakistani journalist in which he discussed the current struggle in Afghanistan. His views about WMD came up in the course of this conversation. He said, "I wish to declare that if America used chemical or nuclear weapons against us, that we may retort with chemical or nuclear weapons.

Mary Habeck is an Associate Professor of Strategic Studies in the Paul H. Nitze School of Advanced International Studies at The Johns Hopkins University, where she teaches strategic and military history. Her latest work is Knowing the Enemy—Jihadist Ideology in the War on Terror. She is currently working on a second book entitled Fighting the Enemy.

We have the weapons as a deterrent.” This is a strong statement about possession and about capability, but it is also a statement about intention—to use WMD only if al Qaeda was attacked first. It is important to note that bin Laden apparently viewed WMD as a deterrent and not as a first-strike capability.

In contrast, Ansar al-Islam made a statement in April 2004 that was quite different. “We will strike you with all the weapons available to us,” the statement read, “including conventional, chemical, nuclear and biological weapons. You will see blacker days than the 11th September incidents.” This is a much stronger statement about interest and intentions, “We *will* use these weapons against you;” and conventional weapons are placed on the same level as nuclear, chemical, and biological weapons.

The third statement was made by Abu Hamza al-Muhajir, the leader of al Qaeda in Iraq, last September 2006. In this statement, al-Muhajir gave an open invitation to scientists of chemistry, physics, management, electronics, media, and all other specializations that require depth of knowledge and, particularly, nuclear scientists and explosives engineers. As he put it: “We call on you to tell you that we are in need of you. The battlefield will accommodate your scientific aspirations. The vast areas in the American camps will be the best test site for your unconventional bombs—especially the so-called germ or dirty variety.”

“[Osama bin Laden] said, “I wish to declare that if America used chemical or nuclear weapons against us, that we may retort with chemical or nuclear weapons. We have the weapons as a deterrent.”

This is again, a very strong statement about intentions and interests, but the capabilities are a little shakier. In fact, this last statement suggested that the capabilities were not yet where al Qaeda and affiliated groups would like them to be, but that their interests and intentions have shifted significantly over the past 5 years. This paper will focus on that shift and what has caused it.

We need to begin with where WMD fits into traditional Islamic thinking about warfare and then discuss jihadist beliefs about the legal, religious, and ethical barriers to the use of WMD and what has transpired to allow them to surmount these barriers. What is the historical Islamic thinking about WMD? Muslims have thought deeply about mass destruction over the past 1400 years. Of course, the definition of WMD has shifted considerably in that timeframe. WMD, back when Muhammad was alive, meant a catapult, a weapon that would indiscriminately kill civilians, combatants, and non-combatants alike. It did not discriminate amongst its victims, and it killed large numbers of people—a primitive WMD.

“We call on you to tell you that we are in need of you. The battlefield will accommodate your scientific aspirations. The vast areas in the American camps will be the best test site for your unconventional bombs especially the so-called germ or dirty variety.” —Abu Hamza al-Muhajir

During the time of Muhammad and shortly thereafter, four sorts of prohibitions were developed to limit the use of these kinds of weapons: the need to avoid mass casualties, the indiscriminate deaths of non-combatants, the deaths of Muslims who happened to be living in the town that was bombarded, and burning people alive. When most Muslim scholars looked at these four barriers, they came to the conclusion that they were nearly insurmountable. The prohibitions could be overcome only if certain very stringent conditions were met: the weapons had to be absolutely necessary, and no other sort of weapon could be used in their place. In modern terms, Islamic law created a “last use” vision for WMD. They were not to be employed indiscriminately, and an argument had to be made for them rather than against them.

To show just how high these barriers are, let us take a closer look at three of them: the need to avoid killing non-combatants and Muslims and the prohibition on using fire to burn people alive. The distinction between combatants and non-combatants

is extremely important for understanding Islamic attitudes toward WMD because combatants, whether or not they had a weapon, could be killed; whereas non-combatants were to be left entirely alone. Each one of the four established schools of Islamic law argued very strenuously for making and keeping to this distinction, based on Muhammad's words and deeds. The schools also had arguments about attacking a town where Muslims were being used as human shields. Could you attack the town, or should you hold off lest you accidentally kill a Muslim? About half the schools said, "This is a good reason not to attack the town. If Muslims are going to be killed or endangered by our attack, we should find some other way of dealing with this town other than using the catapult or other weapons that kill indiscriminately."

The other two schools said, "If we do that, we would never carry out jihad because people would learn about this weakness; and they would simply use Muslims as human shields." Yet, even these two schools said that this did not allow the use of indiscriminate weapons when Muslims were present in the town. Finally, burning people alive was strictly forbidden by Islamic law because burning was considered God's punishment. Islamic scholars even raised arguments about trees and the environment, with half the schools saying that it was not only wrong to burn people, it was wrong to burn trees or to destroy the environment during a battle.

This is fairly progressive thinking for 1200 years ago. Thus, the cultural and religious barriers to the use of WMD in early Islamic thought were high and remained at that level right into the 20th century. Most Muslims adopted international law and the standards of international law and argued, in fact, that if Muhammad was there first—he would have seen this as a natural progression—and ideas about WMD as understood by international law fit, in this view, perfectly into Islamic law. It is these barriers that jihadis had to deal with when making an argument for the use of WMD.

The stiff barriers to the use of WMD within the Islamic community explain why, before 2004, there were no serious arguments by jihadis about using WMD. Yet, something happened between 2001 and 2004 that would change this attitude. In 2003,

Nassir bin Hamad al-Fahd, a radical Saudi sheikh, issued a fatwa (a legal ruling) called, *A Treatise on the Legal Status of Using Weapons of Mass Destruction against Infidels*. In it, al-Fahd carefully analyzed the four major objections that Muslims have traditionally raised to the use of WMD (mass casualties; indiscriminate deaths of non-combatants; deaths of Muslims; and horrific ways of dying, including being burned alive), explained away each one in detail, and then provided a general justification for using these weapons.

“. . . first, you should chastise even as you have been chastised; second, you should repay evil with evil; and third, who so commits aggression against you, do you commit aggression against him in like manner.”

Al-Fahd begins with a general statement that there is no obligation when there is inability, and there is no prohibited thing when there is necessity. Those two statements are taken directly from Islamic jurisprudence—a very different section of Islamic jurisprudence than that dealing with WMD or even with warfare in general. But he uses them to make an argument that there is an obligation to use WMD—not just permission but an actual obligation—and their use cannot be prohibited because there is a necessity to do so. Al-Fahd then goes on to refute in detail the four taboos. With respect to mass casualties, he argues that there are three different statements in the hadith [traditions about Muhammad] and in the Qur’an saying that mass casualties are justified in this case. First is a statement that you should chastise even as you have been chastised; second, you should repay evil with evil; and third, who so commits aggression against you, do you commit aggression against him in like manner. Al-Fahd argued that America and its allies have caused massive casualties in the Islamic world for which America should be held responsible. In addition, the Americans have killed men, women, and children without discrimination, so that Muslims have the right now to kill without discrimination as well.

But where have Americans been massively killing Muslims indiscriminately? Al-Fahd referred specifically to the sanctions against Iraq imposed after the first Gulf War. According to his reasoning, the U.S. purposely killed Iraqi men, women, and children through these sanctions—indeed, the sanctions were designed to kill Muslims. Not only that, but the U.S. also invaded Somalia solely to inflict massive casualties on Muslims. During the nineties, the U.S. then armed, trained, and helped the Serbs to kill Muslims in Bosnia and elsewhere. It was only when the U.S. was exposed that America pretended to back away and do something about the casualties that were taking place. One might have some disagreement with these three propositions and others that al-Fahd brings up, but they are arguments that resonate in the Islamic world and especially resonate with jihadis, who believe them wholesale.

How then does Al-Fahd get past the prohibition on indiscriminate deaths, especially of non-combatants—women, children, old people, monks and so on? He brings out what might be termed “the catapult defense,” which is used by all jihadis when talking about this issue. He also raises the idea of attacking the infidels at night. There are some hadith that tell about Muhammad using a catapult against a city, a weapon that, like WMD, kills indiscriminately. Another hadith reports that in a raid carried out at night, Muhammad accidentally and unintentionally killed non-combatants—women and children. Using analogy, al-Fahd argues that therefore it is permissible to attack the infidels with weapons that do not discriminate between combatants and non-combatants and at a time or place when one cannot distinguish between combatants and non-combatants. It is important to notice that both of the cases raised by al-Fahd have to do with unintentional collateral damage. But al-Fahd argued that collateral damage is not just reluctantly permitted but is, in fact, desirable, which is a seismic shift from traditional Muslim tenets.

In his refutation of the ban on the death of Muslims, al-Fahd cleverly turns the argument into one about intentions rather than results. Recall the human shield argument that was earlier

used by the two schools of Islamic law: if we give up on jihad because Muslims are being used as human shields, we will have to give up on jihad entirely. Al-Fahd said that this was actually about intentions: we do not mean to kill Muslims, and they were purposely being used against us as human shields. Thus, our lack of intention to kill them, as well as the bad intentions of our enemies, allows us to carry out massive attacks using WMD that will kill Muslims.

Finally, what about burning the enemy's land, the destruction of the environment, and killing people through burning? Again, a hadith that talks about Muhammad saying nothing against the burning of fruit trees during a siege is used as an argument to justify killing people through burning. Even someone who has had no exposure to Islamic law would say that this is a very bad argument. But immediately after Al-Fahd's treatise appeared in 2003, every single one of these arguments was adopted by jihadis in multiple groups to explain why the use of WMD was allowed.

In all of their writing, there is the repeated appearance of the catapult defense, of the burning of the land defense, of the human shield defense. The result has been a movement away from the use of WMD as a deterrent—if they are used against us, we will use them against the enemy—to their use as soon as jihadis have the capability. From a close analysis of jihadist statements it is possible to say that intentions have shifted, and interest has shifted; but capabilities may not have changed at all.



Q: *Prof. Thomas Keaney – The first question is for our first speaker, Michael O’Hanlon. “Originally, Iraq was denied as a safe haven, and the rationale for invading Iraq was claimed to have been to prevent the use of weapons of mass destruction. An important secondary effect has been that we have kept the fight over there. Please assess the strategic validity of this assertion. And if you disagree, please assess why we may not have been attacked on the U.S. mainland since 9/11.”*

Dr. Michael O’Hanlon – Thanks for the question. My overall assessment would be that the Iraq War was undertaken for a sound strategic rationale to reduce Saddam’s potential future threat to the region, for a traditional strategic state-on-state sort of reason. It has nonetheless increased the threat of terrorists. We can debate that, if you wish, but I think, on balance, it has provided a huge rallying cry for the Islamic world. Mary talked about the sanctions, and I would concede that was an important argument in favor of considering the invasion in the first place—the previous policy wasn’t as good as war opponents seem to want to nostalgically remember today. Nonetheless, I think there was a potential strategic benefit—to getting Saddam and potentially his sons out of power. But there was a net increase in terrorism as a result because of what the war has meant in the broader Islamic world. One additional point complicating it even further is that, given where we are, I think to withdraw would probably make things even worse on the terrorism front. So, the terrorism argument, in other words, is not a good justification for why we went in in the first place; and on balance, the war has made things worse. But they could get even worse if we were to be seen as having been defeated in Iraq by al Qaeda.

Q: *Prof. Thomas Keaney – Specifically, does the threat to the homeland extend beyond weapons of mass destruction—that is, information warfare? Have you done anything specific on that?*

Dr. Michael O’Hanlon – I don’t know that I have any huge insight to offer on that. What we see from al Qaeda, as Brad pointed out, is that they have gone back to some of the traditional playbook. I would worry about WMD because of the potential for devastation and because there is debate within the Islamic world and among the jihadists about whether it’s legitimate as a tool. But I would still, day to day, worry most about airplanes, truck bombs, and other such traditional uses of explosive or tactics that al Qaeda’s been employing for years now.

Q: *Prof. Thomas Keaney – Here’s a specific question for Brad Roberts. It’s about what Mary talked about and you captured in terms of intentions and capabilities. “Why haven’t the jihadists attacked us?” Mary’s point is that starting around 2003/2004, there was a change, which explains the lack of data you mentioned earlier. Did you see the same change around the same time that could affect the intentions and capabilities?*

Dr. Brad Roberts – That’s a great question. That would be the striking contrast between our two presentations. Listening to Mary and reading her work, I’m reminded of General Cartwright’s proposition about how different the adversaries are and the world we’re moving into. They are not organized, they are not hierarchical—although they have organized and have hierarchical attributes. But since this particularly important fatwa was issued, we’ve seen bombs under chlorine canisters; and undoubtedly, there are other development activities going on. We have a gauge from Afghanistan in terms of understanding how al Qaeda leadership takes responsibility for certain high-priority activities—it creates compartmented R&D, black programs, funds them lushly, and sends those people off to go to work.

