Proceedings on Integrating Strategy, Analysis, and Technology
in Support of the U.S. War on Terrorism Campaign

2008

UNRESTRICTED WARFARE SYMPOSIUM

SPONSORED BY:

JOHNS HOPKINS UNIVERSITY

APL SAIS

NATIONAL INTELLIGENCE COUNCIL NIC

DEPARTMENT OF STATE UNITED STATES OF AMERICA

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

OUSD(P)

RONALD R. LUMAN, EXECUTIVE EDITOR

UNRESTRICTED WARFARE SYMPOSIUM
2008

PROCEEDINGS ON COMBATING THE UNRESTRICTED WARFARE THREAT:

INTEGRATING STRATEGY, ANALYSIS, AND TECHNOLOGY

10-11 MARCH 2008

SPONSORED BY:

JOHNS HOPKINS
UNIVERSITY

APL SAIS

NATIONAL INTELLIGENCE COUNCIL NIC

DEPARTMENT OF STATE UNITED STATES OF AMERICA

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
OUSD(P)

RONALD R. LUMAN, EXECUTIVE EDITOR

ACKNOWLEDGMENTS

Executive Editor:	Ronald Luman
Managing Editor:	Ellen Wilkinson
Project Editors:	Natalie Dickins
	Judith Marcus
	Heather Pontius
	Daniel Portwood
	Ellen Wilkinson
Art Directors:	Catherine Peacock
	Ian Courtney
	Brenda Waltermeyer
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 Department of State's Coordinator for Counterterrorism (DoS/CT); 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/

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

Dr. Ronald R. Luman,
Head, 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

CHAPTER 4
ENABLING PARTNERS TO COMBAT THE ENEMY

CHAPTER 5
DETERRING TACIT AND ACTIVE SUPPORT

Chapter 6
Eroding Support for Extremist Ideologies

Chapter 7
Defending the Homeland

Chapter 8

Senior Perspectives

Afterthoughts

Appendix A

Appendix B

Foreword

Welcome and Perspective on Unrestricted Warfare

FOREWORD – WELCOME AND PERSPECTIVE ON UNRESTRICTED WARFARE

Ronald R. Luman

INTRODUCTION

Thank you all for coming to the Third Annual Unrestricted Warfare Symposium. We are here today to share ideas on the DoD campaign plan for the war on terror. Our nation is facing tremendous challenges from both state and nonstate actors, who are using unconstrained methods of conducting warfare. I started this symposium series in 2006 because I am convinced that an integrated community of strategists, analysts, and technologists can be more creative in meeting those challenges than communities working separately.

I would also like to acknowledge our cosponsors: OSD Policy, Department of State's Coordinator for Counterterrorism, and the National Intelligence Council, as represented by Dr. Tom Mahnken, Ambassador Dell Dailey, and Mr. Dan Flynn.

I would like to take a few minutes to talk about the theme of the symposium—what unrestricted warfare is and what is it not. Unrestricted warfare spans three of the four quadrants of the DoD policy illustration of modern warfare. The chief characteristic of URW is unrestricted use of measures, not unrestricted strategies or objectives. Surprise and deception are often involved, as are

Dr. Ronald R. Luman is Head of the National Security Analysis Department at The Johns Hopkins University Applied Physics Laboratory. Dr. Luman now addresses a wide range of national security issues, building upon a broad base of technical experience in areas such as ballistic missile guidance systems, unmanned undersea vehicles, mine warfare, missile defense, and intelligence systems, with particular emphasis on systems engineering.

integrated attacks to exploit more than one vulnerability of a conventionally stronger opponent.

The battlefields have also moved into different domains. Today and tomorrow, we will discuss some of the linkages between terrorism and other cultural, economic, and financial areas.

Our new adversaries are organized in small units, not large military forces. They are cell structured and integrated within normative societies, not apart. Technology has given them a global reach.

We have seen unexpected and dynamic alliances between state and nonstate actors that are difficult to trace and enable the few to impact the many. Most surprising and interesting is that small-scale events that we formerly would have considered tactical engagements now have immediate strategic implications.

We call this kind of conflict unrestricted warfare because the enemy takes actions that cause shock and fear, offend us, and even generate disbelief in the American mind. Some recent attacks in Iraq illustrate violation of our cultural sensibilities and norms. A disabled man in a wheelchair was wheeled into a police station, where explosives underneath his seat detonated, killing a deputy commander. In addition, there have been reports of mentally impaired women being used to carry out suicide attacks. Further, al Qaeda has made a renewed commitment to top 9/11.

With respect to information warfare, the President of Iran has the temerity to twist the IAEA [International Atomic Energy Agency] report to validate his claims of a peaceful nuclear program. This kind of disinformation is very difficult for us to understand. We continue to be surprised that the enemy uses techniques that we would not consider using ourselves.

The objective of this symposium is to pull together a community to develop new approaches to combat unrestricted warfare. The first year, we focused on defining aspects of the challenge. The second year, we tried to push a little closer to solution approaches. We had two strategy panels, an analysis panel, two technology panels, and panels on the information domain and the physical domain. This year, we are focusing on the GWOT [Global War on Terror] campaign concept.

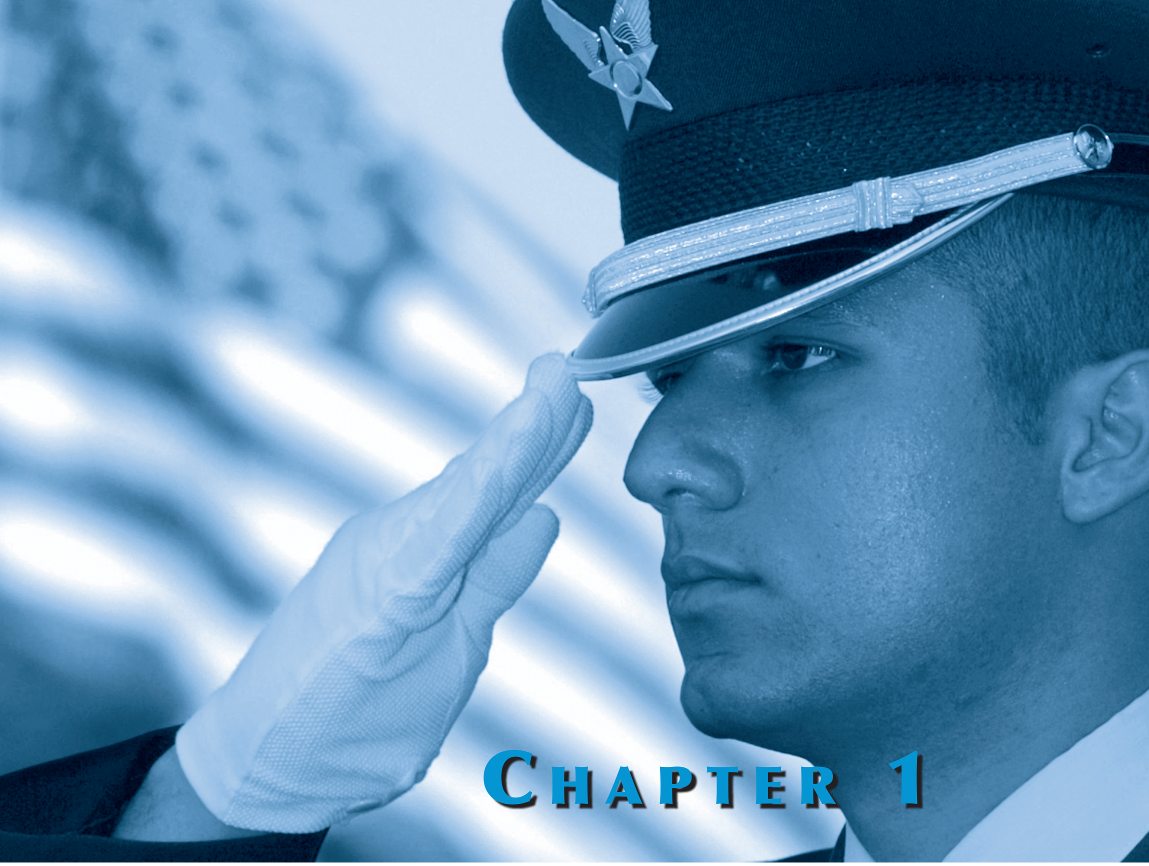
Briefly, there are two direct and three indirect lines of operation in the campaign plan. Our Keynote Speaker, Admiral Eric Olson, will address these in more detail. Also, we have to remember that for deterrence purposes, it is important to have a robust homeland defense—if I can show that I am resilient to attacks, my enemy is less likely to attack. Thus, resilence is becoming well recognized as a valuable complement to prevention.

So what ideas are we coming up with? We have discovered, obviously, that we need to press on with nonkinetic approaches for combating new threats. Also, deterrence, dissuasion, and conflict have to be tailored. Different parties value different issues. The analysis community probably faces a particularly severe challenge to define metrics relevant to modern warfare.

We do not understand URW well enough to apply quantitative technologies amenable to modeling and simulation, so there has been a reemergence of competitive games and war gaming. We have to approach these in a structured way so that results are repeatable and we can validate them. As General Cartwright pointed out last year, technology may enable us to shorten response times and protect our networks and information.

Why is working together so important? Each of the communities needs something from the others. For example, the strategy community needs to understand, through rigorous analysis, the risks and benefits of different courses of action and strategic postures. They also need to understand the potential effects of technology on the information and the physical domains. Analysts need to understand what, in a strategic sense, is valued in the geopolitical domain in order to develop supporting measures of effectiveness. Also, analysts need to know enough about technology to understand the concepts and represent them in their analyses.

Technologists need to understand what strategists want to do across a full range of warfare to influence areas. Technologists also need to understand, in context, the value of their particular technological approach. Otherwise, people can advocate ideas that may not have significant value added. An integrated community will enable us to develop tailored deterrence postures and courses of action, prioritize ideas and systems, and guide our science and technology investments.



Chapter 1

Featured Papers

1.1 KEYNOTE ADDRESS

Eric T. Olson

ADMIRAL OLSON'S KEYNOTE ADDRESS

I applaud the theme of this year's symposium. It marries strategy, technology, and analysis in support of the U.S. War on Terrorism as a campaign. Johns Hopkins is certainly an ideal place to bring together those disciplines. This year, the Department of Defense campaign strategy against terrorism is the framework underlying our discussions. This is a Concept Plan (CONPLAN) that was crafted at the United States Special Operations Command headquarters. It was a new effort and an innovative way of approaching strategies that required significant time and staffing. It was approved by the Secretary of Defense—first Secretary Rumsfeld and then Secretary Gates—and in this venue, serves as a foundation for study toward the integration of technology, analysis, and policy.

As DoD's supporting plan to the national implementation plan (designated as such by the Secretary), it is both the guiding plan within the Department of Defense and the supporting plan

Admiral Eric T. Olson, eighth commander of U.S. Special Operations Command (USSOCOM), leads joint special operations forces and conducts operations worldwide. He is a Naval Special Warfare officer, a graduate of the Naval Academy, and has earned an M.A. in National Security Affairs at the Naval Postgraduate School. His studies in Arabic and French at the Defense Language Institute have served him in SEAL Team operations and the Naval Special Warfare Development Group. He has commanded at every level, including in Israel, Egypt, Tunisia, and as a Joint Specialty Officer and Political-Military Affairs sub-specialist on Africa and the Middle East. His awards include the Distinguished Service Medal and Silver Star.

in the interagency environment. Hence, this framework (depicted in Figure 1) is the focal point of this conference and has authority within the Department of Defense and influence in the interagency environment.

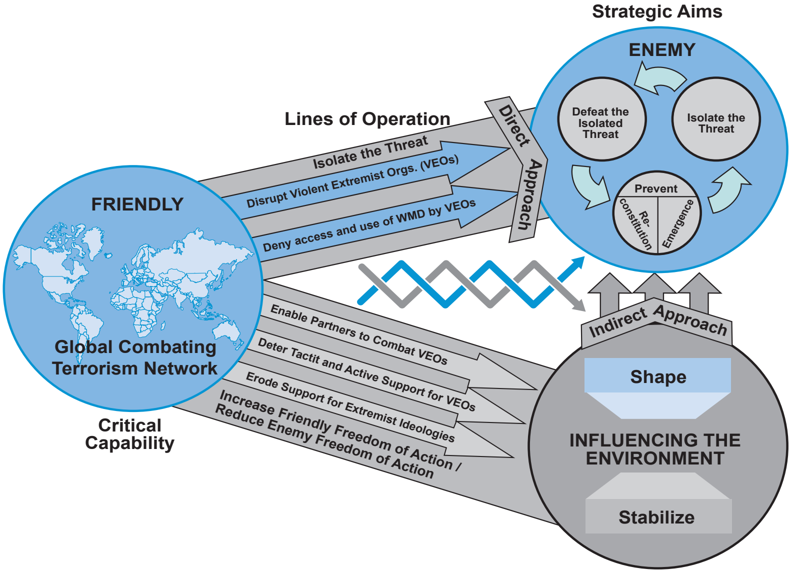

Strategic Aims
ENEMY
Defeat the Isolated Threat
Isolate the Threat
Prevent
Re-constitution
Emergence
Lines of Operation
Isolate the Threat
Disrupt Violent Extremist Orgs. (VEOs)
Deny access and use of WMD by VEOs
Direct Approach
FRIENDLY
Global Combating Terrorism Network
Critical Capability
Enable Partners to Combat VEOs
Deter Tactit and Active Support for VEOs
Erode Support for Extremist Ideologies
Increase Friendly Freedom of Action /
Reduce Enemy Freedom of Action
Indirect Approach
Shape
INFLUENCING THE ENVIRONMENT
Stabilize

Figure 1 CONPLAN 7500

It is certainly the single best source from which to draw DoD strategy. It is supported by regional War on Terrorism plans crafted by each of the geographic combatant commanders around the world, which detail specific actions required to implement the strategy. Requirements, suggestions for force allocation, and application can then be drawn.