Yet, their bio program had those attributes; and they had a response to a posting on the web to come and bring us your expertise—we need you. All of that happened, and yet no capability resulted even after some time. In contrast, Saddam

made the decision for bio and went from beginning to a deployed capability in 3 years and had a development activity under way that would've brought a lot more. This adversary doesn't make that kind of top-down decision to put the pieces in place, make it go happen. It counts on jihadi fervor to make these moral legitimizing statements become operationally real somehow. General Cartwright rightly emphasized the rapid decision-making loop of these new adversaries, but their operational loop of going from an ambition in one part of the network to knitting together all of the pieces to implement it—and not just in ones and twos but in a campaign of attacks—that is a capacity they don't seem to have or at least have not so far developed.

Q: *Prof. Thomas Keaney – I've got several questions from the audience. Let me take one out of order because it applies to just this issue, and it is also for Mary Habeck. "It seems that Islamic culture is more adaptable to unrestricted warfare as evidenced by its willingness to reverse the previously held beliefs. Western culture, on the other hand, has carefully restricted the use of violence and created legal, moral, and cultural barriers to unrestricted warfare that seem insurmountable. Can western civilization adapt rapidly enough to survive the unrestricted attacks we may face? Can we overturn our beliefs and laws as rapidly as this fatwa did?"*

Dr. Michael O'Hanlon – I guess I should've been clearer at the beginning that what I'm talking about here is a very small percentage of the Islamic world. I think that the reason—besides capabilities—there has been no use of WMD so far is an uncertainty about how the rest of the Islamic world would react to such an attack. I don't make any argument at all that the jihadis are representative of the Islamic community; and in fact, many different clerics have issued fatwas saying that WMD are not Islamic, are not something that should be used, or are just for anybody to create and use. I didn't talk about that because the focus here is obviously on the jihadis, but there are still huge barriers for these guys to overcome within the Islamic world itself. Even though I think that some portion of the jihadi community believes that WMD are perfectly fine, and that portion is associated with what is generally called the Salafia Jihadia, that

is, the Wahabi-influenced Jihadis. They're the ones who are most likely to have these intentions to use WMD and have the interest in using WMD. Even within the jihadist community, it's not as if all of them have put out statements saying: WMD are fine, and we believe in using them. Unfortunately, al Qaeda and affiliated groups are members of this Salafia Jihadia and follow along in its ideological footsteps. This particular sheikh Nasir bin Hamad Al-Fahd is well respected by al Qaeda's leadership and is seen as somebody whose thoughts should be followed. So, I'm really not making an argument about the greater Islamic community and where it is on this issue.

Q: *Prof. Thomas Keaney – Mary, the next question asks you to extend that just a bit. “How worried should we be about Muslim attempts here in the United States to not assimilate with the infidels in American culture—that is taxi drivers refusing service to passengers carrying alcohol, et cetera. How far should we allow the envelope to be pushed?”*

Prof. Mary Habeck – One of the arguments that I generally make about why we've had no attacks in the United States is that Muslims in our country are pretty well assimilated and are generally on the far liberal moderate mainstream edge of the Islamic world. In other words, they're the farthest away from the Wahabi Salafia Jihadia. They're not the kind of people who accept this sort of thing at all. So, I don't actually see that there's a huge problem with lack of assimilation in this country and certainly not on the scale that you have in places like France or Britain. You also don't have the secondary issue that has developed in Britain, where 10 to 20 of the top jihadist preachers in the world were allowed into the country and welcomed for about 15 years; and they spent the entire time building up a following of several thousand people. There are several reasons we've been protected from attacks here. It may have to do with capability; but mostly, it's because of lack of desire. Muslims here see themselves as Americans.

Q: *Prof. Thomas Keaney – For this question, let me start with Brad since he's addressed several of these aspects and then continue with Michael. “Based on the whole term ‘weapons of mass destruction,’*

we neatly categorize a number of things—chemical, biological, nuclear weapons, delivery vehicles—which are clearly not the same.” I’ll first ask Brad to parse those into what we should really be worried about: chemical, biological, and nuclear in different issues or different situations. And specifically for Michael, when he talked about the Asia Pacific region, “Should we consider that some of these weapons—for example, chemical weapons—may be used more routinely and not in the sort of catastrophic way that we sometimes think they would be?”

—Dr. Brad Roberts – N versus B versus C, as most of you know. Most of you have the view that C doesn’t really count much. Chemical weapons aren’t really weapons of mass destruction; and that’s pretty much true against a large conventional force with very strong passive defense capabilities. But these are weapons that can be used readily, particularly in closed environments, and delivered by aerosol from very simple delivery devices, including Cessnas, to create large effects on unprotected populations. So, I think we do ourselves a disservice to write off the CW piece. On nuclear, I’m not sure what to add to our understanding of that—we’ve all done a lot of thinking about that.

The bio piece is one where I think people have a hard time calibrating how big a deal it is. The expert community is roughly divided into two camps that don’t at all agree. Either it’s a really big deal, and the sky’s going to fall; or it’s been hyped for so long, and it hasn’t happened so there’s nothing to this threat. As my slides suggested, biological weapons are particularly appealing to states facing the necessity of an asymmetric conflict against the United States in which they don’t want to use nuclear weapons. Using a nuclear weapon against the U.S. in a military conflict is a pretty stupid thing to do. An enemy using a nonlethal bio weapon to create a potential fait accompli while we’re engaged in some main military operation could be potentially highly crippling to our activities, as would the use of lethal bio. I want to come back to a point about the fatwa on WMD, which is that it established a number. It’s morally legitimate to kill—was it 4.2?

—Prof. Mary Habeck – Ten million.

—**Dr. Brad Roberts** – Ten million. Ten million. This is germane not to an al Qaeda calculation of the use of chemical weapons, and, frankly, not to an al Qaeda calculation of the use of nuclear weapons. Killing 10 million people with crude fission-style improvised nuclear devices is hard if you're building them in a cave somewhere. Bio is probably the way to go for 10 million—and let me be crude about this: If you're familiar with the CSIS [Center for Strategic and International Studies] Dark Winter scenarios, I find 10 million reassuring. Bio with a crude pathogenic—smallpox, for example—could kill in the multiple tens of millions. This is the distinction between weapons of mass destruction and the full lethal potential of a weapon of mass destruction. If there's a moral barrier between killing 10 million and 50 million or 100 million, I'm happy to celebrate its existence even if it is deeply troubling on its own.

Q: *Prof. Thomas Keaney – Briefly, Mary and then Michael.*

—**Prof. Mary Habeck** – The 10 million figure is based on his calculation of how many Muslims have been killed by Americans in the last 40 years. But, he says, if you need to kill more than 10 million, just come back for another fatwa.

Q: *Prof. Thomas Keaney – Michael, the conventional use of these weapons.*

—**Dr. Michael O'Hanlon** – I'm just going to throw out one scenario. I've already apologized to any Russians and Chinese in the crowd, and I'm going to apologize to Japanese. There are a lot of ways in which WMD could plausibly be threatened or used in Asia Pacific theaters; but, for the sake of simplicity, I'm just going to mention two that I think are not out of the question, and they both potentially involve nuclear weapons. To some extent, the unifying theme here is the dislike of many in the region for the Japanese and perhaps the willingness to think of American bases in Japan as a legitimate military target. You combine all that together, and I could see ways in which the North Koreans, while they might not want to use nuclear weapons against South Korea, and they might not be able to use them against the American homeland or see the

value of engaging us, might say, in the context of an ongoing war: “Why not hit the Japanese?” The South Koreans might not even mind that much. The North Koreans might convince themselves of this logic. Then, they may also say: “The Americans need military bases there enough that if we hit some of those bases, we’ll kill a few hundred Americans, but that’s a legitimate number in a time of war. And if we kill a million Japanese who live next to that base, we can put up with that because we have this historical animosity, and they’ve killed so many of us.” The proportionality argument of the type that Mary was just mentioning regarding the western world and Muslims could come into play there in terms of how the North Koreans or for that matter, the Chinese, think about retribution against Japan.

Moving now to China, in a Taiwan Strait scenario, let’s say we get to the point where the United States has decided to sink the Chinese submarine fleet as comprehensively as we can because we’ve decided that’s the main threat to Taiwan’s economy. If the Chinese really want to go air-to-air with us, we can always escalate or match them as needed. But the submarine threat is one we want to eliminate at a certain point in this conflict. Then, the Chinese could say: “At this point in the conventional competition, we’re out of luck; but what about a nuclear weapon against facilities in Okinawa, for example, or for that matter, Yokosuka?” All of a sudden, there could be an escalation of that type, where they argue that it’s against a military target. Of course, the people they’re killing are Japanese with whom they have a historical animosity and owe payback. I would worry about a North Korean or a Chinese mind constructing that sort of an argument. That’s one very particular answer to your question, Tom.

Q: *Prof. Thomas Keaney – A quick one for Brad. “What do you make of the chemical weapons, the chlorine gas that is being used in Iraq? Do you see that as some sort of opening of the door? Is it something to be really concerned about?”*

Dr. Brad Roberts – It reinforces the experience the terrorists had in their first forays in this area; they crossed what we thought was a significant threshold, and they haven’t gotten much for it. There’s the more famous case of the LTTE [Liberation Tigers of

Tamil Eelam] in Sri Lanka using chlorine gas to attack a military base in 1991 or '92. They never used it again. It didn't work very well for them, and they had other techniques that have worked better. It seems to me that these attacks have not succeeded in inflicting significantly different numbers of casualties or inducing any other reaction from the targeted society than they were already getting.

Q: *Prof. Thomas Keaney – A question for Brad or Mary on biological weapons or biological issues: “What’s the likelihood that the recent pet food problem may be a testing or training exercise for a chemical or a biological attack factor?”*

Dr. Brad Roberts – I've been in the U.K. for the last 10 days, and my *USA Today* this morning said, “Pet Food Scare,” and that's all I know about the subject. May I make a footnote comment? If you're trying to understand the bio threat, I recommend a piece on the web by Seth Carus at National Defense University, entitled *Bioterrorism and Biocrimes*¹. He's at the Center for the Study of WMD, and he set out 10 years ago to compile a list of all of the incidents in the 20th century in which a biologic agent was used for some illicit purpose. He issued a first edition in 1996 and then got a whole bunch of phone calls telling him, “You missed this, you missed that, you never heard...” Now, there are five editions; there's a sixth coming out; and the list is long. What's striking is that criminals have been much more interested in the use of biologic materials for extortion than have terrorists, and assassins have been much more interested in the use of these materials than state structures. This is a very striking pattern drawn from a very large dataset. I'm completely ignorant about the pet food business; but if there's any tampering involved here, it's not consistent with our expectations about the terrorists' level of interest in this.

Q: *Here's a question that really takes us in a new direction, open to anyone who wants to address it. “Michael O'Hanlon focused on traditional strategic warfare options—diplomatic, economic, and military. Dr. Roberts focused on weapons of mass destruction. Why aren't we talking*

1 W. Seth Carus, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*, National Defense University, Center for Counterproliferation Research, Fedonia Books, 2002.

about the elephant in the tent—strategic communications? In the current war, our enemies are exploiting our political and cultural differences to defeat us.” Strategic communications seem to pair with another question: “Do we place the burden of responsibility on the press and the infotainment focus business that exploits the relatively small numbers of Islamic trash or fails to report on Muslims that are devoted to pluralistic democracy, as those are who are culturally western. In other words, what about strategic communications—are strategic communications exploiting both what the Islamics are doing and what they are trying to do to us?”

☰ Dr. Michael O’Hanlon – Big topic. I’ll just say a word and pass the baton. There’s a very good paper being done at Brookings that is going to be on a new website we’re creating called Opportunity08.org, focused on the presidential race. Peter Singer and a colleague in the Brookings Doha Qatar Office have recently proposed a strategic communications strategy. I was very frustrated that the 2004 presidential race didn’t address this issue. George Bush, to be fair, had a part of it. Democracy promotion was intended to be part of the answer; unfortunately, it hasn’t had a very good 3 years since then. But it was still an attempt to engage this question of the long-term threat, the strategic communications threat, although maybe not in quite the way the questioner meant.