In other words, this document has operational application as well as resource application within the DoD. Again, the United States Special Operations Command is the crafter and remains the custodian of this plan. The plan is reviewed periodically. It is in another review now, and I will talk about one change that we have recommended as a part of this review process. I was there for the crafting of the plan so I can give some perspective on how it was derived.

DEFINING TERMS

This is a symposium on unrestricted warfare, which is not a doctrinally defined term. When I am asked periodically what is the most difficult thing I have done since 9/11, my answer is “define terms.” Nothing means what it used to. A lot of the terms that we currently use are not doctrinally defined, and they mean different things within the Department of Defense, across the United States Government, and certainly when we work with our international partners.

War does not mean what it used to. There is unrestricted warfare, irregular warfare, the new variety of counterinsurgency warfare, guerilla warfare—a term that has dropped off the map—and unconventional warfare. We refer to the War on Terrorism, but war in this country means something different when translated into most other languages.

Intelligence certainly has a different meaning now than it had in the past. Some of the more dramatic terms like detainee and torture do not have exactly the same meanings that they used to. It is essential that we define those terms because words are how we frame our discussion and our actions. We have to get it right, and I fear that we are a long way from doing that.

THE LONG VIEW

Unrestricted warfare and irregular warfare characterize the nature of the warfare that we are experiencing—and will experience for the foreseeable future. I am convinced that we are many years from arriving at a coherent approach to unrestricted warfare, let alone some resolution of it. I was quoted around November of 2001 as saying, “This is going to go on long enough that the people who are currently serving aren’t going to be the solution; it is the people who are in high school who are going to end up solving this thing.”

Some of the people I was talking about in high school have already passed through service and left. I am convinced now that I severely undershot the mark when I talked about the high schoolers. We have to be prepared for unrestricted warfare, irregular warfare, unconventional warfare, and all the other kinds of warfare that are coming together in this new world in which we live. We still have to continue to prepare for major combat operations against a significant peer competitor. Clearly, the ability to conduct major combat operations is not a subset of the capabilities that you develop for unrestricted or irregular warfare, and the ability to conduct irregular warfare is certainly not a subset of capabilities that you develop to fight major combat operations.

Doing both requires a holistic government approach—even an international approach. We have to be prepared to act in a proactive and sustained manner. We must take care of the people, equipment, and the intellectual approach that will enable us to act.

> *"This is going to go on long enough that the people who are currently serving aren't going to be the solution; it is the people who are in high school who are going to end up solving this thing."*

The type of warfare that we fight on the ground is not determined by our forces on the ground; it is determined by our adversaries, and we need to be responsive enough to adjust rapidly to what they throw at us. We need to have the agility to transcend the spectrum of conflict. In many cases, we fight at various levels of conflict simultaneously.

THE PLAYERS

There is no dominant player within the interagency environment with respect to unrestricted or irregular warfare. There is no referee or conductor with a wand, who is guiding investment in irregular warfare capabilities development or allocation of forces. It is not too much of an exaggeration to say that as coherent as thought may be within the Pentagon on this issue, it is not truly coherent.

Outside the Pentagon, in other units and organizations, various groups are engaging in what I would call random acts of pursuit of irregular warfare excellence—without real discipline behind them, without a coordinating body, and largely self-initiated. There is no clearinghouse of ideas on how to develop capabilities to counter unrestricted warfare.

The great value of this symposium is that it brings the Department of Defense, other agencies, international players, and industry and nongovernmental organizations together to discuss these issues and help arrive at an intellectually based solution. Lengthy discussions across organizational lines will be needed to arrive at a much more coherent approach.

RESPONSIBILITIES OF THE SPECIAL OPERATIONS COMMAND

We have been assigned some specific responsibilities with respect to the campaign against global terrorism by the Secretary of Defense, by the President, and through the Unified Command Plan. We are in this position because of the history of Special Operations Command. We were well postured to do what the nation asked us to do following the events of 9/11 and have continued to do so through the changes in the world since then.

The Special Operations Command is a unique command. Among the ways in which we are unique is our two-part mission requirement. The first part is to organize, train, equip, and deploy capable Special Operations Forces (SOF) to serve combatant commanders around the world. In this case, serving combatant commanders includes coordinating with ambassadors, U.S. Country Teams, and other agencies around the world.

Special Operations Command was created by an act of Congress, uniquely so among the nine combatant commands. We were afforded certain authorities and a budget. As the Commander of Special Operations Command, I have combatant commander authorities, as you would expect. I also have many service chief-like authorities, military department secretary-like authorities, and head of defense agency-like authorities with respect to research, development, and acquisition authorities.

We can invent our own technologies. We can come up with the idea, invest in the R&D, and field the technology—all within the authorities of Special Operations Command. Those authorities were intended to streamline, simplify, and enable us to field items more quickly than other agencies of our government can, including the Services. We are almost at that point, and although we are still beholden to processes and certifications by the Services, we do have flexibility that other organizations do not have.

A jewel of Special Operations Command is the budget that I am specifically provided by the Congress—for investing in operations that are peculiar to Special Operations—materials, services, and supplies. It is provided to me directly and then monitored so that I do the right things with it.

The second part of our mission is to plan and synchronize operations against terrorist networks. This part of the mission is derived from the Unified Command Plan, signed by the President. That document assigns each of the combatant commanders roles and missions. It says the Commander of the United States Special Operations Command is the lead combatant commander for planning, synchronizing, and, as directed, conducting operations against terrorists and terrorist networks globally.

What does that mean? We had to figure it out as we went along. It evolved from a statement by Secretary Rumsfeld at a press conference in 2003 in which he said, "I hereby designate the United States Special Operations Command as the supported command in the Global War on Terrorism." He did not tell us what he meant by that, and he did not tell anybody else that they were supporting.

We codified this language in the Unified Command Plan. So what does it mean to plan, synchronize, and, as directed, conduct Department of Defense operations? We must consider not just Special Operations but Department of Defense operations in a Global War on Terrorism. What it has come to mean over time is that every day we plan operations. The strategic plan you will see today is a manifestation of that directive.

Every day we synchronize plans—not operations. We synchronize plans and planning at Special Operations Command, and that is a distinction that we have grown comfortably into through a series of battle rhythm events, global synchronization conferences, and daily video teleconferences with all of the combatant commanders. The interagency plays a part in a robust way. Every morning down in Tampa, about 120 interagency representatives come to work on our compound, and about 70 Special Operations representatives go to work in other agencies of government. That is an example of synchronization of plans and planning to address the Global War on Terrorism. Whoever is responsible for executing the plan synchronizes the operations themselves, if you are a combatant commander wondering what United States Special Operations Command is doing synchronizing operations globally.

The following list shows the core activities—and that is the legal term—of the Special Operations Command related to Special Operations. We do not claim ownership of any of them; we claim niche tasks specific to Special Operations in all of them. The core activities that we have invested our resources in since we were created almost 21 years ago are:

1. **Counterproliferation of Weapons of Mass Destruction**: Actions taken to locate, identify, seize, and destroy or capture, recover, and render such weapons safe.

2. **Counterterrorism**: Actions intended to respond to or preempt terrorist activity against us, including offensive measures taken to prevent, deter, and respond to terrorism.

3. **Special Reconnaissance**: Battlefield information gathering for specific target development, allowing SOF to acquire information about the capabilities, intentions, and activities of an actual or potential enemy.

4. **Direct Action Operations**: Raids and assaults that are peculiar to Special Operations and are usually smaller and more surgical than other forces, including short-duration strikes and other small-scale offensive actions taken to seize, destroy, capture, recover, or inflict damage in denied areas.

5. **Unconventional Warfare**: A broadly misunderstood term and clearly not the opposite of conventional warfare; specifically, those operations normally of long duration and conducted by, with, and through indigenous or surrogate and paramilitary forces of other nations for purposes of mutual benefit and interest.

6. **Foreign Internal Defense (FID)**: U.S. participation in the programs of a foreign government to free and protect its society from subversion, lawlessness, and insurgency. This normally is training actively with foreign forces in their country.

7. **Civil Affairs Operations**: Activities that establish, maintain, influence, or exploit relations between military forces, civil authorities, and the civilian population.

8. **Information and Psychological Operations**: Designed to convey selected information to influence the behavior of foreign governments, organizations, groups, or individuals; truth-telling for a purpose.

9. **Synchronizing**: Directing forces in time, space, and purpose to achieve maximum effect.

Note that FID [Item 6] focuses on enhancing the internal security of other nations, primarily through unit-to-unit engagement and training events. Most of our activities around the world are in the category of foreign internal defense. They could involve a Special Forces A-team, a SEAL platoon, or some other small tactical element of our force working in a remote place with a handful of counterparts. We send the best available unit; the host nation handpicks its participants because this is the most prestigious training that they will get all year. Very important relationship building occurs during these foreign internal defense events. Special Operations Command's forces are in about 61 countries, and about 30 of those countries relate to FID.

Civil affairs operations [Item 7] represent the softer side of warfare: nation building and humanitarian assistance. Under the umbrella of civil affairs operations, we do not paint schools and dig wells, but we help determine which schools need to be painted and where the wells should be dug. We normally contract with local forces to do that so everybody wins.

Information operations [Item 8] will be the subject of much greater discussion later in this forum. Information operations are primarily designed to interrupt or influence adversary systems and networks while protecting our own. I describe psychological operations—another broadly misunderstood term—as truth-telling to influence behavior in the population that has been selected for that operation. Generally, this new behavior is intended to prevent bad acts from occurring.

I talked about synchronizing Department of Defense efforts in the GWOT. What I left out is counterproliferation of weapons of mass destruction. That is at the top of the list because failure to prevent proliferation has the most significant consequence—the highest regret factor, if you will. It is interdiction of supplies, materials, precursors, weapons systems at the point of storage, somewhere in transit, or at the point of receipt with specialized skills to render those items safe as they are interdicted. That is the menu to which we apply our intellectual capital, our people, and our money.

CONPLAN 7500

The purpose of Special Operations is typically to gain access and establish relationships in countries where we have a particular interest. Considering those who wish to do us harm, we have to isolate that threat, defeat that threat, and then prevent the reconstitution and reemergence of that threat.

As Figure 1 shows, we start with a friendly association of people and organizations. We call this the Global Combating Terrorism Network. However, there is no such thing. If I ask a room full of people to raise their hands if they are a member of the Global Combating Terrorism Network, they generally do not know what I am talking about. Clearly, military organizations feel that they are part of that network. Other agencies of government feel it to varying degrees. Partners in the Global War on Terrorism—some by treaty, some by coalition membership, some by simple agreement of goals—are members, as are nongovernmental organizations and the global industry. I would say that the network is a loose association of organizations that share a goal of contributing to a planet that is inhospitable to terrorist activities. That is all it is. Everybody contributes in their own way, some more formally than others.

TWO APPROACHES

This friendly environment can get at the enemy or adversary in two ways. We call them approaches: the direct approach and the indirect approach. We have divided them into five lines of operation, a doctrinal term for a series of actions. The lines within "Isolate the Threat" connote violence (Figure 1). These direct lines of operation are disrupting violent extremist organizations—that is the polite way of saying capture, kill, interdict, and disrupt terrorists and terrorist networks to prevent them from harming us in the near term—to deny access to and use of weapons of mass destruction by violent extremist organizations, many of whom have declared their intent specifically to acquire and use weapons of mass destruction to kill great numbers of people in the U.S. and in other nations with whom we are partnered. These lines of operations are conducted largely by the military; certainly, the DoD is in the lead for the direct approach. The direct approach is urgent, necessary, chaotic, and kinetic, and the effects are mostly short term.

In the indirect approach, we enable partners to combat violent extremist organizations by contributing to their capabilities through training, equipment, transfer of technology, war games, etc. DoD is not the lead agent for deterring tacit and active support for violent extremist organizations where the government is either unwilling or unable to remove terrorist sanctuaries, nor for eroding the underlying support and getting at the root causes of terrorism—the economic depression, the extremism, the intimidation that contribute to the development of terrorists and enable recruiting and other terrorist-related activity. Other agencies of our government, international organizations, and other nations need to lead this effort. DoD admittedly has a greater capacity to do those sorts of things than most of the other agents of our government.

It is probably fair to say that we are leading the direct approach from the front, and we are leading the indirect approach from behind. We are providing powerful support to other agencies to undertake these efforts, particularly enabling partners to combat violent extremist organizations. These efforts are urgent and necessary. They are decisive in their impact. They buy time to have their decisive effect. We will not kill our way to victory, nor talk our way to victory. We will behave our way to success in a global campaign against terrorism.

These efforts shape and stabilize the environment, which impacts the enemy in the long term. People, units, and capabilities cannot be categorized as direct or indirect; only *activities* can be categorized as direct or indirect and only at the time that they are occurring. Sometimes they are intertwined and occurring simultaneously (Figure 1).

A great example is what Special Operations forces are doing on most days in Iraq and Afghanistan: training with the Afghan National Army, Afghan National Police, and Iraqi Special Operations Forces at a very high level—conducting raids and assaults with them as well as eating, sleeping, living, working, planning, and fighting with them. When these forces fight, it looks like the direct approach. They look like us, they move like us, they shoot like us, they hop in and out of High Mobility Multipurpose

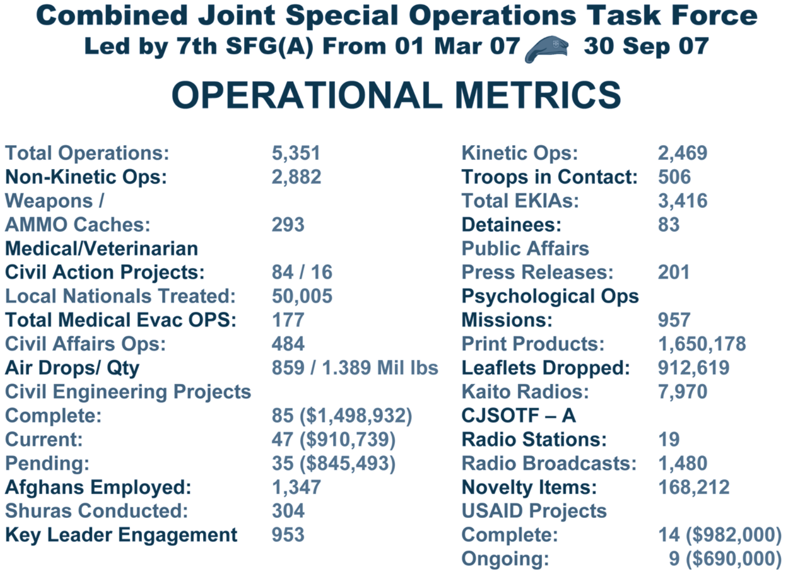
Wheeled Vehicles (HMMWVs) like us, they separate the noncombatants from the combatants, and take all of the actions to meet the objective. Through night-vision video, you cannot tell them from us. It looks like disrupting violent extremist organizations when they burst into a house and apprehend the bad guys in that house. The ultimate effect is enabling partners to combat violent extremist organizations themselves so that eventually we can leave—and they will have the capability to control their own destiny. That intertwining happens several times a night, in several places across Iraq and Afghanistan, and it consumes most of our force on any given day. I want to emphasize that these are the decisive effects. Disrupting violent extremist organizations has had a powerful effect in Iraq, in particular, and we are seeing a dramatic withering of al Qaeda's capability.

In Iraq, the emphasis has got to be on unrestricted warfare, which is exactly the focus of this symposium and of the major discussion that we are having across DoD and across the world on irregular warfare, and it is a fundamental way ahead for the Department of Defense. SOCOM's role in Homeland Defense is to treat it as an away game, not as a home game. SOCOM is less concerned about aspects related to the continental U.S. in this plan.

OPERATIONAL METRICS

In action, Figure 2 illustrates what I just talked about. Figure 2 is what I call the 7 by 7 model: 7 months by the 7th Special Forces Group (Airborne) out of Fort Bragg, North Carolina, and commanded by a SF Colonel. At this time, it was Colonel Ed Reeder, who was on his fourth consecutive rotation to Afghanistan with the same headquarters. He had a force of about 2,400 people, Combined Joint Special Operations Task Force–Afghanistan, from March through September 2007. They conducted 2,882 operations, where the operation was expected to be nonkinetic, with no anticipation of an exchange of gunfire.

They did anticipate an exchange of gunfire 2,416 times, where they killed 3,416 enemies. They also treated 50,005 local nationals in medical, dental, and other kinds of clinics. By the way, the humanitarian projects listed in Figure 2 have huge impact on the people. They dropped 1.4 million pounds of aid and supplies in places that would not have otherwise received any supplies.



Combined Joint Special Operations Task Force
Led by 7th SFG(A) From 01 Mar 07 30 Sep 07

OPERATIONAL METRICS

Total Operations:	5,351	Kinetic Ops:	2,469
Non-Kinetic Ops:	2,882	Troops in Contact:	506
Weapons /		Total EKIAs:	3,416
AMMO Caches:	293	Detainees:	83
Medical/Veterinarian		Public Affairs	
Civil Action Projects:	84 / 16	Press Releases:	201
Local Nationals Treated:	50,005	Psychological Ops	
Total Medical Evac OPS:	177	Missions:	957
Civil Affairs Ops:	484	Print Products:	1,650,178
Air Drops/ Qty	859 / 1.389 Mil lbs	Leaflets Dropped:	912,619
Civil Engineering Projects		Kaito Radios:	7,970
Complete:	85 ($1,498,932)	CJSOTF – A	
Current:	47 ($910,739)	Radio Stations:	19
Pending:	35 ($845,493)	Radio Broadcasts:	1,480
Afghans Employed:	1,347	Novelty Items:	168,212
Shuras Conducted:	304	USAID Projects	
Key Leader Engagement	953	Complete:	14 ($982,000)
		Ongoing:	9 ($690,000)

Figure 2 Operational Metrics – Seven Months in Afghanistan

They established 19 radio stations for psychological operations capability and action. To make sure that someone would be listening to those radio stations, they distributed almost 8,000 radios. It is an exaggeration, but when these guys go out, they set up three tables—the first table is food, and everybody runs to the food line. If the second table is medical supplies, everybody gets out of the food line and gets into the medical line. If the third table is radios, everybody gets out of the medical line and gets into the radio line because what they are really starving for is communication. This was an interagency operation in partnership with the U.S. Agency for International Development (USAID), which has capability but not great capacity. SOCOM was in a supporting role supplying USAID. You can see the level of engineering projects. These are culverts, bridges, and school houses—all tremendously important in the places where they go.

That force of about 2,400 people employed 1,347 Afghans. They became dominant players in the local economy in these remote places where they were—an A-Camp or a firebase in Afghanistan, typically in the middle of nowhere, at risk, and behind barricades and barbed wire. Living inside that camp were 15 to 20 Americans, 100 Afghan police or security forces, and a handful of interagency representatives who were there for intelligence or aid purposes. The soldiers who lived in that A-Camp left that base every day. For example, a shura is an organized meeting of local leaders that takes place at a predetermined place and time. A Special Forces A-Team commander shows up, a mid-twenties captain with a huge responsibility, who negotiates with these leaders for any number of things: "How can we help? How can we engage? What do you know that we might want to know?"

The captains went to those meetings 304 times in seven months. In addition, there were less formal meetings, where military on a routine patrol would stop in a village and talk to the village elder. There were 953 of these meetings. A total of 1,257 engagements with local leaders in the course of seven months kept them busy. This mixture of threat isolation and the increase of friendly freedom emphasizes my point that it is not units or people that are following the path of one line of operation or another (direct or indirect); it is their intertwining actions that have a powerful effect on the battlefield (Figure 1).

PRIORITIES

I am going to go quickly through my priorities, which I have listed in Figure 3, because it lets me highlight a couple of other things. Every commander has priorities. I have told the people at my command if they are going to copy one thing and put it under glass on their desktop, this is it. This is one, two, three—A, B, C—mission, people, stuff. That is the way we are addressing things at our command.

Deter, Disrupt, Defeat Terrorist Threats

- Plan and Conduct Special Operations
- Emphasize Culturally Attuned Engagement
- Foster Interagency Cooperation

Develop & Support Our People & Families

- Focus on Quality
- Care for Our People and Families
- Train and Educate the Joint Warrior/Diplomat

Sustain & Modernize the Force

- Equip the Operator
- Upgrade SOF Mobility
- Obtain Persistent Intelligence, Surveillance, and Reconnaissance

Figure 3 Priorities

Cultural Engagement: Project Lawrence

Under "Deter, Disrupt, and Defeat Terrorist Threats" in Figure 3, I want to highlight cultural engagement. I do not mean sprinkling language dust and culture dust on the masses; I mean making people expert so that they can engage. The measure of success is not 75% accuracy in machine translation; the measure of success is exchanging photographs of their families after several years of engagement with the same people in the same place.

I am embarking on what I call Project Lawrence. We need our Lawrence of Arabia, our Lawrence of Pakistan, our Lawrence of Paraguay, our Lawrence of Indonesia, and our Lawrence of Mali—and we are woefully inadequate as a department at developing and sustaining those kinds of people. All of our systems actually discourage it.

When it comes to fostering interagency cooperation, I cannot solve interagency cooperation, but I can contribute my share to the interagency cooperation challenge. It is much better than it has ever been by a long shot. The farther you get away from Washington or Tampa, the better it is. As people are focusing on what is going to happen that day and that week, policy tends to stay out of it. Even within policy, we are seeing much higher levels of cooperation than we have ever had. I do not buy the horror stories about interagency cooperation; I think it is pretty good but just needs to be better. What we are seeing is what I am calling second- and third-generation interagency contact. People who worked together in one place in the world are reporting someplace completely different and finding former colleagues. It has had a powerful effect. In another 15 or 20 years, this will just be the way it always was.

Equipment

I will talk about the third priority in Figure 3, "Sustaining and Modernizing the Force," particularly the equipment, because the technology resides in the equipment. We must equip the operators to fight and survive in the environments in which we ask them to work. We need the technological edge and survivability in virtually all that we do—in night operations, in maritime operations, and in the full range of optics.

> *"What I want to highlight here is this cultural engagement. I do not mean sprinkling language dust and culture dust on the masses; I mean making people expert so that they can engage."*

We used to think of SOF mobility mostly as aviation, but more and more now, it is ground-based mobility. Those of you who are familiar with Army Special Forces know that not too many years ago, of our five Special Forces Groups, only one was mounted. Only one was even assigned vehicles. Now, everybody is mounted. We have got some sort of an advanced vehicle for about every four soldiers in our organization. We are purchasing the RG31 and the RG33 medium-mine protective vehicles as fast as we can.

We fielded 45 RG31s to Afghanistan just before Christmas. They were out to the camps and operational by about the end of January. We are now down to 43; two of them were totally destroyed by IEDs [improvised explosive devices]. Eight people were involved, and all eight are alive. If they had been in any other vehicle, we would have lost eight soldiers.

The final priority listed in Figure 3 is obtaining persistent ISR [intelligence, surveillance, and reconnaissance]. I am learning that the platforms are essential, but the bottlenecks are not in platforms—they are mostly in people. It is people who are trained to operate and analyze the products of these systems; it is ramp space, hangers, bandwidth, and training areas. It all contributes to ISR capability and capacity.

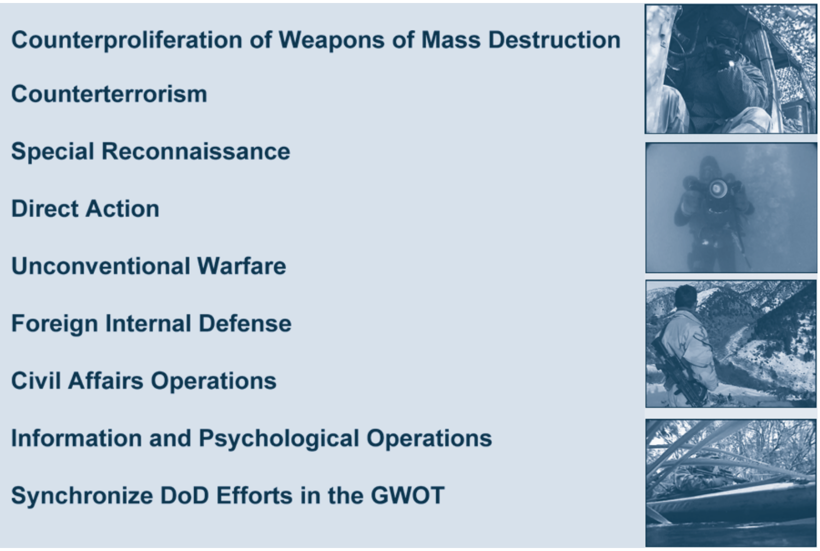
All of these need to move together. As one falls behind, it slows down the whole ISR system. So we are investing heavily in these things, and I have testified to Congress and others that persistent ISR systems are our number one priority within the Department. ISR contributes to force protection, it contributes to battlefield awareness, and it enables the people in these remote camps to determine dominant terrain. You do not know where the enemy is, so you move out; when you take your first round, you find out where the enemy is. Now we can move to tactical dominance rather than move to contact if we have the right sensors over the battlefield.

ISR is a very important capability in the manhunting piece of what we do. You have all seen that bit about the reversing of the triangle: find, fix, and finish. It used to be easy to find and harder to finish. Now it is harder to find but much easier to finish. In the manhunting piece, the specific application of all kinds of sensor systems—overhead sensor systems, ground sensor systems, and human sensor systems—is essential to finding an elusive enemy who is living and hiding within the local population. That is much of what has eroded al Qaeda's capability in Iraq over the last three or four years.

Q & A SESSION WITH ADMIRAL OLSON

Q: *What, in your opinion, is the major priority concerning personnel development?*

ADM Eric Olson – SOCOM's nine areas of responsibility require that we train and educate the warrior/diplomat (Figure 4). You have to train and educate the warrior, and you have to train and educate the diplomat. Many people can do both very well. What we do not have are incentives to be great warriors. We do not have very many incentives within the Department of Defense to be great diplomats.