This is a huge topic and can be interpreted in many different ways. I’ll finish with an anecdote. I was lucky enough to see Senator Bill Bradley last week at a conference, and I asked him, “How much do you regret not having been President on 9/11 or after 9/11?” He gave an extremely eloquent answer about all the different things that might’ve been done. One of them was to convene a meeting of western and Islamic religious leaders and ask them for advice about conveying to Muslim and western secular political leaders what steps might be taken to try to bridge some of these divides. We’ve been taking some smaller steps, such as increasing the number of American centers around the world, putting more money into broadcasting, etc. But I think we have to be even more creative and find ways to actually get Islamic and western communications going.

I was just at a conference that Brookings Sabon Center does every year, which tries to do a little bit of what Bradley was talking about and ask people to criticize one another. At the end, it tries to find a more constructive set of messages about how we can exchange our different views on history, try to share the better side of one another's cultures, make sure some of the ignorance is broken down, and find new tools—Internet and other tools—for spreading information about one another's cultures. As Mary said, "So many American Muslims are such wonderful people who are so involved in our society, and it's really something we should be celebrating even more and underscoring that our society is a melting pot that's intended to respect diversity."

I just hope that, in this next presidential race, we see both sides willing to engage this question of how to prevent the second-generation al Qaeda from forming—to answer the old Rumsfeld challenge—instead of just focusing on the more narrow, immediate problem of what to do in Iraq.

 **Dr. Brad Roberts** – I, too, would like to weigh in. People use the word strategic communications, and I think everybody has a different elephant in mind. What's so obvious to one isn't so obvious to another. I find it useful to think of two elephants: the external elephant and the internal elephant. The external elephant is the external audience to which the U.S. communicates, and we are hyper worried about the messages sent there, in part, because of the tradition in our own culture of the central role that strategic communications played in deterrence in the Cold War.

I think we vastly overestimate our ability to get the right messages out to external audiences to induce the behaviors we desire. The basic punch line there is like the Hippocratic Oath: First, do no harm and don't expect to do much better. That would be doing a lot. The internal elephant hardly features in our discussion of strategic communications. Al Qaeda's very clear about the importance of our public will.

I believe there are many more opportunities for the national leadership to excel at the business of strategic communications to the American public. If al Qaeda perceives that it can break our

will by getting us to disagree about how to prosecute a long war here, we will have played right into its hands. We won't create long-term will by doing what one of the questioners implied earlier, which is moving away from moral constraint as we understand it. We have to see our actions as just in our own traditions. This is much more important than that the Arabs see our actions as just in their traditions. Very little work has been done in laying this foundation for continued consensus.

 Prof. Mary Habeck – I'd just like to make three quick points. First of all, this is an issue I've been thinking about a lot for the last 6 years; and in 2004, I actually applied for a job in the NSC. It was creating a new position on ideological warfare. It hired somebody else for the job, but I had a conversation at that time with Elliot Abrams and asked him, "Why wasn't this done earlier?" He said, "We attempted to do it but ran into all sorts of issues with both DoD and State, and nobody could decide what in the world they were trying to do." Since then, as we know, there have been positions created at both of these institutions to deal with this issue. The problem I see is that there've been multiple positions created, and nobody's talking to each other. Everybody has their own in-house IO, and it's as if they're reinventing the wheel. "Look, here's fire. Oh, they have fire, too—didn't even know this." It's all over the place and nobody even knows what's being done. That's the real problem. Everybody says: "We need to do something about it." But there are actually other people doing it. That's the first point.

The second point is that we face a huge barrier to dealing with this issue that nobody is confronting head on: How do we deal with religion? How do we deal with religion as non-Muslims? How do we communicate with people who do not come from our religious tradition? The analogy that I like to use is: I believe that the Islamic world is involved in its own reformation. We forget that the European reformation began with 150 to 200 years of bloodshed; and it was only after everybody got sick and tired of killing one another that they sat down and talked and came up with the enlightenment. So, what we're dealing with here is maybe 150 to 200 years of bloodshed, and it's really mostly about

an internal dynamic about authenticity: What is real Islam going to look like? What do we have to say about that? We'd be like the Ottoman Sultan coming to the Pope and saying, "What can I do about your Luther problem?" How much help would that be to the Pope? This is a huge issue, and I don't see anybody dealing with it in any really sophisticated way. We shy away from it. This is why I think we have a strategic communications problem at base. And, if that's true, we really need to find partners within the Islamic world to do the talking for us. But who are our partners? We don't have a real touch and feel to understand peoples' position within their own society.

Let me give you the problem from al Qaeda's perspective. It has a huge communications problem as well. It has had all sorts of stumbles all along the way; we should be encouraged that we're not the only ones who are having this problem. It had two problems. First, bin Laden decided to put out a major statement to influence the 2004 elections. He said, "Anyone who votes for Kerry will not be attacked. Any state that votes for Kerry will not be attacked." We saw how successful that was in getting people to vote for Kerry. As a strategic communications attempt, it was an abysmal failure. Not as bad, by the way, as the [UK] *Guardian's* attempt to influence the election in Ohio.

"The problem I see is that there've been multiple positions created and nobody's talking to each other. Everybody has their own in-house IO, and it's as if they're reinventing the wheel. "Look, here's fire. Oh, they have fire, too—didn't even know this." It's all over the place, and nobody even knows what's being done."

As for their second problem, the American advisor who is giving them the inside story on what Americans are like and how to reach out to them is a goat herder from southern California. How representative is he of general American opinion, and how well has he done in helping them influence events? I often think our partners [in Iraq] might be the equivalent of goat herders from

southern California, but we say they must know more than we do because they're real Iraqis; they're genuine Yemenis.

Q: *Prof. Thomas Keaney – Staying on the issue of strategic communications: “The discussion is focused on nuclear, biological, or chemical. Do you think that jihadists have the capability to attack our critical infrastructure through cyber warfare, or is this too sophisticated for them?”*

▬ **Prof. Thomas Keaney** – I’m not that worried because our cyber systems are constantly under attack by hackers. I think American and Chinese hackers are probably going to be better than jihadist deliberate saboteurs.

▬ **Prof. Mary Habeck** – I would say this is probably where they have the highest capabilities because they actually spend a lot of time on the Internet doing pretty sophisticated things with it.

Q: *Prof. Thomas Keaney – Here’s a question to everyone: “Are we focusing too specifically on terrorists as non-state actors using unrestricted warfare tactics? What’s the plausibility it’s being directed by nation states? For instance, Hezbollah led the response following the U.S.-led strike into Iran.”*

▬ **Dr. Michael O’Hanlon** – If we were fighting Iran, I certainly would worry about how well it would use Hezbollah. You’d have to assume that they would both be all-out agents of reprisal. In fact, this eventuality is fairly well appreciated within the government, which is partly why people are so anti-Iran; and also why they’re wary about launching a strike—it cuts both ways. I think you’d have to assume Hezbollah would fully support this kind of operation.

Q: *Prof. Thomas Keaney – Another question: “Why are Islamic extremists attacking the U.S.? Are there root causes we can engage versus attacking symptoms? Some of those causes might be economic, cultural, Israel presence, etc. Why are they attacking us?”*

▬ **Prof. Mary Habeck** – That’s an entire book. I wrote my first book to explain why those attacks were carried out. The original

title for it was *Why They Did It*². But it's on a very different level than what somebody like Mark Sageman is talking about. There are levels of motivation. At the very top level are the people who are creating the dream that attracts Muslims. That's what the book was about—the dream they're trying to attract Muslims to and their ideas about what they'd like to do. At the bottom, you have ordinary Muslims who might find this attractive. Why they find it attractive and end up becoming radicalized is a completely different question, and something that Mark Sageman deals with. So, there are actually levels and layers of motivation here that have to be addressed. At the top level, you're dealing with people who are like the Bolsheviks: you're not going to convince Lenin that capitalism is a good idea. I don't know what we can do with those people other than kill or capture them. For the other 99.99% of the Islamic world, there are all sorts of things we could be doing to make those ideas less attractive and to create a better environment in their societies that will keep them from being attracted to these ideas. Economic issues, political issues—those are what need to be addressed.

Q: *Prof. Thomas Keaney – A specific question for Michael: “The National Intelligence Council’s 2020 vision³ described scenarios for alternative futures: Pax Americana, Davos World, etc. How would you apply those to your look at the various plausible future scenarios? You were talking about plausibility, not necessarily likelihood. How do you match one with the other?”*

Dr. Michael O’Hanlon – If I understand the question correctly, I’m glad that you summarized with those two scenarios because those are the two that have to be increasingly merged over time. In other words, there is no basis for international stability now absent a strong United States, and that’s going to be true for the foreseeable future. But it’s also probably not totally sustainable because of what Mary was talking about—we’re the focus of

2 Mary R. Habeck, *Knowing the Enemy: Jihadist Ideology and the War on Terror*, Yale University Press, New Haven, 2006, “Why They Did It,” Chapter 1: http://yalepress.yale.edu/yupbooks/excerpts/habeck_knowing.pdf

3 “Mapping the Global Future: Report of the National Intelligence Council’s 2020 Project,” NIC 2004-13, December 2004, http://www.dni.gov/nic/NIC_globaltrend2020.html

hatred and of many peoples' desire to challenge us and the whole system. In addition, Americans don't have the desire to bear the whole burden, and we don't necessarily do very well in every scenario.

So we've got to evolve—maybe not towards a complete Davos World, which is a little utopian—but towards a more multilateral world, where some of our allies play a little greater role and where we increasingly integrate India and hopefully China into this system. The United States has to retain hegemony at some level but not a classic hegemony—there has to be increasingly more power sharing. There has to be a vision. The real issue is how do you get there? I'll leave that for the next panel.

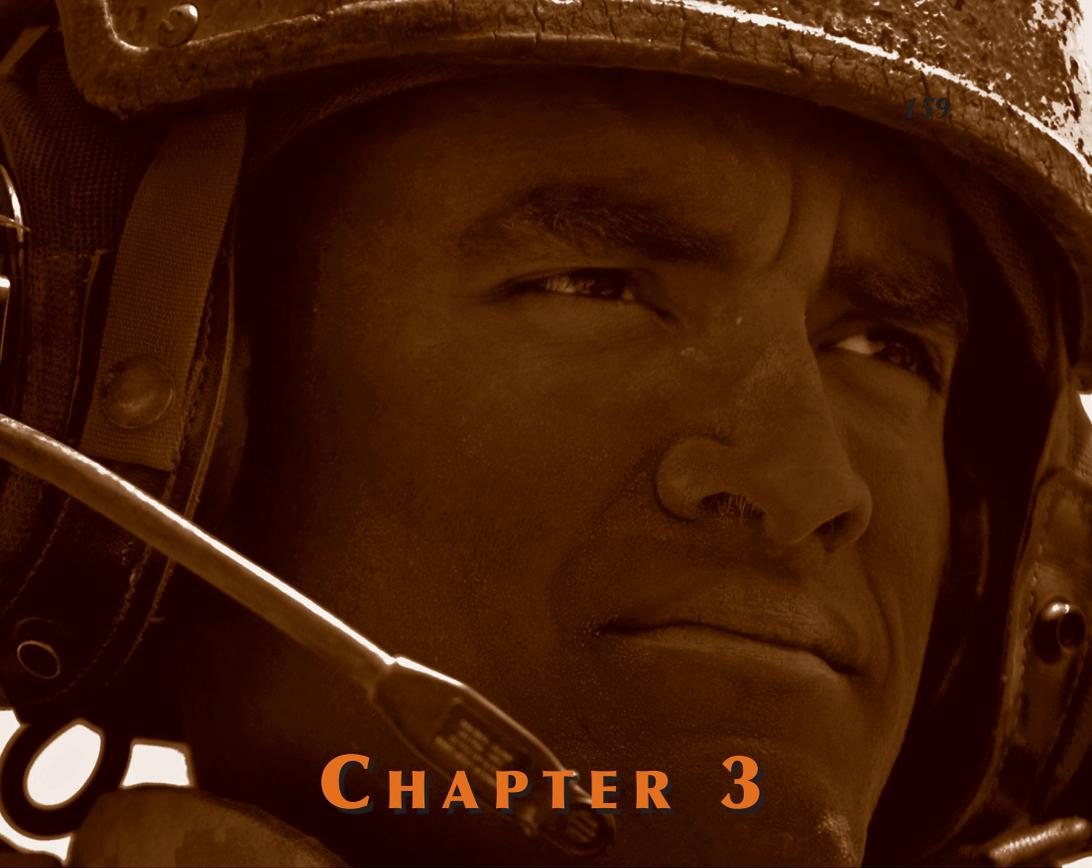
Q: *Prof. Thomas Keaney – Let me pose a couple of quick final questions. First, for Mary: "How do you explain the constant murderous Sunni–Shiite split in view of the Islamic barrier to killing?"*

Prof. Mary Habeck – Throughout the 1400 years of Islamic history, the Sunni–Shia split has been absolutely fundamental to Islam. It began right at the foundation of Islam and is built in. It stems from a political question of who is going to succeed Mohammed as the leader of the community. The result was that the Shia were an oppressed minority for most of their existence; and the Sunnis were the oppressing majority for most of their existence, which is certainly true in Iraq. The view that each has of the other, though, is quite different. Sunnis generally believe that the Shia are at least sinners and heretics if not outright unbelievers and apostates. The Shia believe that the Sunnis are wrong—fundamentally wrong—but they're not heretics. In other words, the way that Iran reaches out to the rest of the Sunni world shows that a fundamentalist—or what would be called Salafi Shia—vision of Islam includes the rest of the Islamic community. But the way that the Wahabis view the Shia is that Islam includes us, and the Shia are all dead or converted. This fundamental asymmetry explains why the Sunnis have no trouble killing Shia, but the Shia were only provoked into killing the Sunni after years of death.

Also in Iraq, the majority of the Sunnis believe that Iraq is a majority Sunni country, that the Shia are a minority; and anyway,

they're all Persians. They also have a saying in Iraqi Arabic—it rhymes—which is: “To us the government, and to you self-flagellation.” This explains their vision of our proper places in the universe and also the disdain they have for the Shia in general, which allowed them to permit the kind of killing that’s gone on there.

Q: Prof. Thomas Keaney – We're out of time, but some of the remaining questions address very good strategic issues. For instance: "Is the United States ready to engage in nuclear warfare over the Taiwan issue?" Or more particular issues: "Is the U.S. ready to lose a war? Is the U.S. ready to lose a war based on perhaps the use of these weapons?" We can't answer very many of these, but I think they should be addressed. In contrast to what we did last year, the objective of this panel was to address much more of the strategic issues. If you recall, last year, a good bit of the first day was spent talking about improvised explosive devices.



CHAPTER 3

**STRATEGIC
POLICY
ROUNDTABLE**

**TAILORED
DETERRENCE:
WHAT WILL IT
LOOK LIKE?**



3.1 TAILORED DETERRENCE: WHAT WILL IT LOOK LIKE?

Thomas M. McNamara, Jr.

INTRODUCTION

Throughout the conference, we have heard the word deterrence mentioned consistently. Earlier today, Professor Hoffman spoke of the importance of knowing the enemy and the importance of strategic communications. Those two concepts play an integral role in developing tailored deterrence, our topic for this session.

By way of introduction, I would like to highlight several salient events related to deterrence (Figure 1). Taking a look at the Cold War, the records show that our deterrence posture was not established quickly but rather took many years of refinement to move into a deterrence state that seemed to achieve deterrence stability with the former Soviet Union. Obviously, today, the world is very different. It has been just 6 years since the introduction of the New Triad of 2001, and even less time has passed since the new U.S. Strategic Command (USSTRATCOM) was established

Mr. Thomas M. McNamara, Jr. is the National Security Capabilities Program Area Manager in the National Security Analysis Department of JHU/APL. His focus is on assessing DoD capabilities for emerging national security challenges and strategic balance and integration of joint defense capabilities. Previously, he has served as the principal point-of-contact for United States Strategic Command and the David Taylor Naval Ship R&D Center. He has considerable expertise in undersea warfare, autonomous unmanned vehicles and systems, advanced R&D, DoD acquisition, systems engineering, and command and control. Mr. McNamara has served on a variety of technical panels, published technical papers, and presented at numerous symposia and technical meetings.

and given “previously unassigned” missions. More recently, the latest Quadrennial Defense Review (QDR) introduced a new concept of deterrence: tailored deterrence. So, in the context of history, it is fair to say that we are in the very early days of looking at this new concept . . . this new way of trying to deter our future adversaries. The following primer describes a historical view of deterrence with state and non-state actors:

HISTORICAL PERSPECTIVE ON DETERRENCE

As you read this section, please keep in mind our National Military Strategy of assure, dissuade, deter, defend, defeat. Note that deterrence is the centerpiece of the group. Getting deterrence right will keep us out of the defend or defeat phase of military action.

Deterrence Background:

- 1960s – 1990s: Deterrence chiefly achieved by balance of nuclear threat between USSR and USA.
- 2001: Nuclear Posture Review introduced the “New Triad.”
- 2003: U.S. Strategic Command was assigned “previously unassigned” missions associated with the New Triad and emerging non-nuclear strategic operations.
- 2006: Quadrennial Defense Review introduced concept of tailored deterrence.
- 2007: Assure, Dissuade, Deter, Defend, Defeat

Therefore, it is important that we put our best minds and best efforts toward achieving success in deterrence. Our speakers today are evidence that we are doing just that.

Colonel Lutes from the National Defense University will open this session and is presenting a brief overview of the theory behind tailored deterrence. Dr. Castillo will follow with a discussion of DoD’s policy implementation of that theory. Finally, Mr. Parker will share his insights on the operational implementation of tailored deterrence policy at USSTRATCOM.



3.2 CAN DETERRENCE BE TAILORED?

Charles Lutes

INTRODUCTION

This presentation is taken from a paper by my colleague, Elaine Bunn, which was the result of a number of conversations on the concept of tailored deterrence. As the security environment has changed, we have had to change our approaches to meet new threats. The 2006 QDR alluded to this shift. In fact, even during the 1990s, when a lot of the department was trying to envision the post-Cold War environment, deterrence thinking was still back in the Cold War. We've got to put deterrence thinking into a 21st century model (Figure 1).

Cold War Model...	21st Century Model ...
<ul style="list-style-type: none"> • Single-focused threat • Nation-state focus • Deterrence by threat of punishment • Responding after a crisis (reactive) • Deterring use of nuclear weapons 	<ul style="list-style-type: none"> • Multiple, complex challenges • Focus on rogue powers, terrorist networks, and near-term competitors • Deterrence by punishment and denial • Preventive actions so problems do not become crises (proactive) • Deterring use and dissuading acquisition of nuclear, biological, and chemical weapons
<p>Principle of Deterrence <i>Ensure costs of action are greater than the benefits of action, while taking into account the consequences of restraint.</i></p>	

Figure 1 The Evolution of American Thinking About Deterrence

Colonel Charles Lutes is a senior military fellow at National Defense University, working in the future strategic concepts area. His focus includes, among others, global terrorism, weapons of mass destruction, proliferation, and interagency coordination. He has been a National Security Fellow at the John F. Kennedy School of Government at Harvard. He is currently working on a PhD.

DETERRENCE IN A COMPLEX WORLD

It is a more complex world out there, and there are a number of actors—both state and non-state actors. During the Cold War, deterrence was primarily by the threat of punishment—more specifically, the threat of nuclear punishment. Now, we have to consider not only deterrence by punishment but also deterrence by denial so that the adversary will think twice about conducting certain actions. There is a more preventive tenor to the QDR in 2005; and we are moving away from deterring the use of nuclear weapons to deterring and dissuading the acquisition of WMD, plus other aggressive acts.

It is clear that deterrence has a role in the 21st century model. In fact, the strategic deterrence joint operating concept recognizes that the basic principle of deterrence doesn't change: We have to ensure that the costs of action are greater than the benefits of action, while taking into account that the consequences of restraint may not be acceptable for our adversaries. In other words, if an adversary risks losing a capability or being unable to act if he waits, he might go ahead and use the capability even if he might not necessarily gain a benefit by doing so.

The concept of tailored deterrence was first offered in the 2006 QDR but without a real definition. Ever since, we have been trying to understand it. I will first discuss the terms deterrence and dissuasion. These terms are not synonymous. Deterrence is focused on convincing an adversary to not undertake acts of aggression; whereas dissuasion is aimed at convincing a potential adversary to not compete with the United States or take an undesirable path such as acquiring, enhancing, or increasing threatening capabilities. In a very simplistic sense, deterrence is about deterring the use of WMD or other capabilities; whereas dissuasion is about deterring the acquisition of WMD. For both, however, we have to understand our adversaries. We have to understand how they perceive ours. We must tailor not only deterrence but also dissuasion. We must also tailor assurance because we need to understand how our allies are going to perceive our actions and our words to some of these other players.

Second, I will discuss several aspects of tailoring deterrence as listed in Figure 2. The first is tailoring deterrence to specific actors. We need to differentiate among deterrees because they are not all alike; they are not all the monolithic Soviet Union. There are major powers, rogue actors, and terrorists; and they all have a different way of making decisions. But there are some commonalities amongst these basic groups.

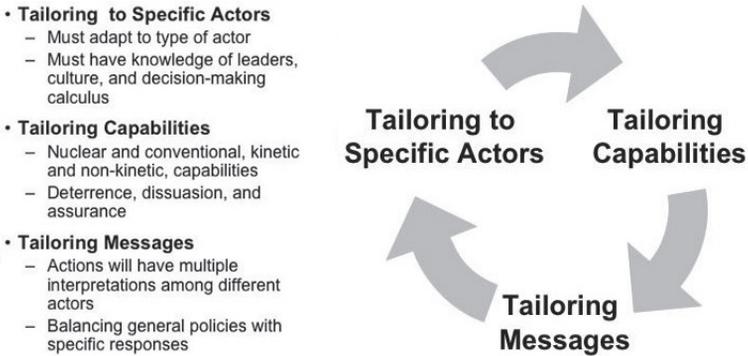


Figure 2 Three Aspects of Tailoring Deterrence

Ambassador Ronald F. Lehman has said that, “tailored deterrence has to be context-specific and culturally sensitive.” We need to understand our adversary’s culture and the context in which he operates. Not only do we tailor for specific actors, we also have to look at their possible actions. We may have to vary how we treat them based on which actions we are trying to deter.

Next, we have to tailor capabilities. Capabilities have to be clarified, both broadly and narrowly, because we do not have a good sense of what constitutes a good mix of capabilities for deterrence, partly because it is very hard to measure deterrence. It is easy to measure our capabilities; it is not easy to measure how they affect the decision-making calculus of the adversary. Although we seem to be doing very well in deterrence lately, that metric could change in a heartbeat. Also, we are no longer the domain of nuclear weapons or nuclear forces for deterrence. There are a number of other aspects to capabilities: conventional

aspects, nonkinetic aspects. Information operations play a very large role in deterrence.

Finally, we need to be able to tailor our communications. We have a distinct problem in communication with our adversaries and with others on the global scene that can actually hinder our ability to deter specific actors from conducting specific actions.

SPECIFIC ACTORS

Specific actors can include major powers, rogue states, and terrorist networks (Figure 3). During the Cold War, the United States spent enormous amounts of time, energy, and effort to understand how the Soviets thought and what might deter them. That knowledge was not easily obtained and often there were differences in opinion about the Soviet thinking. Now, the set of actors is much more diverse, which makes the equation much more complex. Major powers are easier to deter because major powers are going to be more risk averse. They are also going to perceive their stakes as equivalent to those of the U.S., and they are likely to be less concerned about regime change. This makes for a symmetric situation.

- **Involves more than categorizing by type of actor: major power, rogue state, non-state actor**
 - The adversary's values, objectives in a particular scenario, decision-making, perceptions of the stakes of a situation, and how averse to or accepting of risk they are must be taken into account.
 - The adversary's perception of America's objectives, values, decision-making, and risk tolerance also matters.
- **Difficulties:**
 - Deterring terrorists . . . an oxymoron?
 - Messages sent to one actor are heard by all.

Figure 3 Tailoring to Specific Actors

We have a better communication avenue with major powers than we do with what are known as rogue states. We have less confidence in our ability to deter these states, primarily because

the stakes involved are asymmetric. In fact, it is unlikely that the United States would use a strategic capability, particularly a nuclear capability, in response to low-level actions—and they know that. There is also a perceived existential threat by these rogue states that makes the situation a little different. More importantly, they're unfamiliar with how we make decisions because they haven't really studied us in this context.

“In a very simplistic sense, deterrence is about deterring the use of WMD or other capabilities; whereas dissuasion is about deterring the acquisition of WMD.”

It is clear that terrorists, such as al Qaeda and Hizbollah, present another unique challenge. In May 2006, in a commencement address at West Point, President Bush said, “The terrorists have no borders to protect or capital to defend; they cannot be deterred, but they will be defeated.” But can they be deterred? Is deterring terrorists really an oxymoron? Denying benefits to these actors may be some deterrence—a suicide bomber does not want to die for no reason; he does not just walk across a busy street because he wants to be a martyr; he needs to have a result. So, making these actors believe that their results will be ineffective is a way of denying the benefits.