Counterproliferation of Weapons of Mass Destruction

Counterterrorism

Special Reconnaissance

Direct Action

Unconventional Warfare

Foreign Internal Defense

Civil Affairs Operations

Information and Psychological Operations

Synchronize DoD Efforts in the GWOT

Figure 4 SOCOM's Areas of Responsibility

Our promotion systems are wrong, and our schooling systems are wrong, but I am taking that on. When I identified training in these nine priorities, I did so to remind everybody that it is very important. I initially used the term diplomat, but when I started briefing it around, I had a lot of interagency objection to my use of the word. I have decided now that I really like it. It is exactly the right word. The power here is that it reminds our people that they really are diplomats. They will go places that other agencies will never go. They will meet people and work with them in a way that other agencies never will and for a sustained period of time. They will work over years in a career in a way that other agencies will never reach. That makes them diplomats, like it or not. So they have got to strap that on as part of their mindset.

Q: *What challenges are faced with military and industry relations?*

ADM Eric Olson – A lot of challenges exist, and in many cases, industry prefers not to be closely associated with military activity. It works against them. If that is the case, then we have got to bring them in around the edges, learn from them, and let us enable them. I think we are moving down that road slowly. We have got good contacts—at least, we have had good conversations—with industry, but we have a long way to go.

There is a general reluctance to be closely associated with military activity. What we are seeing is that the more they understand the (indirect) side, the closer the cooperation. There are many instances now where we are working with nongovernmental organizations in remote places running medical and dental clinics. It is a good partnership, and it is hard to tell who is who once you get them out there. Especially in the medical field, there are a lot of people who are looking for the opportunity to go out and do exactly that sort of thing. We are their venue for doing that. So it is creeping up on us in a healthy way. We still have a long way to go, though.

Q: *Sir, when you talked about diplomats, what is the difference between your conception of a soldier diplomat and what the British had in 19th century India with their political officers? One of the things that made the British political officer so successful is that he lived with the tribes, say the Bashtoon, Northwest Frontier Province, for an entire career. How can we develop a career process that would support that?*

ADM Eric Olson – There is no way we can do it now given our current systems. That is what I was getting at when I was talking of Lawrence of wherever. We do need to be able to steep people in cultures and languages far beyond what we are able to do now. Just when I get a guy where I want him after four or five consecutive assignments—a language school, an embassy, another agency of government, etc.—I guarantee that he is nonpromotable.

The difference between a diplomat and a British political officer is that one is an assigned position. We need to understand that all of our soldiers are unavoidably diplomats, and they have to conduct themselves accordingly.

We talk about winning hearts and minds or fighting an ideological battle, but I do not fully subscribe to that. I think that it is much deeper than that, and we have a long way to go before we understand how deep it is. It is much less about ideology if you accept that the root word of ideology is "idea," and ideas can be influenced by logic. I think that this is really more about genealogy and theology more so than ideology.

It is about blood lines and tribal associations that go back a millennium. It is not about what you think but what you believe. There is a bridge between thought and faith that we are having a hard time understanding. I think it is going to take people truly steeped in the culture, who can then coach us into the kind of thought that we need to approach this for the long haul.

I am not saying that this is missionary work. We are not trying to convert them. It is about understanding how agreeing to certain behaviors will be of mutual benefit.

1.2 AL QAEDA ON THE RUN OR ON THE MARCH?

Bruce Hoffman

Six and a half years into the Global War on Terrorism, the United States stands at an important crossroads. Certainly the great progress that we achieved during the initial phases of the struggle, particularly in the first two or three years, were tremendous achievements. When we liberated Afghanistan; when we destroyed al Qaeda's training camps and its operational basis and command and control nexus in Afghanistan; when we succeeded in killing and capturing 75 percent of al Qaeda's leadership, at least as it existed on September 11, 2001; and when our allies and partners throughout the world apprehended or killed more than four thousand al Qaeda operatives are all testament to this progress. I think the problem now is that, in recent years, much of what signals success and progress has been threatened and, in some specific cases, been reversed. Today al Qaeda, which once was most definitely on the run, is now arguably on the march. This, at least, was the conclusion both of the National Intelligence Estimate that was released last July and indeed of the

Professor Bruce Hoffman is a tenured professor in the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service and the former Corporate Chair in Counterterrorism and Counterinsurgency at the RAND Corporation. He has advised the Office of National Security Affairs, Coalition Provisional Authority, Baghdad, Iraq and the Strategy, Plans, and Analysis Office at Multi-National Forces-Iraq Headquarters. Dr. Hoffman is a recognized Fellow worldwide, and holds degrees in government, history, and international relations. He received his doctorate from Oxford University and was awarded the United States Intelligence Community Seal Medallion by the Central Intelligence Agency. A revised and updated edition of his acclaimed 1998 book, Inside Terrorism, was published in May 2006.

new Homeland Security strategy that was unveiled only the previous October.

Perhaps more important is our ability to deter terrorists from attacking the most desirable and lucrative targets from their point of view, and the most consequential targets from our perspective have been cast into doubt. Eighteen months ago, we very fortunately unmasked a plot by al Qaeda to simultaneously bomb at least seven American and Canadian airliners while in flight from the United Kingdom to the United States and Canada. This plot was enormously significant.

First, unlike the conventional wisdom at that time, this was not a plot by entirely independent, self-radicalized, self-motivated, and self-selected terrorists but rather a group of individuals commanded and directed by al Qaeda from its base in South Asia. Second, much like many other al Qaeda plots before 9/11, this one involved a multi-year planning process. Perhaps most worrisome though is that this plot contradicts the belief prevalent at the time that a degraded or diminished al Qaeda was capable only of striking at softer, more accessible targets like metros, commuter trains, hotels, and tourist destinations. This attack, however, was directed against, arguably, the most internationally hardened target set since 9/11: commercial aviation.

Equally troubling is our ability to deter al Qaeda from attacking precisely those target sets that it deems the most attractive and most important. During the months leading up to this plot's unmasking, we captured at least one of the known al Qaeda commanders responsible for planning and implementing the attack. We killed another one, yet, rather than being derailed, al Qaeda merely appointed a third individual—at the time its operational commander in Kunar Province, Afghanistan, Abu Ubaydah al-Masri—to assume control of this operation.

The state sponsors of terrorism who were once dormant and cowering in the immediate aftermath of 9/11—particularly Iran and Syria—are now not only threatening but also active in supporting and assisting terrorist activities, not least against our own forces in Iraq.

Finally, those terrorist groups with global reach, those groups that were not jihadi groups, in the aftermath of the 9/11, attacks had become quiescent, had lain dormant, like Hezbollah, and the Tamil Tigersare now is more active and provocative. How has this been able to transpire? How is it that now six and a half years into the war on terrorism we are at this crossroads where many of our successes are challenged or, in some cases, have been slowly reversed?

I think one answer is that our adversaries have shown themselves to be enormously flexible and adaptive. They have changed, adjusted, and demonstrated an ability to overcome even our most consequential countermeasures. Our adversaries are almost like the archetypal shark in the water that has to constantly move forward to survive, adjusting and adapting its course but nonetheless pressing forward. The question we have to ask is how have we changed? How have we adapted and adjusted? Certainly we have undertaken at least two series of massive bureaucratic reorganizations resulting in the creation of the Department of Homeland Security, the Director of National Intelligence, the National Counterterrorism Center, and of our intelligence community. Certainly we have imposed on ourselves ever higher levels of security.

Equally critically, we have to ask to what extent have we fundamentally changed our mindset and approach given what we see are highly adaptive and highly evolutionary adversaries? In this respect, what are some of the challenges we face in effectively countering the irregular warfare threats of the 21st century that will be so predominant in the decades to come? In one respect, I think there is good news, and a year ago I might not have been quite so positive. What we have seen is the military's ability to adapt and adjust in ways that would largely have been unimaginable six and a half years ago. The United States military, until very recently, has had an overwhelming conventional warfare mindset that was based predominantly on an enemy-centric conception that employed mass firepower and maneuver.

What we have seen in recent years, what I saw very clearly in Afghanistan last week with the 82nd Airborne, is a shift in our military units deployed to counter our regular adversaries from an enemy-centric mind set to a far more population-centric orientation, an orientation that is based as much on guile as it is on firepower and involves techniques such as human terrain mapping (intelligence based on cultural and linguistic understanding), anthropological knowledge, immense cooperation with host-nation security forces, and understanding of the local populace. This has in turn strengthened the capacity of indigenous forces to face these threats.

Despite this major shift, further challenges remain. We need to move away from the anachronistic footprint that a conventional warfare approach still perpetuates. In other words, in addition to the 80,000 additional ground forces that Congress recently allocated to the army and marines to confront our current challenges, we need to build up our training capacity and our ability to enable locals to better prepare to defend themselves against these threats.

In this respect, Lieutenant Colonel John Nagel was absolutely right in his formulation. Rather than the 80,000 more ground forces, he said the money should have gone to 20 thousand new trainers. One of the challenges we face, particularly at a time of declining resources in a military that is already overstretched, is not only to increase our ground combat forces but also to build up the training capacity that will in turn build the capabilities of our local allies.

This training will be absolutely essential to reduce the big U.S. footprint that has often been used by our adversaries against us to portray our nation building and other humanitarian assistance activities as occupation and repression. The biggest challenge we face is not so much in the military and not so much in the realm of kinetics, or even in transforming the military, but in transforming our ability, not just to actively combat and engage terrorists but to break the cycle of recruitment and regeneration that sustains our adversaries.

One of our main challenges is knowing the audience of our message. We are at a point where we realize this. However, we are still not at a point where we are able to implement an understanding that fighting al Qaeda and its jihadi confederates effectively involves not exclusively killing and capturing them but also fundamentally and indisputably watering down al Qaeda's brand. Only in this way can we challenge the continued appeal that resonates from al Qaeda and the jihadi message. Here we face enormous challenges. Ten years ago, Professor Gabriel Weimann of Haifa University undertook a landmark study of terrorist use of the Internet.

In 1998, he counted fewer than 50 terrorist or insurgent groups that had Internet sites. Today, a decade later, there are more than 7,000 active terrorist and insurgent sites. Beyond any measure of doubt, it is very clear that our adversaries have seized on the Internet, the Worldwide Web, bulletin boards, and chat rooms as central means of communicating their message to an audience that they believe remains receptive to it. What have we done in response?

To our credit, the voice of America, for instance, has developed new Arabic language television stations like al Hura, new Arabic language radio stations like al Sawa, new newspapers, and so on. What have we done in the critical area of countering electronic communications? Our efforts, in this respect, have been thoroughly inadequate. For example, to date, only about six percent of the voice of American's budget is dedicated to Internet communications.

Now this is not to say that strengthening television, radio, and newspapers is not enormously important to appeal to the elites as we have traditionally done in our information operations. However, we see that terrorists are continually targeting the youth of the world and of countries that have enormous youth cultures where at least a third of the population is under 17 already; we have to ask what are we doing in the critical arenas to counter messages of hate and intoleration in countries that already have severe economic disparity, political instability, and resource deprivation, exactly where terrorists believe they will find fertile ground for their message.

It was extraordinary that in an opinion piece that appeared in the *Wall Street Journal* on September 14th, the director of the broadcasting board of governors rightly commended the Voice of America's enormous contributions to the War on Terrorism. He noted the newspapers, but not once in that article was there any mention of what the United States was doing in terms of Internet communications or the means and the messages we were directing at the youth of the world today. Publicizing these communications remains an important challenge.

Another challenge is adapting and adjusting to an evolving enemy while still avoiding falling behind the curve in the changes that we see unfolding in warfare and in the nature of our adversary. We are sometimes fixated on current trends and threats without looking ahead. For example, in recent years, considerable effort and attention have been focused on suicide terrorism, one of the main threats we face.

At the same time, while we have remained focused on suicide terrorism, we see in many instances our adversaries shifting their tactics and weaponry, using a variety of standoff weapons such as improvised explosive devices, remote controlled mortars, rockets, and missiles, to also target us. We may learn a key lesson from an event 18 months ago in the second Lebanese war, where Hezbollah did not send one suicide bomber against either the Israel Defense Force (IDF) or against the Israeli population. Instead, they fired 4,000 missiles and rockets against the Israeli population and arguably achieved the same degrees of fear, anxiety, and intimidation that other terrorist operations had achieved in the past with more typical terrorist means. Despite the success of the surge in Iraq, we still have not come fully to grips with some of the repercussions of our involvement in that country. Win, loose, or draw in Iraq, what has emerged in recent years might be termed a cult of the insurgent. A phenomenon that will inspire imitation, replication, and the spread of the techniques and procedures in weaponry that have been used against the United States and coalition forces in Iraq. The historical parallel is not so much the bleed-out phenomenon, like the mujahideen from Afghanistan in the late 1980s and early 1990s, but more from Palestine in the 1970s. During the Six-Day War, a technologically advanced, doctrinally superior, better led, better commanded Israel defense force scored a lightening victory against Egypt, Syria, and Jordan.

In the wake of that defeat and the shame and humiliation that followed, the only untainted, credible military force that emerged were the Palestinian commandos. They understood that they could not defeat Israel on the battlefield in direct combat. Through a long war of attrition, the application of insurgent and terrorist tactics, and superior use of information operations, they could succeed in challenging their adversary and over time hoped to demoralize and weaken them.

I see an enormous parallel here with Iraq. Five years ago, the technologically advanced, doctrinally superior, better led, better commanded American and coalition forces swept aside Saddam Hussein's conventional military, dispatching even such highly vaunted units as the Republican Guard. In the aftermath of that defeat emerged an irregular insurgent force with technology, in many cases no more sophisticated than garage door openers or cordless phones, that was able to challenge what is not only the military of the world's remaining superpower but, arguably, the most sophisticated and most technologically advanced military in the history of mankind.