What about actions? What do we want to deter them from doing? Lesser acts—low-level actions that don't directly affect U.S. vital interests—may be harder to deter. The QDR stated that we should be deterring use of WMD, terrorist attacks in the physical and information domains, and opportunistic aggression. Those are some of the deterrence actions we could take, but there are others. What kind of questions do we need to ask about the actors that we're trying to deter? What are the nation's or group's values or priorities? How are these values affected by the actor's history and strategic culture? What are their objectives in a particular situation? Who makes the decisions? How do they calculate risks and gains? What do they believe they have at stake? How risk-averse are they? What do they perceive as America's answers to these questions? For example: What are our objectives? What are

our stakes? What is our propensity for taking risk in a deterrence or dissuasion context?

TAILORING CAPABILITIES

The Nuclear Posture Review—which should have been called the Strategic Posture Review—of 2001 developed a new triad that considers nuclear and non-nuclear capabilities for offensive strike, both kinetic and nonkinetic, and information operations (Figure 4). It includes active defenses, such as missile defense, and passive defenses as well as a responsive infrastructure to enable those defenses. The QDR in 2005 narrowed the idea of terror deterrence, associated it primarily with the new triad, and called it the primary capabilities for deterrence. That is true; there is a primary set of capabilities for deterrence, but that is a limited view. The capabilities of the new triad affect different sides of the discussion calculus—for instance, threat by punishment, threat of denial. Broadly defined, offensive forces increase the potential risks to the aggressors and, as the defense decreases, their gains. For some, the new triad capabilities are still a code word for nuclear weapons and developing new nuclear weapons with niche capabilities, optimized for specific characteristics such as low-yield earth penetration, reduced residual radiation, or biological agent defeat. That is, again, a very narrow view of what the new triad should be and actually what we need for deterrence.

New Triad – 2001 Nuclear Posture Review

- Capabilities can be tailored to achieve specific objectives:
 - Offensive forces increase potential risks to aggressors
 - Defensive forces decrease potential gains: deterrence by denial
- *However* – capabilities alone do not deter:
 - Policies, messages, and actions deter.
 - Must consider how messages will be received by different actors.

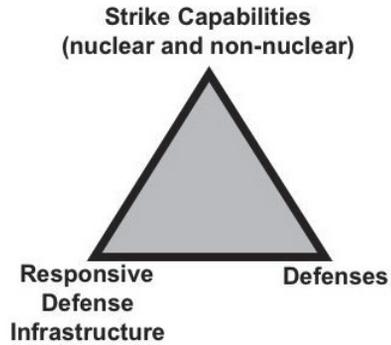


Figure 4 Tailoring Capabilities

The other view is that the capabilities not only in the new triad but also in the force posture at large mean a wider range of capabilities than just nuclear: improved options for conventional global strike and nonkinetic options, such as computer network attack, as well as defenses of all kinds. One example is the conventional Trident missile. It provides us the capability to strike distant targets globally, such as terrorist enemy camps, missile sites, or suspected WMD caches, within a short period of time—in other words, global strike. Currently, if there are no deployed forces, the only option we have for rapid, global reach is our nuclear force. That is clearly not acceptable for dealing with these new threats.

“In fact, it is unlikely that the United States would use a strategic capability, particularly a nuclear capability, in response to low-level actions—and they know that.”

There is an even broader view that says our capabilities, such as forward presence, force projection, and allied cooperation, are all part of the deterrence equation. The capabilities can be broken down into two categories: direct means and enablers.

1. Direct means directly and decisively affect the decision-making calculus of the enemy. These include force projection, active and passive defenses, global strike—nuclear, conventional, kinetic, and nonkinetic—and strategic communications.
2. Enablers are those that indirectly impact or favor: situational awareness, command and control, forward presence, security cooperation, etc. Capability-based planning may be good for determining the type of capabilities, but it doesn't necessarily help us in developing the proper mix and telling us how they should be employed. Some work is needed on capabilities.

TAILORING COMMUNICATIONS

The final aspect of tailoring deterrence is tailoring messages or communications (Figures 5 and 6). The messages are sent by the U.S. in both words and action. More important is how those words and actions are perceived by the adversary. For instance, flexible deterrent options are an example of a specific kind of action that would enhance our deterrent posture. Declarative policy, or official statements, must be consistent with U.S. values, systems, government, and national character. It is also possible to have nonpublic declarative policy, such as when James Baker delivered a letter from [the first] President Bush to President Hussein on the eve of the first Gulf War, which warned that Iraq would pay a terrible price if Hussein used chemical or biological weapons. That message has been credited with its decision not to use chemical weapons.

Deterrence in a Complex and Dynamic Strategic System

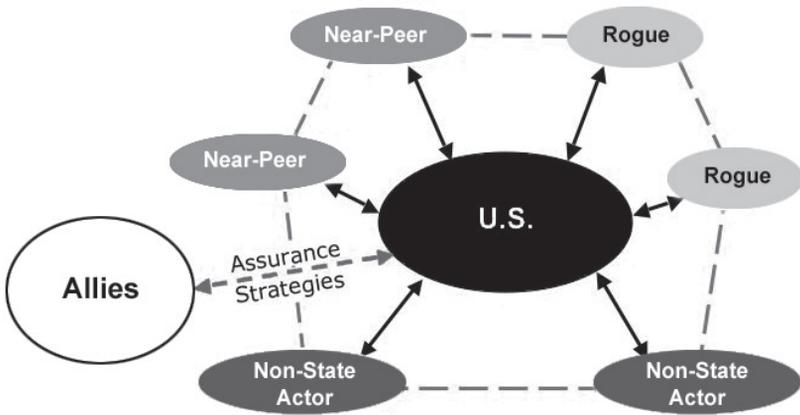


Figure 5 Tailoring Messages (1)

Dealing with Complexity:

- Specific actions, stated policy, and the “Cacophony of public opinion” can contribute to (or detract from) our deterrent posture.
- Communications in peacetime are probably more important than words said or actions taken in times of tension.
- Risk of different actors taking different “lessons” from U.S. actions: Example: Operation Iraqi Freedom
 - Iran and North Korea accelerated their WMD programs.
 - Libya renounced theirs.

Are there a universal deterrence message and set of actions?

Figure 6 Tailoring Messages (2)

We need to match words and deeds because all the actors are paying attention—we cannot have a one-to-one communications relationship. Iran is listening to what we say and what we do

about North Korea. Our allies are watching, and they need to be assured. This issue is difficult and complex. Stated policy can sometimes undermine deterrence as well as enhance it. If we do not stand behind stated policy, our deterrence efforts can suffer. Credibility and the ability to be effective are important. Public opinion matters. If we are not really sure what the right position is, the cacophony of public opinion might plant uncertainty in the minds of our adversaries.

CONCLUSIONS

The feasibility of this implementation of terror deterrence is still unknown. But falling back onto old concepts of deterrence is not an option. We have to be more adaptable. The increasing complexity and dynamic threat environment demand no less. One of the main points about communications is that the message intended is less important than the message received (Figure 7).

- **Tailored deterrence involves a three-part approach:**
 - Tailoring to specific actors
 - Tailoring capabilities toward specific goals
 - Tailoring messages in a complex globalized system
- **Must consider deterrence, dissuasion, and assurance strategies in peacetime and in times of crisis**
- **The United States needs to continue to shift from a “one-size-fits-all” notion of deterrence toward more adaptable approaches.**

The message intended is less important than the message received.

Figure 7 Overview of Tailored Deterrence



3.3 TAILORED DISSUASION AND DETERRENCE?

Jasen Castillo

INTRODUCTION

The logic of deterrence or coercion is still sound. What has changed is the environment. We are faced with an array of actors with differing capabilities and motives, which complicates our decision-making about the kinds of threats that would dissuade or deter.

DISSUADING AND DETERRING URW

How can we dissuade and deter unrestricted warfare? Are there certain conditions or characteristics that we need to take into account to make more convincing threats? Shall we create conditions where competition is not favorable or create incentives for adversaries to cooperate with us? Our adversaries have strong incentives to avoid force on force and to use unrestricted warfare means in conflicts where the stakes are very high for them. To deter unrestricted warfare, we have to deter conflict, which is hard to do when the balance of the stakes does not favor us in a conflict. If our adversaries think they have more at stake and they must fight, it is easier to fight against states.

Dr. Jasen Castillo is an analyst in the Office of the Undersecretary of Defense for Policy. Dr. Castillo worked at the Rand Corporation, where he led and participated in studies on nuclear and conventional deterrence. He holds a Ph.D. in Political Science from the University of Chicago and will shortly join the faculty at Texas A&M's Bush School for Public Policy and Government Affairs.

Successfully tailored dissuasion and deterrence depend on identifying the correct mix of costs and benefits to influence the calculations of our adversaries. During the Cold War, we tried to tailor deterrence against the Soviet Union. We are having the same kind of discussion today about an array of different actors.

THE CARROT AND THE STICK

The terms dissuasion and deterrence are familiar. Dissuasion (i.e., general deterrence) in this context means discouraging states from competing with the United States because it is costly or it is not beneficial. Dissuasion should also be balanced with incentives for cooperation. The carrot should go along with the stick—we should provide incentives for cooperation along with increasing the cost of competition. The same goes for deterrence. Our opponents need to know that we can hurt them or deny them, but also that we will restrain ourselves (Figure 1).

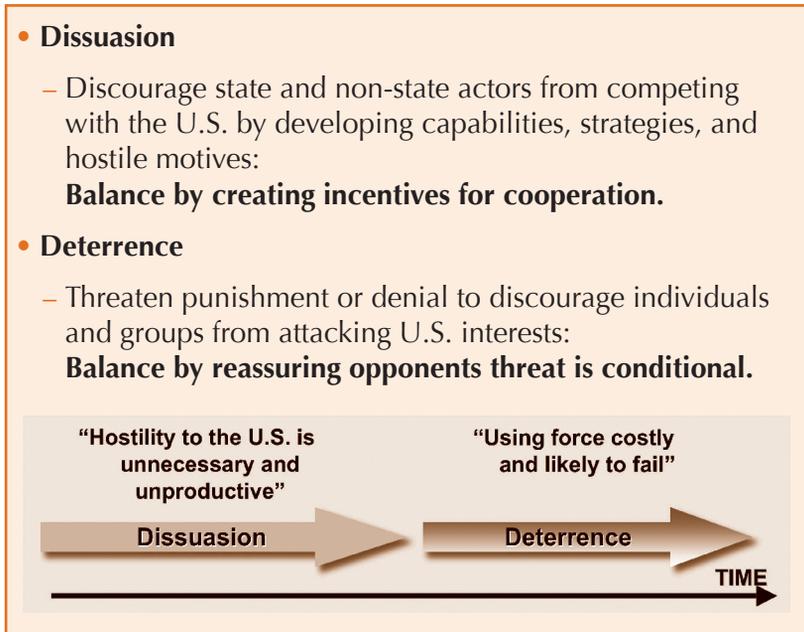


Figure 1 Dissuasion and Deterrence

Dissuasion and deterrence happen over time and require the three Cs: capabilities, credibility (the actions and statements that make our threats believable), and communication (Do the adversaries understand us? What are their perceptions?).

HOW TO STRIKE A BALANCE

One place to start in our consideration of dissuasion and deterrence is our baseline for all our deterrence theory—the Cold War. Because dissuasion is about competition, how do we view long-term military competition with a variety of actors in the international system? In the case of a near-peer competitor, how do we establish an enduring situation that (a) will allow us to defend better, defeat the adversary, and deescalate should deterrence fail; and (b) will allow us to win that long-term military competition without being too provocative and making our adversaries implacable aggressors?

In international relations, we must be provocative to deter, but being provocative may convey potentially malevolent intentions to an adversary. We need to think about how a long-term competition is going to evolve with countries like China. We need to understand this debate between competing and cooperating because we do both. The real difficulty is how to do both in a way that does not start a new Cold War.

Here, the focus is on deterrence. The strategic environment favors unrestricted warfare in confrontations with the United States as opposed to the Cold War, when our conventional weakness led us to compensate by making implicit and explicit nuclear threats. It was a situation where the stakes were high for both sides. Today, we want to emphasize our conventional forces because they are superior. However, if we face adversaries whose stakes are higher than ours, they will have great incentive to turn to strategies that we perceive as unrestricted to deter U.S. intervention in the conflict.

In the background are our allies. Our allies were largely worried about being abandoned during the Cold war. Today, they are worried about being not only abandoned but also getting entrapped. Tailored deterrence was a Cold War term that meant

understanding our adversaries’ perceptions of costs and benefits. Today, we need to apply that same principle to our allies. Does Japan, for instance, want to help the United States defend Taiwan? Is it worried about being entrapped in that conflict? Does it see stakes in that conflict? These are the kinds of questions we need to ask. If the stakes are high, a conventionally weak adversary is going to turn to unrestricted warfare, either in strategy or tactics.

Elements of tailored deterrence or any kind of coercive policy have to take into account how our adversaries think about costs and benefits. What motivates them—fear or opportunism or both? What implications does it have for our threats? How can we get them to understand inducements, and what is the right balance between competition and cooperation? These considerations influence decision making about dissuasion as well as deterrence. We need a better understanding of how our adversaries calculate costs and benefits. We need a baseline to think about deterrence.

CHARACTERISTICS AND DANGERS ASSOCIATED WITH VARIOUS ACTORS

Table 1 is a list of possible missions we would want to deter. The shaded items are in the domain of unrestricted warfare.

Table 1 Possible Deterrence Missions

Missions	
Limited Aims; Quick Land Grabs	
Conventional Aggression on Allies	
Attacks on Homeland or Allies	Domain of Unrestricted Warfare
Coercion Against Allies	
Transfer of Nuclear Materials	
Support of Insurgencies	
Escalation in a Conflict	
Deterring Coercion, Conflicts, and Escalation	

Table 2 lists the categories of adversary characteristics that will influence decision-making about deterrence. Are our adversaries worried about their external security environment, or are they more revisionist? Are we taking actions that generate misperceptions? What about their internal insecurity? We now know that Saddam Hussein took extensive measures to coup-proof his regime, measures that impacted the military effectiveness of the Iraqi army on the battlefield. Will a desire to avert a coup affect our adversaries' decision-making capabilities?

Table 2 Adversary Characteristics Complicating Deterrence and Dissuasion

Characteristics
External Insecurity
Revisionist Motives
Misperceptions
Internal Insecurity
Poor Decisionmaking Capacity
Asymmetry in Stakes
Asymmetry in Capabilities
Vulnerable Forces
Difficult to Punish

Characteristics Associated with Near-Peer or Regional Competitors, Rogue States, and Nonstate Actors

How does the enemy perceive the stakes in the conflict? An asymmetry of capabilities may mean that the enemy will use unrestricted warfare. But what about asymmetries in the vulnerability of the retaliatory forces? The difficulty is how to punish adversaries whom we can't find or how to hold them hostage when they are willing to bear a great cost in pursuit of something they see as valuable.

INTERNAL AND EXTERNAL INSECURITIES

Our assessment of these characteristics will have implications for how we deter a conflict from the start. For instance, if an adversary is worried about external insecurity and misperception, he is more likely to embark on defensive aggression. In that case, we want to consider strategies that do not exacerbate those external fears.

“Dissuasion and deterrence happen over time and require the three Cs: capabilities, credibility (the actions and statements that make our threats believable), and communication (Do the adversaries understand us? What are their perceptions?).”

Some adversaries also have internal security problems, largely stemming from the process of democratization. Jack Snyder and Ed Mansfield showed that states undergoing democratization tend to turn to foreign adventurism and foreign provocation to solve their domestic problems.¹ It is probably going to be very hard to deter those countries. Their decision-making capability will be poor, which means that the general staff of a particular dictatorship is probably not going to tell its leader that the military balance does not favor aggression. It is going to make miscalculations. Even though the conventional balance may not favor it, it may still embark on aggression.

During a conflict, the asymmetry and stakes are going to cause these adversaries to deliberately escalate a conflict. When they begin to lose because of our conventional superiority, they may turn to chemical, biological, or even nuclear responses to convince us that the stakes are not worth the gamble.

¹ E. D. Mansfield and J. Snyder, *Electing to Fight: Why Emerging Democracies Go to War*, Cambridge: MIT Press, 2006.

ADVERSARY CATEGORIES

The typical categories of adversaries are near-peer competitors, rising regional powers, rogue states, and nonstate actors (Table 3).

Table 3 Associated Dangers

Characteristics	Dangers
External Insecurity and Misperceptions	Defensive Aggression
Revisionist Motives	Opportunistic Aggression
Internal Insecurity	Conflicts to Divert Domestic Problems
Poor Decision-Making Capacity	Conflicts Caused by Miscalculation
Vulnerable Nuclear Forces	Preemptive Escalation
Asymmetry in Stakes	Deliberate Escalation in a Conflict
Asymmetry in Capabilities	Inadvertent Escalation in a Conflict
Difficult to Punish	No Restraints on Violence
Dangers Associated with Near-Peer Competitors, Rogue States, and Nonstate Actors	

NEAR-PEER OR RISING POWER COMPETITORS

For the near-peer or rising power, the danger is the ambiguity of our deterrent threats and their fear of our conventional military power. In those situations, we want to emphasize dissuasion—to convince the adversary that there is some form of competition; but it does not threaten their core interests. More importantly, we want to delineate the lines where U.S. interests are firm and the adversary's interests are firm so that

there is no miscalculation about what we will and will not fight for. We do not want to create ambiguity that invites aggression.

If we do exercise our formidable conventional forces in a conflict in a way that would defeat the adversary, the danger of inadvertent escalation is always present. What we think of as regular operational conventions may look to an adversary—especially, if he has a small nuclear arsenal—like the precursor to a conventional or a nuclear counterforce strike. For the near-peer competitor, then, we need to reduce ambiguity about what we will defend and about our commitment to our allies and, particularly, avoid creating inadvertent escalation.

ROGUE STATE

The characteristics that make a state rogue also make this adversary harder to deter than a near-peer or rising competitor. Its decision-making or revisionist motives lead it to be more accepting of risk. For dissuasion, we need to demonstrate that competition with the United States threatens its core interests. This state is going to look for windows of opportunity to seize territory, present the United States with a *fait accompli*, and dare the U.S. to dislodge it. In those situations, we have to make the lines clear and the threats clear. We also want to bolster the denial of conventional forces of our allies so they do not present tempting targets. We want to have plans for managing escalation against these types of adversaries because, in a conflict, they will have incentives to use unrestricted warfare. We should explore damage limitation capabilities because deterrence is likely to fail for the reasons that generated the conflict in the first place and because these states, once they get into a conflict with the United States, are likely to worry about their own survival. The greater part of our decision-making here is on damage limitation.

NONSTATE ACTOR

Finally, for the non-state actor, the danger is that this adversary has revisionist motives. It is difficult to punish him because there is nothing we can hold hostage, and his ideology makes

him immune to pain. The asymmetry in stakes and capabilities means he is going to escalate and pursue unrestricted warfare in a conflict.

IMPLICATIONS

This environment has implications for us in several areas: Policy and Strategy, Intelligence, Capabilities, Global Posture, and Security Cooperation.

POLICY AND STRATEGY

Typically, we think of terrorists or insurgents as undeterrable. Elaine Bunn² outlined these arguments very concisely in a recent article. We need to consider strategies to break up the terrorist's network. Can we cajole or threaten its state sponsors with a variety of inducements or punishments? Can we dissuade the less motivated members of these movements by freezing their financial assets, threatening their families, or jailing them?

“More important, we want to delineate the lines where U.S. interests are firm and the adversary's interests are firm so that there is no miscalculation about what we will and will not fight for. We do not want to create ambiguity that invites aggression.”

We are dealing here with an imbalance of stakes and a perceived lack of our credibility: how we behave in one conflict has implications for another conflict. We are going to make different decisions in the Middle East than in east Asia. We want to have the adversary focus on our forces in the region and pay less attention to our reputation or how we behaved in previous crises.

We need to understand and derive plans for managing nuclear escalation and reduce the incentives for our adversaries to acquire nuclear weapons. Our allies need to protect themselves from

2 E. Bunn, “Can Deterrence Be Tailored?” Strategic Forum (National Defense University), No. 225 (January 2007)

becoming tempting targets so that we are not forced to dislodge rogue states that may have small nuclear arsenals.

INTELLIGENCE

We need to develop an understanding of the adversary's ideological forces, their motivations, and their world views. The Islamist movement is not monolithic; we can try to work with groups that may be less extremist. We also need to develop and deploy new sensor technologies such as remote sensing of concealed and shielded nuclear materials.

CAPABILITIES, GLOBAL POSTURE, AND SECURITY COOPERATION

Capabilities for deterring terrorist threats should include both kinetic (i.e., military) and nonkinetic tools (such as freezing assets and restricting travel). We must use our new global posture to reduce the vulnerability of key military assets and reassure our allies. We can make more credible threats by moving to a hardened basing posture in a region. Finally, we must develop new friends and allies through security cooperation, which will not only improve our relationships and reassure our allies but also strengthen their capabilities so they do not present tempting targets.

CONCLUSION

U.S. conventional superiority creates strong incentives for adversaries to use unrestricted warfare. Consequently, preventing conflict through dissuasion and deterrence is the best way to protect U.S. interests from the effects of unrestricted warfare. Further, successfully tailored dissuasion and deterrence require strategies that recognize the characteristics of near-peer competitors, rogue states, and nonstate actors that motivate their use of unrestricted warfare.



Q: *We'll start with a question for Dr. Castillo and Col. Lutes. "How does the ability to identify the origins of a URW attack—who the adversary is—affect our ability to deter the various actors we face?" I suppose the question may perhaps deal more with cyber attack where attribution might be difficult, but it may also be more general than that.*

▬ **Col. Charles Lutes** – Attribution is very important, but what is just as important is our adversaries' estimate of our attribution capability. I do a lot of work with WMD and the issue of attribution, particularly for the terrorist use. We need to be able to attribute where a nuclear device came from or where the material might have come from. If the state sponsors believe that we can attribute the source of such material, they'll think twice about distributing it to anybody else.

▬ **Dr. Jasen Castillo** – We think attribution might be a tricky issue because there's a tradeoff: How much do you want your adversary to know about your attribution capabilities? The more knowledge you share about your attribution capabilities, the more they might think, "We know the U.S. focuses on bomb designs, so we'll steal a bomb; and we'll use it on the U.S. homeland. That will really complicate their decision-making." You don't want to open yourself up to that kind of threat. Conversely, you do want states to know that you have the ability to do nuclear forensics because, again, attribution usually has a state address. We're worried about states giving these nuclear weapons or chemical/biological weapons to terrorist groups, and you want states to know that you can attribute those weapons to them and that they have return addresses.

▬ **Col. Charles Lutes** – There's also a time element in terms of forensics and attribution. If we can do the forensics to figure out

where the weapon came from, but it takes us a month, that's not sufficient to deter the adversaries or to take the next action. There's also an issue of whether our ability is credible on the international stage. We've had problems with our intelligence community in terms of the WMD issue in Iraq. It's going to take a higher standard now to definitely attribute something to an adversary.

▬ **Mr. William Parker** – The attribution issue, even when we can attribute a weapon or action, is what we can do about it? Who do you go after? Who do you strike? How do you do it? How do I present forces? What is the face of my response? Do I have a response? The time factor is really critical.

Q: *Tailored deterrence is not one-size-fits-all, and it's probably on a timeline—it's not one plan staged continuously throughout the whole event. There's a famous quote: "Enemies have a say in the outcome, and no plan survives first contact with the enemy." How can we analyze and assess the deterrence value of particular courses of action, particularly ones that we've already started? Taking the example presented here, what deterrence value does Operation Noble Eagle have in preventing a terrorist attack? What abilities do we have, or what capabilities do we need to have in place to measure the cause and effect of our messages, our actions, etc.?*

▬ **Mr. William Parker** – Part of the answer is the assessment piece that we talked about, which is very, very critical in an analytical capability—assessment of perceptions, culture, all of the cognitive issues that we discussed. Are we really up to speed inside the minds of the people that we will have to engage and that we're watching or listening to or exploiting at any given moment?

The shift in the nature of deterrence is how specific we must become in the engagement continuum pre-phase zero. As we move into warfighting, we have to be very specific about what we're trying to deter in an adversary's decision calculus and assess just as specifically precipitators, audience reaction, how our message was perceived, etc.

▬ **Col. Charles Lutes** – Operation Noble Eagle was mentioned, and that raises the issue that I assume Brad Roberts covered yesterday: Why hasn't the dog barked? Why haven't we been attacked in the homeland again? It's not just capability; it's not just

Noble Eagle. It's our homeland security posture. It's a very difficult thing to analyze because it's synergistic and it's complex. A lot of times, we end up measuring inputs rather than the outputs.