The ability of the insurgency in Iraq to inflict a degree of pain and suffering that has affected public opinion and the contours of the political debate in the United States is a lesson that future adversaries will take from Iraq. The Iraqi insurgents have come to represent the catharsis of revenge and the empowerment of insurgency and violence, an asymmetric form of warfare that will likely be replicated and repeated elsewhere. What do we need to do? How do we adjust to some of the challenges that I have described?

Our adversary's ability to continue to prosecute this struggle is a direct reflection of their capacity to attract new recruits and to replenish expended resources. Our success will depend fundamentally on our ability to adapt and adjust to the changes we see in our adversary. At the foundation of such a dynamic and adaptive policy must be the ineluctable axiom that effective and successful countering of both terrorism and insurgency cannot exclusively be a military endeavor. It must also involve parallel political, social, economic, ideological, and information activities operations.

To craft such a strategy will critically depend on our ability to think like a networked enemy—to anticipate how they may act in a variety of situations aided by different resources. The challenge we face is to harness the overwhelming kinetic force of our military as part of a comprehensive strategy to counter our adversaries' ability to recruit and regenerate themselves. This requires nothing short of a transformation of capabilities across government—not just within our military—to deal with irregular threats.

We have been remarkably successful in identifying threats, neutralizing those threats, and killing and capturing existing terrorists. To have a truly effective strategy, however, involves looking across generations. They have already been indoctrinated. They have already been radicalized. They are training, and they are arming. They are in the process of being deployed. A successful strategy will be one that looks beyond the next generation to the generation after the next one: that is to the children and the youth across North Africa, the Middle East, and South Asia. We need strategy that generates messages and compelling arguments and effectively disrupts the resonance of the terrorists' message by countering the very arguments that they use in their messages.

Finally, the fundamental question we face is how we sustain this struggle. Countering terrorism and insurgency is a decade(s) long endeavor, not one bounded by months. It will be absolutely critical for our leadership to clarify the core nature of the threat that we face and how it varies region by region and to develop and explain the global campaign plan that extends beyond the military and harnesses all instruments of our national power: diplomatic, informational, economic, and our collective knowledge.

It is one that will place equal emphasis on the hard power, the kinetics of killing and capturing, and the soft power of persuasion and of countering the terrorists' message. It will also be based on a strategy that recognizes that we cannot have a one-size-fits-all solution but one that tailors approaches and policies to local circumstances and conditions.

Q&A Session with Bruce Hoffman

Q: *What challenges in the future might we face, differing from those in the past?*

Bruce Hoffman – The challenges we face in the future are not the clean, neat ones that we might have faced in the past, particularly in the realms of conventional warfare. Rather, the compound phenomena we face have insurgents but also terrorists, militias, bandits, and common criminals who operate both separately and together and whose activities bleed into one another.

In the case of Afghanistan, we already have multiple insurgencies that are both indigenous and are sustained across borders by the insurgents' ability to generate and raise revenue. Certainly the poppy cultivation, that in recent years has exploded in Afghanistan, presents a significant threat to everything that we have accomplished because it is a means of bonding the population closer to insurgents who protect and advance the trade to line their own pockets and advance their political cause.

We face a depressing situation similar to Colombia. It may sound like I am getting off the subject, but I am not. This August, al Qaeda will celebrate its 20th anniversary. The adversaries that are emerging today are not flashes in the pan. They have deep roots. They have a legacy of changing and adapting to survive.

The FARC in Colombia is a perfect example. It was founded in 1964, and it has been able to sustain itself, even in a changing political dynamic, because of its heavy involvement with narcotics cultivation. The revenue that it has been able to attain has created a system of patronage, effectively binding the population closer to them, to provide goods and services almost as a shadow government.

This has been absolutely pivotal in sustaining their struggle. Your question demonstrates one of the last points I was making about the decades-long duration of this challenge. Among the many challenges we have in Afghanistan, poppy cultivation has to be one of the main ones. Again, this goes back to my point that it is one that cannot only be left to the military; it has to involve other instruments of national power.

From my observations, both in Afghanistan and in Iraq, that is where there are asymmetries. We expect our military to do the kinds of things that civilian agencies would have done years ago. This is partially a reflection of the cutbacks in resources we saw at the end of the cold war.

Q: *Did you get a chance to go to Joint Special OPS Task Force (J-SOTF) when you were in Afghanistan?*

Bruce Hoffman – I was able to get a perspective on our special operations in that theatre. I also gained an understanding of our adversaries' strategy there: violence that increasingly has been directed against the UN and are the non-governmental organization (NGOs) as well. This is part of a deliberate strategy on the part of our adversaries to fracture the coalition of forces supporting the democratic Afghan government.

One of our perennial mistakes is that we believe our adversaries are devoid of a strategy and that the violence they engage in is mindless and wanton and not in pursuit of specific goals.

In the beginning of our involvement in Iraq, we saw exactly the same thing in August and September 2003 when the insurgents targeted the United Nations headquarters at the Canal Hotel to force the United Nations out. They targeted the offices of the International Red Cross to get the NGOs out. They kidnapped and then brutally murdered individuals like Margaret Hassan, an Anglo Irish Iraqi aid worker. Their goal was to force other governments and NGOs to abandon Iraq and thereby to isolate the United States and to portray this situation not as any sort of humanitarian assistance or economic development effort but rather as a military occupation. That is what I see as one of the key shifts going on in Afghanistan now. The current insurgent strategy is designed to split the allies, to divide the United States, to force out NGOs and international organizations, and to attempt to replicate this portrayal of the United States presence as an occupation.

One of the biggest challenges we face, when violence specifically targets precisely what the insurgents see as the weak link in the chain, is to push back against it. Frankly, the biggest problem we face in Afghanistan is the importance of a phrase that was once only used in the State Department of "draining the swamp."

In terms of the efforts in governance and economic development in Iraq, we are addressing the draining of the swamp in Afghanistan. That is only one side of the coin, though. At least historically, we have not seen any insurgency or terrorist campaign that has been able to rely on the use of a sanctuary, particularly a cross-border sanctuary. With insurgents that have been able to rely on a government that is tacitly acquiescent, the difficulty of defeating that insurgency is enormous.

Their belief is that time is on their side in whittling down the allies in the coalition in Afghanistan. A formidable challenge for the U.S. is to buttress our alliances and to roll back the violence. That means thinking in terms of both sides of the border.

Q: *What are the major strengths and weaknesses concerning our security forces?*

Bruce Hoffman – Despite the wide disparity in troop strength, and also the strength of the Afghan security forces, we have been successful in the clearing and building part in that country. We have been less successful in the holding. That is because the coverage of security forces to population is much lower than even the deployments in Kosovo or in the Balkans during the 1990s.

Secondly, it is also a problem of governance in that the progress that we made with the Karzai government and representative government in the early years is now threatened by rising corruption. We face compound problems that have to be addressed like the criminality of narcotics and endemic corruption.

Narcotics and corruption creates a population that is very susceptible to fast solutions, even from an oppressive force like the

Taliban. In many respects, Afghanistan has been the Cinderella of the War on Terrorism, unfortunately. That is where this struggle started, but it has not been resourced to the extent needed to succeed. We have done a remarkable job with the available resources, but the question is whether to invest more resources in Afghanistan to ensure the success of democracy, which is critical.

Q: *Is there a call to increase our special forces?*

Bruce Hoffman – If there was a way that we could create special forces quickly, 20,000 more people would be the best solution. That was President Kennedy's vision of 50 years ago—to have these special forces be the type of political warrior that would build capacity among host nation forces, have local knowledge and linguistic familiarity, and would leave this very light footprint so as not to suggest an occupation that the big footprint of large numbers of conventional forces can create.

The challenge we face is that the special operations forces are stretched to the limit as is, both in direct action and in their critical unconventional warfare—or nation building—mode. The numbers of them available and the training of special forces is just much more complex and takes much longer. To my mind, the 20,000 advisors is the next best solution.

Our other main problem is that we do not have the ability in the civilian realms of government, in the State Department, to build up indigenous police forces. This is one of the biggest challenges we still face in Iraq and also in Afghanistan.

The Afghan National Army is probably the most highly respected institution in the country. The Afghan National Police force is not. We can draw exactly the same conclusions in Iraq. We have been very successful in building up the army. The police there are still inadequate. Do not forget, 2006 was supposed to be the year of Iraqi police, and all those metrics failed. It is something that I think you have to have specially trained forces to do; that is to train police.

The idea is to have police officers that could do this, but that is not the reality. We have to turn to building up a very competent training component, such as we had in Vietnam. Studies in Vietnam demonstrated that specified trainers that stayed with a unit over an extended period of time, not just rotated in six weeks or three months but actually stayed with those units from the start in almost a mentoring role, were far more successful than most of the training we do with police.

We put them back in an environment where whatever good we have achieved is often vitiated because they are surrounded by corruption. There is no mentoring. I see this as the long-term solution in terms of facing the insurgency and terrorist threats and building local capacity. Partially, this has to also build up the local ability to engage in force protection of the trainers.

Q: *What options do we have, given the fact that the federally administered tribal areas have become a sanctuary in a training base for a variety of insurgent groups, not just for al-Qaeda?*

Bruce Hoffman – That is a good question and a tough question. I do not have an easy answer because the policies in recent years have led us into a cul-de-sac.

For too long one of our fatal problems has been putting too much faith in President Musharref, and we are left with a very difficult situation today.

The challenge is careful response.

Q: *What do you think we could be doing better?*

Bruce Hoffman – First, we need to have a coordinated message, which we do not have now. We already have the plan: the national strategy for combating terrorism that the National Security Council released a year ago in September. In my view, that was a vast improvement over the 2003 version. I think it said all the right things.

Recognition that this is not just the military's solution, the importance of information operations, the importance of building up capacity and strength outside of the military, the recognition that the military is being overstretched—all those things were in that document. The main challenge that we face is the implementation. We know what the problem is. We know what the solutions are. We need the national will to implement them.

It is easy to order the military to change. The good news is that the military has shown itself capable of changing. It is the rest of the government that is the main challenge. The State Department, for example, still functions in a world of government-to-government relations when government/non-governmental relations are just as important. It is no longer sufficient to train foreign service officers in just Urdu, the main language spoken in Islamabad, when you have to know Pashtun to effectively operate in the border areas far from the capital. The bottom line is to much more aggressively and faithfully implement the changes that have already been identified.

Having studied terrorism and counterinsurgency for so long, and at least episodically being involved in the implementation, recognizing the solutions is not hard. Implementation is the key. That requires tremendous unity of effort and tremendous will. How long do we want to be fighting the war on terrorism? We do not want to make this the generational struggle that our adversaries have defined it. They have defined this in epic terms precisely because they know they cannot defeat us on the battlefield, but they believe they will fundamentally wear us down. That is the greatest danger and why I concluded that the biggest challenge we face is not only to sustain it but to implement it. I think we already have a good blueprint, though.

Q: *If we send a message to the adversary that we want it to be short-term, what domestic measures should we take to keep our eyes open to the reality of the situation?*

Bruce Hoffman – This is one of the key issues, and this is why kinetics and military force are so appealing; you can measure it. It is demonstrative, and you can assess the effects. Even when I am talking about building up an Internet capacity, these are not as easily measured and are not as amenable to metrics. This is also a key area where we have to build the capacity among our allies and also have a very light touch.

The point is the difficulty with these other key initiatives and approaches that do not just rely on kinetics is that they are not amenable to metrics. That is part of what we have to understand. We are a very metric-driven culture, society, and government. These are long-term approaches that are going to be measured beyond the life expectancy of a presidential administration and pose serious questions of sustainment.

It is critical to have a clear strategy, explain it clearly to the public, and accept that this is not something that can be easily won. Part of that too is looking at the problem of terrorism realistically and more candidly than we have looked at it. A global war on terrorism suggests that there is a single adversary in a single place that we can defeat, as apposed to multiple adversaries in different places.

Terrorism surfaces spasmodically, and this is why it affects us so profoundly psychologically; it is not a continual threat. Six and a half years after the war on terrorism and after 9/11 began, there is a general conception that we have done remarkably well and that we have defeated our adversaries or prevented their ability to strike. As that airline plot shows, one single act can vitiate years of progress.

Part of sustaining the struggle is educating the American public. It is building up the psychological resilience that terrorism is not a threat that can be eliminated, a tactic that can be defeated, or a phenomenon that can be abolished. Yet, it been described all those ways in recent years in the War on Terrorism. We need to accept that it is a phenomena of the 21st century and that we can certainly weaken and contain it, but we cannot completely eliminate it. Therefore, I think when we have realistic expectations, we will not necessarily fall into the terrorists' hands of reacting in ways that, in the long term, are counterproductive. We will not become as susceptible to the fear and anxiety they hope to create.

Q: Thinking about what happened in Madrid and how that affected the Hispanic election, and to the FARC in October 2008, imagine you are on the other side. What are you going to do and where, as a terrorist?

Bruce Hoffman – This, to me, is the biggest challenge right now, and this goes right back to my point about the sophistication of our adversaries information operations. What worries me fundamentally is last year was a banner year for al Qaeda's communications. Al Sahab was basically putting out an audio or a video every three days and produced nearly 100 such releases. That was more than double the 2006 figure.