▬ **Dr. Jasen Castillo** – I'm going to depart slightly from the emphasis on tailored deterrence, which involves understanding all of the complexities and nuances of our adversaries. I'm going to say that maybe we don't know the nuances of our adversaries, so let's go back to basics and think about the kinds of missions they're trying to execute and the likely strategies they're going to use to pursue those missions. Noble Eagle is a denial threat—it makes it harder for the adversaries to carry out their missions. Sometimes, you do want to plan to defend because, by planning to defend, you make it harder for the adversary to execute the offensive strategy. Planning to defend gives you a first cut, some metrics, to evaluate effectiveness because sometimes the dog does not bark. The enemy doesn't attack, and you don't know why. You want to be able to judge if you're able to defend; and if so, whether you can deter.

▬ **Mr. William Parker** – Planning to defend is different than planning to defeat. I sometimes get the sense that defend always takes a backseat. I have no argument with that, but planning to defeat is actually the lesser option.

▬ **Dr. Jasen Castillo** – There's an assumption that, when you move into the warfighting phase, you're no longer coercing; you're using brute force, and you're going to disarm the enemy. That has unintended consequences, and it's wrong not to think of that in a coercive framework.

Q: We had a question about an assessment of deterrence value. That would be what we in the analysis world call experimentation; but in reality, in this context of deterrence, it would be real-time experimentation. Are we, for lack of a better term, probing? Are we initiating actions with potential adversaries for deterrence partners, etc., to generate or stimulate a response so that we can get smarter about those adversary responses and then feed them back into our tailored deterrence plan? Do we have the capability of doing that today, and are we doing that?

▬ **Dr. Jasen Castillo** – I don't know about that capability; but as a building block, one of the things that our office is thinking about is how to dissuade. It sounds good in practice; but it's very difficult because, in an ideal world, you would convince your adversary not to compete with you at all. The question is: Can you shape that competition in ways that are useful and beneficial to you? We also want to think about the different steps in that competition. This is the input to any kind of simulation or modeling, but we want to start thinking about dissuasion as a long-term competition: What those steps entail, the unintended consequences of what we might do, and how we shape them and force them to pursue particular actions that are advantageous to us. How do we force an adversary to go down a road that actually makes deterrence easier for us?

▬ **Mr. William Parker** – I agree with everything you've said. I'm a real stickler for taking every opportunity to make contact and engage because that establishes a record of behavior that we should be able to funnel to the technologists and the analysts to create what-if scenarios. There's been this tendency to engage too little and too late—and entities and people don't respond to too little, too late.

▬ **Col. Charles Lutes** – I'm a big believer in red teaming. I don't think we do enough, and I'm not sure that we do it properly. A lot of times, you'll get a bunch of military guys and say you be blue and you be red, and let's play it out. What you really need to have on a red team is people who are steeped in the culture and the decision-making process of the adversary. They certainly will have a different outlook than our standard military planners. I think that's what we need to move to in terms of experimentation.

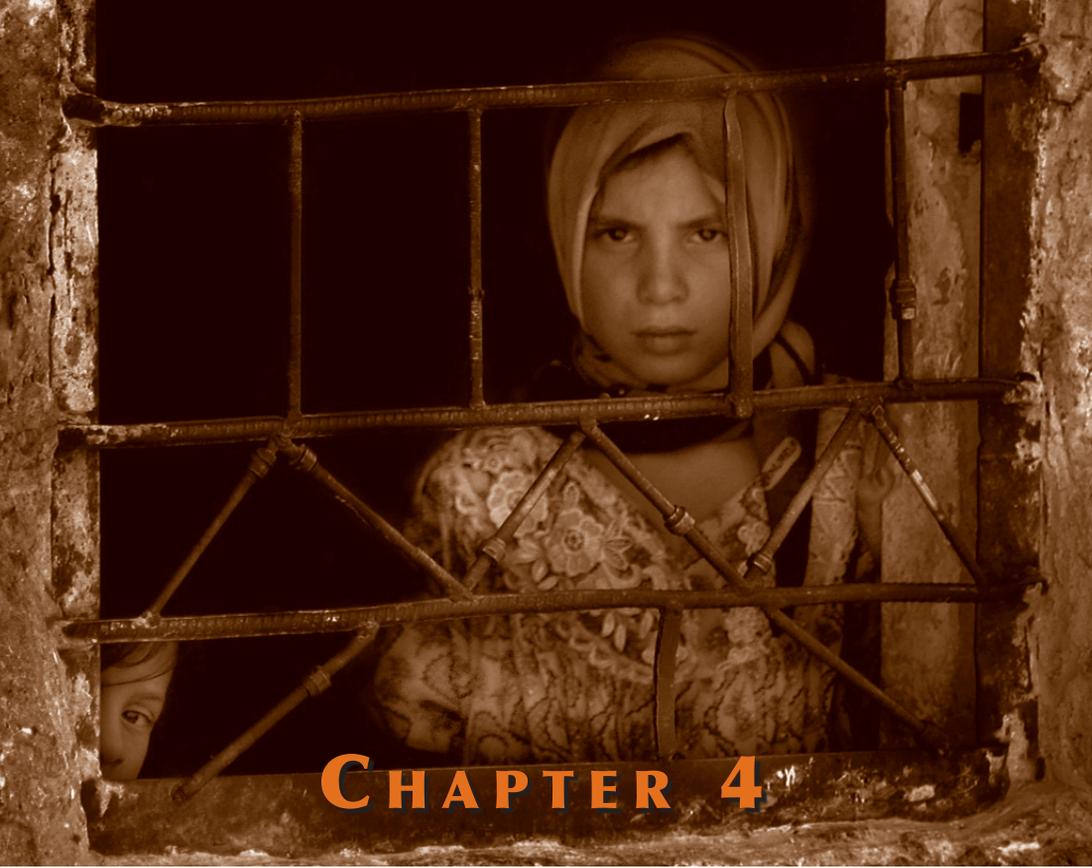
▬ **Mr. William Parker** – Some of the most dynamic and sharpest people in uniform I've ever met are the foreign area experts. The entire personnel system has to change somehow to allow these people to rise up through the ranks. We put a lot of money and effort into these folks, but they never make it through the system as quickly as others.

Q: *We look at deterrence, and we think of the challenges in the area of tailored deterrence; but the “M” part of DIME is just one fraction of the whole set of means available to us. Certainly, a lot of the economic, the commercial, and the informational will be driven more by nongovernmental activities; we certainly see that in the globalization reach to China. One of the encouraging results of the China situation is the close economic ties between our two nations. Are there any plans in place to try to better leverage the nongovernmental elements that are available to us to understand the adversary, to tailor our messages, etc.?*

▬ **Mr. William Parker** – That’s one of my pet peeves. You talk about people with exquisite situational awareness, people whose livelihoods depend on black ink. That’s the e-concept. When you’re overseas or down range and usually in a remote part of the world, there is no chancellery; you’re it. The Pepsi distributor, the MacDonal’d’s distributor, Mr. Pizza Hut; they can make you a star. For some reason, as you get over one of the big ponds, either east or west, the people become capitalists. We don’t engage them, and they don’t come to us. It’s almost like you need departmentalism. We need a global outreach corps that will make the Peace Corps look like Cub Scouts and get out there and unmask, then engage.

▬ **Col. Charles Lutes** – This is clearly a problem. In general, we don’t have a good system for getting all elements of national power together. I’ll give you an example. Right now, we’re conducting a big project at NDU [National Defense University] to write a theory of space power. What is space? How does it contribute to the elements of national power? We found that there’s a different approach in the civil, commercial, and military realms to looking at space. That’s something we need to work on because other nations are better at it.

▬ **Dr. Jasen Castillo** – I’m kind of old-fashioned on the DIME issue. There’s good historical evidence that strong economic ties don’t prevent states from going to war. In terms of diplomacy, a lot of talk is cheap. Recognizing those two factors means that you focus on the military. That’s one way of making costly signals and creating less ambiguity in deterrent situations.



CHAPTER 4

ANALYSIS ROUNDTABLE

**ANALYTIC
SUCCESSSES AND
APPLICABILITY TO
URW**



4.1 MODERATOR'S SUMMARY

L. Dean Simmons

The objective of the 2007 URW Symposium's Analysis Roundtable was to discuss analysis approaches that have worked well in the past and, where possible, to extrapolate their applicability to the intelligence, operations, and capability assessments that will be needed to respond to the demands imposed by URW. As the symposium has stressed, however, the analysis community does not work in a vacuum but, rather, provides the assessments that are needed by the Strategy and Technology communities to make choices on overall U.S. military strategy and the force structure, force employment, and system concepts that will best enable its implementation. The strategy and technology communities, in turn, provide essential inputs to the analysis community.

The relationships among the three communities are outlined in more detail in Figures 1 and 2. Figure 1 shows the interconnections between strategy and analysis. As indicated, the strategy community identifies the measures of success that

Dr. L. Dean Simmons is a National Security Studies Fellow at The Johns Hopkins University Applied Physics Laboratory. Dr. Simmons served as an Assistant Director in IDA's System Evaluation Division, developing expertise in manned and unmanned tactical aircraft, rotary wing aircraft, surface ships, and combat lessons learned assessments. He has twice received IDA's prestigious Andrew J. Goodpaster Award for Excellence in Research. Early in his career he served at the Center for Naval Analyses, specializing in amphibious warfare systems. Dr. Simmons has contributed on the Defense Science Board, Naval Studies Board, and Air Force Scientific Advisory Board. He has published articles in the Journal of Defense Research, the Marine Corps Gazette, Vertiflite, and the Proceedings of the Naval Institute.

can be used to quantify the outcomes of URW conflicts. Using these measures, the analysis community provides assessments of the risks and benefits of alternative strategic postures and force-employment courses of action as well as measurements of force and system capabilities.



Figure 1 Relationship Between Analysis and Strategy Communities

Figure 2 shows the interconnections between the technology and analysis communities. The analysis community provides assessments of the potential value added of new concepts for specific military technologies, systems, or effects identified by the technology community. The technology community, in turn, provides the analysis community with specifics regarding the technical characteristics and performance parameters of the technologies, systems, and effects of interest. Although the analysis community's technology-related assessments have a different focus than the strategy-related assessments, both types of assessments should be based on the URW measures of success identified by the strategy community.

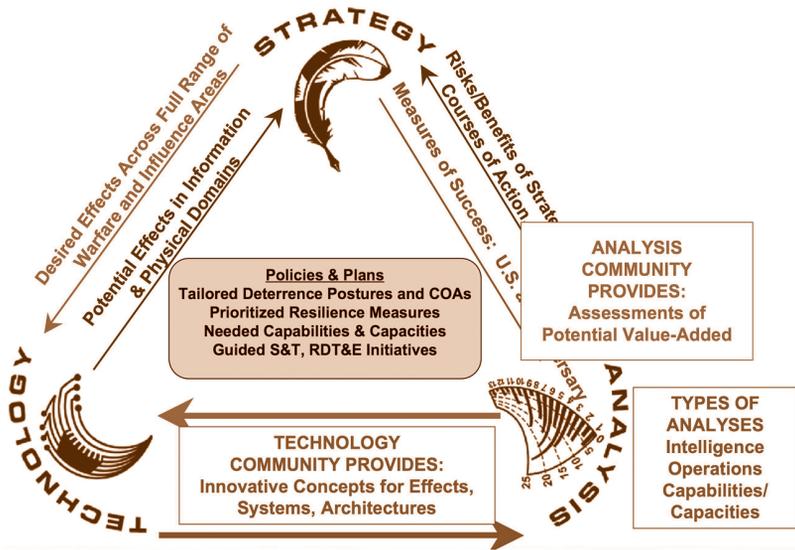


Figure 2 Relationship Between Analysis and Technology Communities

SUGGESTED ACTIONS FROM THE 2006 URW SYMPOSIUM

To conduct quantitative analysis of the strategies, operations, tactics, systems, and technologies that might be employed to combat URW, the 2006 URW Symposium’s Analysis Roundtable recommended that the analysis community (1) expand the set of success criteria beyond the traditional conventional warfare measures of damage inflicted on an adversary and own forces and territory gained or lost in the course of military operations, (2) identify and use measures of effectiveness that show defensive as well as offensive options, (3) include the perspectives of the knowledge and behavioral sciences in addition to those of the physical sciences, and (4) incorporate mathematical and quantitative techniques from these other scientific disciplines when developing tools and assessment approaches for examining URW.

ROUNDTABLE PERSPECTIVES

The 2007 URW Symposium's Analysis Roundtable provided three perspectives on the analysis community's progress in implementing the recommendations identified last year.