First, I do not think you engage in that type of activity unless you do not think you have a listening audience and a message to communicate. By the same token, you can only talk so much; you have to back it up with action. What worries me is that, in the past two presidential elections, al Qaeda has made its presence known.

In October 2000, they attacked the USS Colt, whether it did or did not have an affect on the election; nonetheless, I think it was calculated in time, particularly at a moment when they probably realized the administration would be reluctant to do something for political reasons because of the election. Clearly, I think bin Laden's October 29, 2004 appearance was designed similarly to have an influence on the election, at least according to some observers.

There was a *News Week* poll that showed, in the aftermath of bin Laden's appearance, President Bush got a six point lead in what had been a neck and neck race between President Bush and Senator Kerry. When they polled people, they said it was because bin Laden's appearance reminded them of the specter of the possibility of a terrorist attack. In Ron Suskind's book, *The One Percent Doctrine*, he quotes discussions at the CIA that said this was calculated to affect the election.

From the jihadi point of view, we know that they believe they affected the 2004 outcome of the Spanish election. They certainly calculated the timing of bin Laden's appearance. I think even bin Laden's appearance was designed. He did not have a camouflaged jacket and an AK-47. He had robes and head dressing, arguably in an attempt to look more statesmen-like than threatening. Why have we seen in the past year this tremendous upsurge in al Qaeda communications, and what does it mean?

I think that we are entering the most dangerous period, in the run up to the elections. Why are they so active in terms of their publicity last year? I do not have an answer to that, but it is remarkable; we wonder how much an organization can be on the run when they have a media arm that is so active.

Second, they not only were putting out these video and audio tapes but now have multiple lines of communication where they do not even need al Jazeera anymore. They are capable, in multiple redundant ways, of communicating throughout the world in real time and getting the message out. Therefore, you have to ask to what purpose, and is it an attempt to influence the election.

Given their appearances and surfacing in the last two elections, it is not something that I would casually neglect.

1.3 IRREGULAR WARFARE CHALLENGES

Thomas Mahnken

TRENDS AND SHOCKS TO NATIONAL SECURITY CHALLENGES

I want to discuss the challenges that we face, particularly the irregular warfare challenges, and some of the ways that those challenges may evolve over time. We face a period characterized by many diverse challenges to our country. The growth of international terrorism; the development and acquisition of nuclear, chemical, and biological weapons by a growing number of countries; the spread of conflict into space and cyberspace; and the prospect of strategic state collapse all pose novel challenges for decision makers in the United States and across the globe.

The Challenge of Hybrid Wars

For the foreseeable future, the United States, its allies, and friends will find themselves combating violent extremist groups. We will neither be at peace nor fully mobilized for war. Quite apart from Iraq and Afghanistan, this conflict will generate significant

Dr. Thomas G. Mahnken, Deputy Assistant Secretary of Defense for Policy Planning, provides advice on strategy to the Deputy Secretary of Defense and the Under Secretary for Policy. He develops defense-planning scenarios and guidance for war plans. He has served on the Robb-Silberman Commission and the Naval Special Warfare units in Iraq and Bahrain and was part of NATO's initial deployment in Kosovo as a Navy Reserve intelligence officer. Dr. Mahnken was Professor of Strategy at the Naval War College and a visiting Fellow at The Johns Hopkins University Paul H. Nitze School of Advanced International Studies (SAIS), where he earned his M.A. and Ph.D. in international affairs.

demands for forces over the long term. In addition to the long war, we could face a broad spectrum of contingencies, including a variety of irregular challenges in which enemy combatants are not regular military forces.

These challenges include the potential use of weapons of mass destruction and the possibility that an adversary could disrupt our ability to maintain our qualitative edge and project power. Some of these conflicts may start and end rapidly; others may be persistent. In many, the need for combat operations will be paired with the need for stability and reconstruction. To add further complexity, these modes of warfare may appear not only in isolation but in combination. We are thus increasingly likely to face what strategists are beginning to call complex or hybrid wars. Just as we may encounter a spectrum of conflict types, we may face a variety of different adversaries, including insurgent groups, states, and transnational movements as well as coalitions between states and nonstate actors.

Trends and Shocks

I would like to talk about trends and shocks in conflict in the context of the struggle against violent extremism. I am going to address five questions: Is this conflict in fact a war? If so, what is the nature of this war? Given that nature, what is the appropriate strategy? How might this conflict evolve over time? Finally, what will victory look like?

Is this a War?

Now considerable attention has already been given to whether the conflict that we face is or should be termed a war. Those who oppose the use of the label argue, with considerable justification, that the word war implies that violent extremism can be defeated militarily. They also worry that the term could legitimize terrorists as combatants. These points are clearly valid. Success in this conflict requires not only capturing or killing terrorists but also delegitimizing their ideology and redressing the grievances that spawn extremist behavior. Military force has a role to play but one that will generally be subordinate to other instruments of statecraft.

I believe that the current conflict is a war in the classical sense. For both us and our adversaries, it is an act of force to compel an enemy to do our will in pursuit of larger political aims. It is a strange war—a struggle waged by irregular forces with unconventional means. However, because it is a violent clash of wills, it is amenable to strategic analysis—again, very much in line with our goal here to pair strategy with analysis and technology.

The ends sought by the United States are most clearly stated in the 2006 National Security Strategy: to help create a world of democratic, well-governed states that can meet the needs of their citizens and conduct themselves responsibly in the international system. Our adversaries, for their part, clearly see themselves as being at war and are using military force in pursuit of their political aims. These aims include the elimination of groups that do not adhere to their extremist view of the world, the overthrow of what they see as apostate regimes, and the restoration of the caliphate in the heart of the Islamic world. Although there is disagreement among extremist leaders on the priority of these aims and how to achieve them, they have no question that these ends can be achieved only through force.

"Just as we may encounter a spectrum of conflict types, we may face a variety of different adversaries, including insurgent groups, states, and transnational movements as well as coalitions between states and nonstate actors."

What is the Nature of this War?

This is a strange war. This war's heroes attest to its strangeness. They include not only the men and women of the U.S. armed forces and the armed forces of our allies and our partners but also policemen and firefighters. They include intelligence officers operating in remote regions and in urban areas to penetrate and disrupt terrorist networks. They include the London ambulance crew that noticed smoke coming from a parked car and thereby foiled a bombing. They include the numerous bystanders who offered aid to the innocent victims of bombings in Madrid, London, Delhi, Cairo, Algiers, and Amman, among others.

Wars have battlefields, and this war will unfortunately have more before it is over. Some of these battlefields, such as Tora Bora and Fallujah, are rather conventional. A student of mountain or urban warfare would instinctively grasp the problems that commanders faced as they fought these battles. If these locations are battlefields, so too are the site of the World Trade Center, the Bali nightclubs, the Madrid train station, and the London underground. This war's battlefields include bank and financial networks and the Internet as well as the mosques, madrases, and universities where extremism is cultivated. What is the nature of this war? What is the appropriate strategy for prosecuting it?

There have been a lot of catchy descriptions of this struggle. One that is perhaps more descriptive and maybe less elegant is "a protracted global, irregular conflict." Each one of these words helps describe the nature of the war, and each one helps point the way to the strategy we need to pursue to prevail. This war is global in scope. Like communism and fascism before it, extremist ideology has transnational pretensions and is able to draw adherents from across the globe. Like its secular antecedents, extremist ideology offers nothing short of an attack on the international state system. Our adversaries do not recognize state sovereignty, nor do they respect international boundaries. Rather, they exploit our respect for these norms for their own purposes.

Paradoxically, extremists use the very instruments of globalization—the unfettered flow of information and ideas in open societies and the unfettered flow of goods and services, capital, people, and technology. They use instruments coming from the globalization they claim to reject to further their goals. Although driven by a global ideology, our adversaries are, in fact, a coalition of regional and local extremist groups pursuing regional conflicts tailored to the specific circumstances in each region.

Al Qaeda itself grew out of an agglomeration, a coalition of regional extremist groups, and al Qaeda has, in turn, spawned a series of regional franchises, including al Qaeda in Iraq, al Qaeda on the Arabian peninsula, and al Qaeda in the Islamic Maghreb. It also has regional associates, such as Jemaah Islamiyah in Southeast Asia and others. As a result, this struggle is being waged on many fronts—globally, regionally, and locally. Local grievances fuel it, and it thrives in ungoverned, undergoverned, and misgoverned areas. Besides a global struggle, it is also an irrite war—a violent struggle for legitimacy and influence over the population. Hence, the use of force will continue to have a role. More important, over the long term, there will be efforts to build up local forces to deal with extremist groups on their own territory.

What is the Appropriate Strategy?

Military efforts to kill or capture terrorists are likely to be subordinate to political measures to ensure participation in government and economic programs to spur development. For these reasons, arguably the most important military component in this struggle against violent extremists is not the fighting we do ourselves but how well we help prepare our partners to defend and govern their own countries. The indirect approach is central to our strategy. Often, partners are better positioned to handle a given problem because they understand the local geography, social structures, and culture better than we ever could.

In collaboration with our interagency and international partners, we will assist vulnerable states and local populations as they seek to ameliorate the conditions that foster extremism and to dismantle the structures that support and allow extremist groups to grow. By improving conditions, undermining sources of support for extremism, and assisting in addressing root causes of turmoil, we will help states stabilize threatened areas. Countering the totalitarian ideological message of terrorist groups will help further undermine their potency and will also require sensitive, sophisticated, and integrated approaches. It is a global struggle, an irregular struggle, and, finally, a protracted struggle that will last decades rather than years.

How will this War Evolve?

It is hazardous to predict the course of a protracted war. The southern leaders who launched the American Civil War could hardly have imagined that the conflict would end in the defeat of the Confederacy and the devastation of the South. Similarly, the monarchs who launched World War I could hardly have imagined that it would lead to their ouster and the wholesale reconstruction of Europe. History is a strong warning to those who see outcomes as preordained. Still, the study of the past, particularly past protracted wars, points to the elements of a successful strategy. First, coalitions play an important role in determining success or failure. Certainly, coalitions play an important role for us. That is why building the capacity of our partners through military efforts and much broader political and economic efforts is central to our strategy.

Maintaining and building our coalition is key for us. Extremist groups also require coalitions for their long-term success. These coalitions can take several forms. Some involve states. During the 1990s, for example, Sudan and then Afghanistan provided al Qaeda with a sanctuary that they used as a base of operations. Today, we face the challenge of extremist groups using ungoverned and undergoverned areas as safe havens. A main thrust of our policy is to address those safe havens. More fundamentally, al Qaeda itself is a coalition. It is both an international movement and a collection of national and regional movements that have joined forces in their ideological struggle. This protracted conflict will challenge the cohesion of both our coalition and that of our adversaries.

"Military efforts to kill or capture terrorists are likely to be subordinate to political measures to ensure participation in government and economic programs to spur development."

Our coalition problems are often on display on the front page of the newspaper. We need to realize that our adversaries are hardly united. The Islamic world is driven by competing ethnic, political, and sectarian identities. The extremists are themselves on the very fringe of the Islamic world. They face considerable barriers in trying to build and maintain their own base of support. One of the most important tasks facing the U.S. over the long term is to hold together our coalition and prevent extremist groups from expanding their coalition while we work to fracture it.

Just as coalitions are important, so too is public support. Public support is key to our long-term effectiveness, and it is also key to the effectiveness of our adversaries. Military success or failure will win or lose hearts and minds. A successful strategy must provide tangible proof that the side is making progress and will eventually prevail. Therefore, we should seek to deny our adversaries the incremental victories they need to sustain and build their support over the long term. We need to portray our adversaries as losers rather than heroes. Should they prove inept or ineffective, they will lose support.

As I said, protracted conflicts evolve over time, often predictably. In my office, we are trying to understand how this struggle might evolve over time. Our goal is to give senior decision makers the information that they need to consider as they formulate policy and strategy over the long term. Accordingly, we are looking at a variety of trends, not just traditional military trends but also nontraditional trends: demography, governance, culture, identity, economics, the environment, and resources.

With respect to unrestricted and irregular warfare, we see violent extremist organizations continuing for some period of time. These movements and other types of non-state movements will be driven by not just political factors but cultural values, such as the failure to build healthy civil societies and longer term demographic and economic trends.

“History is a strong warning to those who see outcomes as preordained.”

These groups provide one clearly defined form of resistance to the complexity of globalization and the poor governance of some states. Poor governance and the lack of political, educational, and economic opportunity, coupled with population growth that creates youth bulges in key states and migration pressures, will increase the risks of radicalization and instability in strategically important states. How these extremist movements develop, the threat they pose in terms of scale, the resources available to them, and their aims will be influenced ultimately by long-term outcomes, not just in the operations we are currently waging but also developments in neighboring states. It is also clear to us that the agility and resources of some terrorist organizations are operationally greater than those in many developing states.

Many developing states face many different types of deficits, such as a freedom deficit or an economic deficit. Of greatest concern is the security deficit faced by many developing states. Our efforts to build partner capacity and to train and advise local forces are aimed at remedying that security deficit and helping our friends, partners, and allies deal with problems on their own territory.

Globalization is increasing the likelihood of the acquisition of weapons of mass destruction by more states, including nuclear weapons, and it has raised the risk of proliferation to terrorist or criminal groups. We are working very hard to de-stem that threat. The problem is that legal frameworks for addressing the range of challenges posed by non-state actors, not just proliferation, are intrinsically one step behind. Many of the legal frameworks that we have inherited were crafted to deal with yesterday's challenges, not today's. The intersection of trends in conflict with those of energy, the environment, and economic and proliferation concerns creates a series of serious long-term risks that could manifest as shocks to the international system. We are preparing our leadership for the possibility of these shocks, both to prevent them if possible and also to mitigate them if prevention is not possible. Some of the shocks we are particularly concerned about include the potential failure of a strategic state, a major oil shock, and the possibility of a catastrophic WMD attack, particularly involving sites of economic, cultural, and military significance. How the United States and others respond and the ability of a globalized and interdependent economic system to ride out such shocks will have far-reaching implications for the security environment and for our country.

Thinking more narrowly, one way that the long war could escalate—one that has already gotten considerable attention—has to do with the means used to prosecute it. One justifiable concern is that extremist groups could obtain and use nuclear, biological, or chemical weapons. We are certainly focused on preventing that outcome, but the conflict could also escalate in terms of the passions involved. In other words, this war could become a true clash of civilizations, pitting the Islamic world, or a substantial part of it, against the West. Our strategy to prevent that possibility is to work with and through our friends and allies to isolate the extremists from the greater population of responsible law-abiding citizens, both here and abroad. Finally, this conflict could escalate geographically. Just as Afghanistan sheltered al Qaeda in the 1990s, extremist groups could gain a new sanctuary and sponsor, such as Sudan. We are working with our allies and friends to preclude such a possibility.

> *"Some of the shocks we are particularly concerned about include the potential failure of a strategic state, a major oil shock, and the possibility of a catastrophic WMD attack, particularly involving sites of economic, cultural, and military significance."*

What is Victory?

It is my job to prepare for the worst case and to prepare our leaders for the worst case. I would say overall, I am optimistic. Time is on our side. As the ideals of democracy and the positive aspects of global integration spread, they will reinforce moderate voices against extremism and address its causes. Much of what we do and, particularly, what we do in the Defense Department in the short term is aimed at buying time for such progress to take root.

One of the 20th century's most able strategists, Winston Churchill, drew a distinction between short wars and long wars. Speaking in some of the darkest days of World War I, he made a somewhat optimistic note:

> *The old wars were decided by their episodes rather than their tendencies. In this war, the tendencies are far more important than the episodes. Without winning any sensational victories, we may win this war, even with a continuance of extremely disappointing and vexatious events… All the small states are hypnotized by German military pomp and precision. They see the glitter, they see the episode. But they do not see or realize the capacity of the ancient and mighty nations against whom Germany is warring to endure adversity, to put up with disappointment and mismanagement, to recreate and renew their strength, to toil on with boundless obstinacy through boundless suffering, to the achievement of the greatest cause for which men have ever fought.*
>
> *—Speech to the House of Commons, 15 November 1915*

Beyond his soaring rhetoric, Churchill reminds us that in protracted wars, battlefield triumph and tactical success do not bring victory. Something more is needed to achieve ultimate victory. This current war will not end in a single battle or a campaign. Rather, extremism will be defeated through the patient accumulation of quiet successes and the orchestration of all elements of national and international power. The victory will include discrediting extremist ideology, creating fissures between and among extremist groups, and reducing them to the level of a nuisance that can be tracked and handled by local law enforcement groups. Like communism in the early 21st century, extremists of the future will still exist, particularly in the more backward corners of the globe, but they will inspire bemusement rather than terror. Such an outcome is unlikely in the near term. Such a vision is a necessary first step for eventual victory.

Q & A SESSION WITH DR. MAHNKEN

Q: *Can you speak to the question of whether the U.S. Defense Department is offering training and advice to help our partners remedy security deficits?*

Dr. Thomas Mahnken – Those are two different questions. One of DoD's main areas of emphasis is training and advising foreign security forces. We do have that capability; we actually have the capacity to do it. Beyond the Defense Department, however, it is more of a challenge.

We use some of our military capability to advise some foreign militaries and train some foreign police. That really is not our mission, though. There are other parts of the government that are better equipped and have the authority to do that. There is a capacity deficit. We are engaged in dozens of countries every day, largely doing training and advising. It is often below the radar, and we are perfectly happy with it that way, as are our friends and partners. That capacity issue is a major emphasis for the Department and something that we identified in the 2006 Defense Review as a major area to work on.

Q: *Do you think the defense budget is adequate?*

Dr. Thomas Mahnken – I think ultimately there needs to be a political conversation on how much this country spends on defense. What we deal with in the Defense Department is how those resources are allocated. Given that allocation, Secretary Gates has been clear that the Department's capability in the area of irregular warfare is the top priority. That is the conflict that we are waging and will continue to wage.

At the same time, we need to acquire capabilities for the future. Even though this war is our top priority, and it is the war we are waging now, it is not the only type of contingency that we have to face. We certainly work within the budget. Congress has been extremely generous in providing resources. However, we certainly do not plan that that will always be the case moving forward.

Ultimately, our top line is determined by what the Executive Branch, working with the Legislative Branch and considering the views of the American people, believes we should be spending on defense. The good news for waging the long war is that we are not talking about millions of men and women under arms. We are actually taking the most effective approach of supporting dozens of relatively small teams working over a long duration in many different countries. That is not a resource-intensive strategy, and I think it is the right strategy. As the only superpower, our challenge is to figure it out and to prioritize. Part of what we are trying to do by building capacity is building up the ability of our friends and partners to deal with their own challenges so that our involvement will be finite.

The best thing that we can do is to provide our friends and allies the means necessary to police themselves so that we do not have to do it and our allies do not have to do it over the long term.

Q: *Putting aside disagreements that you have about future strategy, what challenges do we still face?*

Dr. Thomas Mahnken – The biggest disagreements have to do with moving forward and thinking for the long term. I do not think there is a lot of disagreement over what needs to go on now. We are fundamentally on the same page. Any disagreements have to do with looking at the future and the extent to which irregular warfare is going to be the top priority. What is the mix of other capabilities that are required and the other types of contingencies that we may need? Those are honest disagreements because the future has not occurred. Those disagreements are, to a certain extent, helpful because they are different points of views.

I do think there is great convergence over the strategy. The challenge is extending that convergence and that consensus beyond the Defense Department and to other parts of the government. We can make too much of interagency conflict. The State Department, for example, USAID, clearly knows what needs to be done, and there are a lot of very hard-working, dedicated folks associated with those departments and agencies who are trying to make that happen.

Just as we operate in a legislative context, so do they. Even when they know what needs to be done, getting the resources from Congress and getting the authorities is a real challenge. Unfortunately, we are going to be facing that challenge for some time to come, not because we want it to be that way but because it is extraordinarily difficult to get this type of change done.

Q: *In war, surprise happens. We might try to use technology to find a way to get through that, but at the end of the day, surprise happens. How we respond is actually important. The question is, how well are we doing in terms of enabling the political leadership to respond to shocks, especially as we transition to a new administration? I think that history shows you that the weak win by getting the strong to overreact. So how do we install the institutional capabilities so that we can transition to different leadership to respond to shocks appropriately? If we respond the wrong way, it could be counterproductive for the long-term goal.*

Dr. Thomas Mahnken – This is the first time since 1952 that a sitting president or vice president has not been on the ballot. That will be a challenge, but it also will pose some real opportunities for the Department.

It is certainly something that we have been thinking about. I will not go into any greater detail than that, but the transition will be key. Ultimately, as of January 20, 2009, the ball will be in the new administration's court. We are spending a lot of time to prepare the next team, more so than in recent transitions.

1.4 INTERAGENCY PERSPECTIVE – 10 LESSONS

Peter Feaver

TEN THINGS A HUMBLE ACADEMIC HAS LEARNED ABOUT THE INTERAGENCY WHILE SERVING AT THE WHITE HOUSE

I have been asked to talk about what I learned about the interagency and its performance in the broader War on Terrorism during my recent tour in government. They are not in order of importance, but here are 10 important lessons that I learned and that many of you probably learned long ago.

Do What You Are Doing

I arrived with something of an outsider's perspective, so the first lesson I want to mention addresses outsiders' critiques. I learned that 60% of the critique of the administration's performance in the War on Terrorism consists of a very strident recommendation that the Administration do what the Administration is trying to do. About 30% of the critique reduces to a complaint about Iraq, and 10% is about torture and related issues.

Professor Peter D. Feaver is the Alexander F. Hehmeyer Professor of Political Science and Public Policy at Duke University and Director of the Triangle Institute for Security Studies (TISS). Previously, he served as Special Advisor for Strategic Planning and Institutional Reform and as Director for Defense Policy and Arms Control on the National Security Council. Dr. Feaver is widely published with several monographs and over 30 scholarly articles on American foreign policy, public opinion, nuclear proliferation, civil-military relations, information warfare, and U.S. national security. He has earned a Ph.D. from Harvard University in political science.

I discovered this insight while at a conference, where I listened to a very long critique of the administration's bad performance in the War on Terrorism and all the things that were going wrong. Then the speaker proposed a very sensible strategy as an alternative, and I said, "That is a very good idea. What you just described is exactly what we're trying to do." When I pressed him on it, he retreated to criticizing Iraq. I said, "What's your alternative now that we're there? What do you propose?" What he proposed was essentially what the administration was trying to do.

NEW DOCUMENTS WILL BE IGNORED

The problem may not be with what the administration was trying to do. The problem may be with what the administration was accomplishing, which leads to the interagency and the performance of the interagency. Before we get there, let me mention in passing my second lesson, which is a variant of the first: When strategy documents are refined to address critiques, people ignore the new documents and go back to the old ones.

I was hired, in part, to work on the revision to the National Security Strategy (NSS). That was one of the few lanes that I owned in my office; much of the time, I was kibitzing on everyone else's work or helping them with their strategies, such as Juan Zarate with the National Strategy for Combating Terrorism, which was a derivative document of the NSS.

The explicit mandate that came down to us for the NSS was: "stay in the President's voice and stand in the shoes of the 2002 strategy but reflect on what we have learned since then and on the new challenges and the new opportunities." The implicit mandate was: address some of the cartoon critiques that had been levied at earlier documents. I think we succeeded; if you have not read the 2006 version, I encourage you to do so. My measure of success is that virtually no critic quotes the 2006 NSS. They always quote the 2002 document.

I was at several conferences where some of the major critics of the administration went on at length. I asked them if they had read the 2006 document because it addresses the very issues and concerns they were raising. They said they had not. I am sure it is not flawless, but it is certainly harder to lampoon. One of the things I learned was that in this business, there is an industry of criticism that has to be served. If you answer the criticism, you have not solved the issue because more criticism will come.

LABELS CAN DRIVE POLICY

That being said, there are still a lot of things that could be critiqued, and this brings me to my third lesson. If you wanted to bring interagency activity in the War on Terrorism to a grinding halt—I saw this happen a couple times—just raise the issue of what we should call this effort—or what we should call the enemy. Before I got to government, and many times since, I participated in countless academic seminars on this very topic. I cannot tell you how many academics I have heard say, "You cannot wage a war on a tactic, and you should not call it a war because that implies the only relevant tools are military."

I assumed that academic benchwarmers were the primary practitioners of this form of debate. It turns out that it also animates those inside. I came face to face with the problem in fall of 2005 when the President wanted to give a speech focusing on the ideology of the enemy and what motivates him. We worked on that speech, and it produced a fur fight that was quite alarming to see. Each department and each intelligence agency had very strong and contradictory views on the matter. Some departments had *several* strong and contradictory views on the matter.

We were told, for instance, that we absolutely could not call the enemy "jihadis," doing so would deal such a blow to the effort that we might never recover. Better to call them "Islamic extremists." Then, the next principal would say, "Whatever you do, you must not call them Islamic extremists because using the word "Islamic" will set our efforts back so far we may never recover." They refused to clear any speech that had the adjective "Islamic" in it. Some even said, "You cannot talk about the ideology of the enemy because it has a religious-based component. We are a secular government, and just talking about it would make the problem worse."

We were stuck until we hit upon a pretty clever workaround. We had the President say, “Some call this evil Islamic radicalism. Others call it militant jihadism. Still others call it Islamo-Fascism. Whatever it is called, this ideology is very different from the religion of Islam.” In other words, we mentioned each label once, addressed the religious issue head-on, and then we moved on to discuss the ideology and what we were trying to do.

I am not trying to ridicule terminological precision. I am an academic after all. I understand that definitional debates are the lifeblood of many peer-reviewed articles; in my experience, however, it has rarely led to different operational (leave aside communications) policies. I have yet to find anything in the War on Terrorism that we are doing primarily because of the label that we have given the conflict. Put another way, there is nothing that I wish we were not doing that we would stop doing if only I could get folks to label it differently.

I understand the communications challenge of labeling, and I am very aware of the problem of making a problem worse by using terms that are offensive. Should that drive policy? More importantly, should that paralyze policy? I do not see it. There are many legitimate policy debates in the War on Terrorism, and we should focus our energies on them, not on this endless labeling exercise.

GIVE AN ISSUE A HOME

I call my fourth lesson “Feaver’s Iron Law of Interagency Operations.” If no one owns an issue, everyone will be working on it. If everyone is working on it, no one really leads it, and it is not really getting done. That is a sad truth about the war of ideas part of the War on Terrorism. The President deserves a lot of credit for identifying that component from the beginning, almost within hours of the start of the war. The early message coming out of the White House recognized that this conflict is a war of ideas, not just a battle of arms.

However, implementing a war of ideas is very hard. One of the hardest parts of the War on Terrorism is to execute the war of ideas as vigorously as we need to. This issue will be a major priority for the next president.