MR. TIMOTHY BRIGHT: ASSESSING IRREGULAR WARFARE

The first presentation was by Mr. Timothy Bright from the new Irregular Warfare Division within OSD's Program Analysis and Evaluation Directorate. Mr. Bright framed his perspective by noting that there are many questions surrounding irregular warfare that require evaluation, but traditional analytic tools and approaches do not appear to be applicable for this purpose. At the same time, however, development of new assessment tools is proceeding slowly; and PA&E has relied on wargames and informed judgments to provide insights. Mr. Bright expects that it will take some time for the analysis community to develop enough corporate analytical expertise to have confidence in a new generation of irregular warfare-specific analysis techniques. In the interim, decision-makers and the analysts who support them will have to rely on rules-of-thumb that fit the available data.

DR. ANDREW ILACHINSKI: COMPLEX ADAPTIVE SYSTEMS, MULTIAGENT-BASED MODELS, AND SOME HEURISTICS REGARDING THEIR APPLICABILITY TO URW

The next presentation was by Dr. Andy Ilachinski from the Center for Naval Analyses. According to Dr. Ilachinski, the complex nature of URW makes untenable the traditional analysis approach of searching for, or computing, "optimal solutions." Analysts can no longer afford to ignore qualitative factors such as the effects of human interaction and reasoning. The explanatory mechanisms that relate the many aspects of URW problems are not "simply" linear as is assumed in many, if not all, of the detailed, high-resolution scripted models used by the community. Dr. Ilachinski goes on to explain that complex adaptive systems and multiagent-based models provide a means of overcoming these problems but present new difficulties in their application

and interpretation that will require a concerted effort on the part of the analysis community.

PROFESSOR GARY SHIFFMAN: ECONOMIC ANALYSIS AND UNRESTRICTED WARFARE

Professor Gary Shiffman from Georgetown University gave the final presentation. Arguing that economic analysis offers a powerful tool for the study of and application to unrestricted warfare, Dr. Shiffman focused on two key economic concepts: the Individual, who is assumed to act in his own best interest, and the Institution, which imposes constraints on individuals. Dr. Shiffman showed how the behavior of rulers as diverse as Fidel Castro, Saddam Hussein, Usama bin Laden, Kim Jung Il, and the leaders of the Peoples Republic of China can be understood from an economic perspective.

“Analysts can no longer afford to ignore qualitative factors such as the effects of human interaction and reasoning.”



4.2 ASSESSING IRREGULAR WARFARE

Timothy Bright

INTRODUCTION

The Irregular Warfare Division was established by the Director of PA&E last fall. The context for the establishment of my office was the QDR [Quadrennial Defense Review], finished early last spring, which set forth several key strategic guidance precepts for strategic challenges (including irregular challenges) and four focus areas in which the Department of Defense should be building additional capabilities (Figure 1). Defeating terrorist extremism is one of the focus areas that falls squarely in the irregular warfare quadrant. In addition to the strategic challenges and the focus areas identified by the QDR, we have a new force planning construct for force planning missions; and irregular warfare capabilities occupies a new importance in sizing and shaping forces in the future. My division focuses on arraying our talents across PA&E and trying to advance these objectives.

Timothy E. Bright, Director of the Irregular Warfare Division PA&E Office of the Secretary of Defense, is responsible for leading evaluations of a broad spectrum of defense program and budget issues. Mr. Bright previously served as the director of PA&E's Regional Assessment and Modeling Division; Assistant to the Director of PA&E; and as an operations research analyst in the Projection Forces and Land Forces divisions. He has earned the Secretary of Defense Medal for Exceptional Civilian Service, the Office of the Secretary of Defense Award for Excellence, and the Joint Meritorious Unit Award. Mr. Bright has a Bachelor of Science degree from Virginia Polytechnic Institute and State University and a Master's of Public Administration from Syracuse University.



Figure 1 Strategic Guidance

WHAT IS IRREGULAR WARFARE?

How do we think about irregular warfare? In the Department of Defense, we have a new working definition of irregular warfare, as shown in Figure 2. There are three major types of operations: irregular warfare operations; major contingency operations;

need to undertake in the future years—not current operations or supporting TTPs [tactics, techniques, and procedures] for what we’re doing in Iraq or Afghanistan today. Our time horizon is 2008, 2009, and all the way out to 2013 and beyond.

RESOURCING THE GLOBAL WAR ON TERROR (GWOT)

Last year, we conducted an exercise to gain some insight into the capabilities required for irregular warfare. We had clearly been told that GWOT was our highest priority, and we were also searching for high-impact QDR initiatives not addressed in the previous years that we could bring into the baseline budget to resource our GWOT needs. Early in the year, the Deputy Secretary contacted the combatant commanders, who were developing their own subregional campaign plans for GWOT. Other parties, like General Cartwright and TRANSCOM [U.S. Transportation Command], that are also providing supporting capabilities were asked to identify the capabilities they needed to implement their subregional campaign plans for GWOT along with any capability gaps. This inquiry revealed (Figure 3) about 50 individual capability shortfalls.

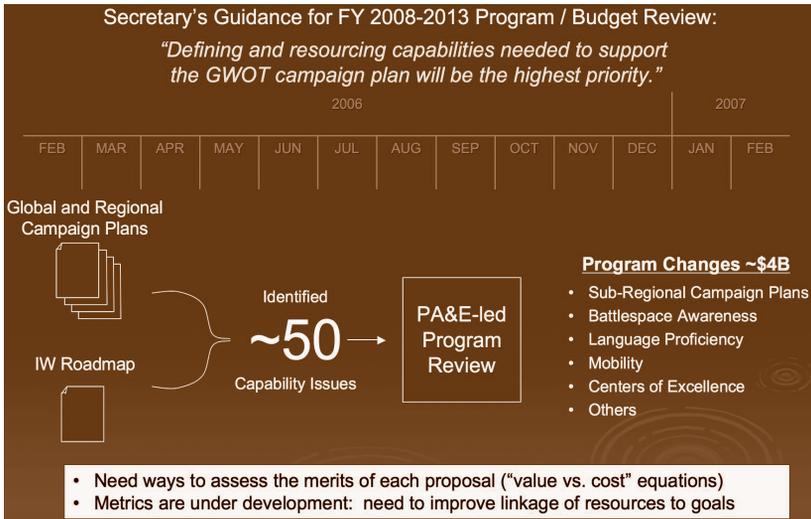


Figure 3 Resourcing GWOT

Our responsibility in PA&E was to investigate and understand the issues surrounding those 50 shortfalls. In many cases, as General Cartwright indicated, not only were the gaps revealed, but specific solutions were identified. Then, we asked ourselves if there was any other way to satisfy the shortfall other than through what the combatant commanders were seeking and if that capability existed in some other aspect of the defense program. Accordingly, we divided those 50 issues among a dozen or so separate issue teams, which were responsible for doing the discovery, packaging the issues, and taking the issues to senior leadership. The senior leadership forum is the Deputy's Advisory Working Group, co-chaired by Secretary Gordon England and Admiral Edmund P. Giambastiani.

Throughout the course of those presentations, senior leadership made a series of decisions, shown on the right-hand side in Figure 3, resulting in about \$4 billion in funding directed toward these new GWOT initiatives. Funding was focused not just on the CENTCOM [U.S. Central Command] region but included the subregional campaign plans, such as OEF [Operation Enduring Freedom], trans-Sahara initiative in EUCOM [U.S. European Command] AOR [area of responsibility], PACOM [U.S. Pacific Command] for the Philippines, several SOUTHCOM [U.S. Southern Command] initiatives in the Caribbean area, and the triborder region. The kinds of initiatives that were funded through the course of our year-long review included battle space awareness, language proficiency, mobility, small aircraft to serve the subregional campaign plans, and a center of excellence for the SSTR activities.

GWOT X-GAME METHODOLOGY AND RESULTS

As a result of the exercise, we found that we really needed better ways of linking the effectiveness of these various proposals to our objectives. In many cases, we are finding that subject matter expertise and qualitative assessments are the coin of the realm as opposed to quantitative analyses. We have metrics under development, but we need to continuously improve them.

Last year, PA&E undertook an experimental GWOT wargame to try to identify not only the demands for irregular warfare capabilities in the future but also the capabilities needed to source those demands; i.e., the resources that we would need to have within the Defense program to source the projected demand. Figure 4 shows our methodology. The wargame represents red and blue forces over time representing several different terrorist organizations in a number of countries over a period of about seven years. The red CONOPS [Concept of Operations] varied over time. We tried hard to focus not just on the military aspects but also to assess effects across political dimensions, the military, economic, social, and other aspects.

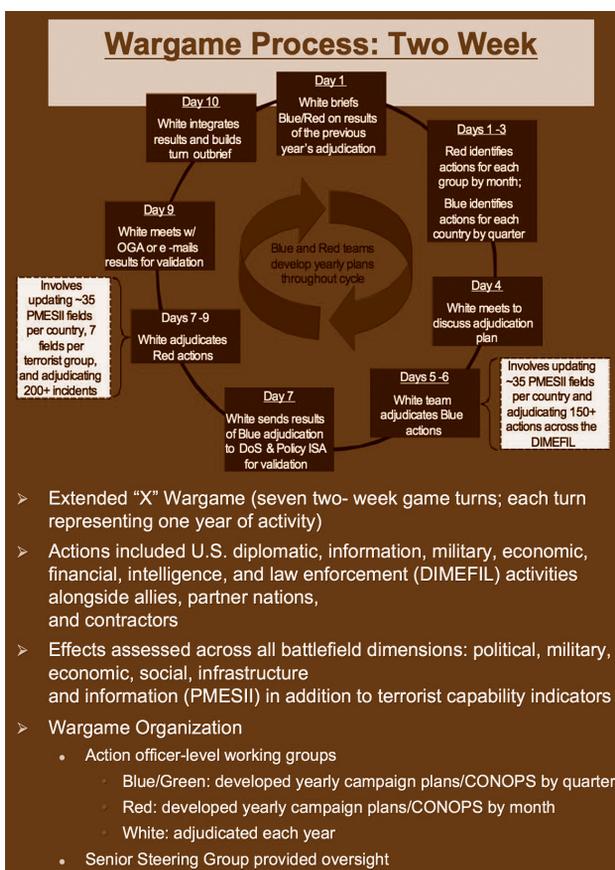


Figure 4 GWOT X-Game Methodology

Many of the results were classified, but a common theme throughout the study was the importance of our Special Operations Forces (SOF) and the likely stresses on them in the future (which mirrors the current state of our SOF). They carry out the preponderance of our foreign internal defense missions today—the foreign training mission—and we investigated potential ways of realigning them and their missions. We spent quite a bit of time considering the potential use of general-purpose forces in that capacity. The Marine Corps recently established four military training units that have since migrated into the MARSOC [U.S. Marine Corps Forces Special Operations Command] units. We considered at length the merits of establishing foreign training units within the conventional forces that would be dedicated and specially trained for that particular mission.

KEY ANALYTIC CHALLENGES

As we considered the challenges faced by our office and PA&E in general, we developed a list of key issues that needs to be addressed. One of the issues we are currently wrestling with is how to define “winning” in a nonlinear counterinsurgency. How do we know that we’re at the end? How do we devise metrics for issues like psychological operations? These nonlinear issues don’t necessarily have a direct tie to operational or strategic objectives. For example, last week in Iraq, some Marines were explaining to us how they thought they had performed an act of good will on an earlier deployment by distributing soccer balls to the kids in the Fallujah area. In subsequent deployments, they discovered that the children’s fathers felt shamed by the gifts because they were unable to give their children these toys. The plan now is for locally recruited and trained police forces to distribute the soccer balls. Establishing that relationship among the Iraqis themselves made the locals feel as though they needed to pay for the soccer balls in kind, and they are starting to deliver more information. We need to think through the metrics. It’s not just giving out soccer balls—they have to be given by the right people.

We’ve spent quite a bit of time today talking about data. That’s entirely appropriate. We do not know exactly what data

information we need to collect; and we need to do a much better job of identifying the right data, collecting them, and employing them. We have a whole series of nonlinear challenges—multiple sides and parties, each with its own agenda and point of view; and we do not have good ways of evaluating them and assessing the capabilities that we need to address them. In the near term, at least, we may not be able to model the theory of victory for irregular warfare. In the meantime, we are relying on rules of thumb, subject matter expertise, and war games like the one I described.

“Last week in Iraq, some Marines were explaining to us how they thought they had performed an act of good will on an earlier deployment by distributing soccer balls to the kids in the Fallujah area. In subsequent deployments, they discovered that the children’s fathers felt shamed by the gifts because they were unable to give their children these toys.”

CONCLUSIONS

We have got our job cut out for us. Our traditional tools are not well suited for the kinds of issues that we are dealing with. It is going to take quite a bit of time for us to acquire the right tools and expertise. In the meantime, we have got to do the best we can and apply the best thinking.