There are many reasons why more needs to be done in this area, but one of the major reasons is that this is the quintessential interagency mission. No one has the lead for the war of ideas. There are people who have the lead for portions of it, like the Undersecretary for Public Diplomacy, who had the lead for public diplomacy but not for the entire war of ideas. Public diplomacy is just one piece of it. Others who might logically have the lead do not because of its operational nature. There is resistance to making the National Security Council (NSC) operational. That is one of the lessons of the Tower Commission.

When there is no natural home for a job, no one does it, and everyone plays. Just tally up all the people who are working on a piece of this business. Everyone plays, but no one has the lead; there is still much more to be done.

STAY IN YOUR OWN BACKYARD

This leads me to my fifth law, which I will call "Feaver's Iron Law of Interagency Competence or Incompetence." It says that interagency players find it very hard to contribute based on factors within their competence because they find it very tempting to contribute based on factors outside their competence.

I wish I had a nickel for every time someone—usually in DoD—would tell me quite confidently what Karl Rove was advising the President in terms of political issues. I think we have taught Clausewitz too vigorously in our war colleges because all the graduates would follow the Clausewitzean dictum about war being the continuation of politics by other means and then tell me exactly what Karl Rove was thinking. They almost always were wrong. I would also have State Department types tell me that they could make pretty confident assessments about what the American people would and would not stand for. Their judgments, policies, and recommendations at the interagency meeting were also based on those perceptions, or the Joint Chiefs of Staff (JCS) would seek to adjudicate a risk rather than measure it—for example, Title X concerns about raising and maintaining a force versus combatant commanders concerns about winning a war. The idea of the interagency is to bring people with specific competencies to the table so that everyone has the benefit of hearing what they have to say. At its most dysfunctional, the interagency can blend incompetencies, with everyone playing in someone else's area.

EVERY STRUCTURE WORKS FOR SOMEONE

This brings me to my sixth law: every dysfunctional structure or organizational setup is functional for certain powerful players in the bureaucracy. There will inevitably be a buildup of inertial interests behind the existing structure. In other words, the structure exists because that is how interests have wanted it. The virtuoso bureaucratic players have figured out how to make the system work for their interests.

The structure is working for them, and the structure is reflecting powerful interests over time; otherwise, it would be changed. Even if you are a victim of a dysfunctional structure, you have to recognize that it is probably functional for somebody and for somebody who matters.

INTERAGENCY REFORM REQUIRES CONGRESSIONAL REFORM

A lot can be done to improve interagency effectiveness on the margins. However,—and here is my seventh lesson—dramatic change will require congressional reform.

Let me explain why. The President has taken the lead in many important reforms in this area. Institutional reform in the interagency is important, and while it can certainly be improved on the margins, the NCTC itself represents a substantial improvement over what we were doing before. There is good work going on in linking the national implementation plan to the Office of Management and Budget (OMB), which is the next natural step in the progression.

That reform is continuing. There have also been reforms at the White House to the Homeland Security Council, the Homeland

Security Advisor, the Counterterrorism Security Group (CSG), and the Policy Coordinating Committee on Terrorism Finance (PCC-TF). All of these areas represent improvements over the processes or functions in place before 9/11. We are close to the point where dramatic improvements will require reforming Congress.

I say reform *of* Congress, not reform *by* Congress. Congress has been fairly assiduous in seeking to reform the Executive Branch. The Office of the Director of National Intelligence (ODNI), the Department of Homeland Security (DHS), and many of the organizations represented in this symposium are proof of that reform. Yet, Congress has been less enthusiastic about reforming its own operations and processes—understandably so because they understand that all reforms of the Executive Branch produce unintended consequences that are tough to deal with.

The deeper problem—which relates to my sixth law—is that existing functions that may not work well at the interagency level do work for others. Any reform of Congress at this stage is going to take power away from powerful members of Congress and perhaps divide it up in new ways. That change is going to be very hard to implement when those reforms would have to go through the very committees on which the powerful people serve.

MAJOR REFORMS WILL SQUASH MODEST REFORMS

It might even reduce an individual legislator's power vis-à-vis the Executive Branch, bringing me to my eighth lesson: whom the gods would destroy they first make interested in grand interagency reform efforts.

One of Secretary Rumsfeld's rules was that if a problem looks intractable, expand it. He probably regrets listing that rule because it is too easy to parody. Most people who have thought about interagency reform embrace the logic of Rumsfeld's rule because they recommend a very grand Goldwater-Nichols-level reorganization for the interagency. A lot of very good work has been and is being done in this area. I am confident that Jim Locher [Executive Director of the Project on National Security

Reform] and his team are going to produce a very high-impact study. Locher and the Project may also be our best chance of producing ideas that will result in reforms of Congress, which is a very important development.

I worry, however, that focusing on the largest of the problems and the largest of the solutions will allow more modest reforms to languish that could be implemented now. Some of them are being pursued right now; the next administration will likely put some of them in place. Even the best-designed plans will have to overcome some the stubbornness that underlies most of the efforts towards better interagency functioning.

MORE PERSONNEL – GREATER EFFECTIVENESS

I come to lesson nine: to make a lasting change in a department's effectiveness and, therefore, its ability to function in the interagency, it must have more resources—specifically, personnel resources.

Let me illustrate this point with the effort to improve interagency strategic planning. I have looked at most of the proposals to further the process, and the only ones that seem promising are the ones that provide for more resources so that more personnel can be devoted to the effort, and more importantly, so that, with their increased capacity, agencies and departments can take operators offline to work on strategic planning. The most glaring flaw in interagency planning is the seemingly unbridgeable divide between the level of strategic planning done in DoD and the level done everywhere else.

"The most glaring flaw in interagency planning is the seemingly unbridgeable divide between the level of strategic planning done in DoD and the level done everywhere else."

If you have ever participated in any interagency strategic planning, the divide is scary. It is due to many factors. Some of it is cultural. The raw materials of DoD are weapon systems, which cannot be judged until about 10 or 15 years out. The raw material at State Department is diplomatic engagement, which is obsolete before the cable is written about it.

A big part of the problem is that DoD is structured to function at 90% of personnel end strength. There is a 10% float that has time to go to the National War College or on other assignments. The State Department, however, is designed to operate at 115% of end strength, so they are always short-handed. They do not have the time or the people to go offline to develop new skillsets or spend six months on a strategic planning exercise. When we would ask for State people to participate in a contingency or planning exercise, they would say: "Okay, which embassy do you want us to empty? Which country desk should we stop monitoring?"

The resources problem is a very important part of the strategic planning problem and many of the other interagency coordination challenges.

PERSONALITIES MATTER

Here is my last lesson: personalities and relationships matter as much as formal lines on the organizational chart.

I am a card-carrying academic, political scientist and proud to be one. I am sorry to report that most of our theories assume that personalities do not matter. Yet it is painfully obvious to anyone who has worked in government that personalities matter greatly. Consider the formal organization at the State Department, for example. It has not really changed much over the last 10 years. There have been some organizational chart changes, but by and large, the formal bits that govern the State Department's interactions with the interagency are those that prevailed during the tenures of Secretary Christopher, Secretary Madeleine Albright, Secretary Colin Powell, and Secretary Condoleeza Rice. However, the functioning of the Department was very different under each one of those secretaries.

The State Department is always the State Department, but the operation's effectiveness, as measured by its ability to prevail in interagency disputes, has varied widely over those four secretaries. Many of you have been in the business long enough to know that their capacity to prevail in policy and coordination has varied as well. Yes, the organizational chart matters, but what also matters is whether the secretary has private calls with the President. Is the secretary a legitimate candidate for a national office? Is the secretary able to work closely with the other principals? Is the secretary feuding with one of the other principals? The factors that are personality-driven or relationship-driven matter as much as the organizational chart.

It reminds us of the consequences of elections. Elections not only bring in different governing philosophies, but they also juggle the relationships at the top level. You get a different lineup of personalities and a different lineup of relationships that will matter. GWOT is the ultimate interagency mission that makes a mockery of interagency stovepipes; ultimately, it can be managed only by one interagency actor, the President. In the final analysis, the President is the only one that has the clout to really take charge of the War on Terrorism. I will make a very confident prediction: whoever wins in November will make some mistakes, will get some other things right, and will depend very greatly on a diverse counsel.

Q & A SESSION WITH DR. FEAVER

Q: *Supporting the Global War on Terrorism seems to be a relatively new activity of the Department of Homeland Security. What is the DHS relationship with some of the old graybeard State and Defense people? Or is it too new to figure out how they are going to interact?*

Dr. Peter Feaver – There is a debate about the DHS function in this business and the wisdom of DHS reform. This was the kind of reform that made sense in peacetime, when there would be a lot of time to deal with all of the startup friction. It could be done only in wartime when the urgency would overcome the bureaucratic resistance. So you had this paradox of a reform that probably should not be done in a war but could only be done in a war.

We have seen both of those results. DHS has had a hard time reconciling the competing cultures of the subordinate agencies folded into it. It has gotten better as time goes on, but it is a daunting challenge to blend agencies and departments whose principal focus may be internal, domestic, and not even national security-oriented (like Health and Human Services) and have them play well with agencies that have a very different organization.

The gap that I mentioned between DoD and State on strategic planning applies in spades to these other organizations that are more in the DHS orbit. As rough as you think it is to coordinate interagency strategic planning with, say, the State Department, try doing it with an agency that has a totally different organizational culture and mandate and for whom national security is not the first, nor the second, nor the third thing that drives what they are doing in their agency.

For Homeland Security to function correctly, you have got to get all those players on side. That has been a real challenge. It has been handled better than some of the doomsayers predicted it would, but as Hurricane Katrina pointed out, there are still a lot of coordination challenges, both within DHS and with outside agencies.

Q: *In the State Department, people have jobs even when they are between assignments. In the rest of the government, you do not have a job unless you are filling a slot, so you cannot have a float unless you create fake jobs for people to fill with civil service competition. Assuming that you are going through reform, how would you do it?*

Dr. Peter Feaver – One of the guys I worked with said that on my tombstone he was going to put the epitaph, "It's worse than that," because I would say that at every internal meeting – apparently that was my contribution. What you are telling me is that the problem of interagency strategic planning is even worse then what I had described, and you are right. I do not want to punt back to Congress, but this problem cannot be solved in the Executive Branch.

It probably took decades of Cold War experience, but DoD appropriators understood that it is functional for the U.S. government to have float that allows people to do training and development. Other appropriators do not have that same view or do not see the same mission or make politically understandable calculations that the money can be better spent elsewhere.

It requires a conversation with Congress, and not just a conversation—it requires leadership from Congress that changes their view of what float means. Is float bloat? If it is seen that way, it is never going to fly. If float is seen as functional, it might. One of the initiatives in the last year or two was to set up new national security education that was designed to migrate out some of that which worked in DoD. That is slowly happening, and there is certainly leadership on the Hill in the authorizers' committees.

The authorizers' committees understood it. The challenge is getting the appropriators to take the same view. It may take a change in parties, or it may take one party holding both chambers and the Executive Branch. Maybe this reform will be one of the outcomes of Jim Locher's project. I hope it is because I think that this would go further than almost any other reform you could imagine to increase interagency capacity. I do not have a good answer, but I applaud you for identifying that it is worse than that.

Q: What is the project Jim Locher is working with? I am not familiar with it. Can you describe what that is? Is it the Project for National Security Reform? When you mentioned the need for congressional reform, were you thinking they have to realign their committees and minimize how much jurisdiction there is?

Dr. Peter Feaver – Yes, that is the project. Jim Locher was one of the Congressional staffers who worked on Goldwater-Nichols. He has been one of the leaders on the outside who said post-9/11that all of the challenges that we have seen and have talked about at this conference require a deeper reform of the interagency than has ever been done thus far. He has a very large effort that involves all of the usual suspects, and some of the experts in this room are probably working on it. The goal is to have something deliverable in time for the new administration and the new Congress. [If any one wants any more information on it, their website is: www.pnsr.org.]

I do not know what they are going to say about Congress. Previous studies have shied away from that because if you want to sell the rest of your proposal to Congress, you do not lead with reforming Congress. I think Congress has to invest in staff so that they develop the bench and the capacity to do effective, sustained oversight on policy.

Some members have excellent staffs, and other members have other priorities. Imposing staff increases would be hard. That is one piece of it. Another piece is the multiple jurisdictions and the prevalence of earmarks—for example, foreign aid reform. The administration made a heroic effort on foreign aid reform and took several cuts at it, but it was hard to get around the earmarks.

A significant portion of the foreign aid budget is earmarked for various areas. It is very hard to do strategic planning and strategic prioritization when large chunks of your pie are already earmarked. It is not just jurisdictional reform; it is also practice or behavioral reform that would free up earmarks. Some of my best friends are Congressional staffers who write those earmarks, and they tell me the administration could do a better job of presenting a sustained and coherent strategic plan. There is another side to it, obviously. But I believe that earmarks would have to be relaxed a bit to improve some of what I am talking about, though.

Q: *What is your opinion of proposals regarding transforming the State Department and their responses?*

Dr. Peter Feaver – You have to deal with the organization that you have. The better part of wisdom begins with accepting that State Department is here for a reason. Its culture is there for a reason, and Schumpeter's creative destruction and starting from scratch is not an option. Many times, people have said that we need to get rid of the State Department and the Defense Department and have a new one that is built on the Potomac. The reality is that the State Department is what it is.

I am more of an incrementalist. I believe that you can improve things at the margins with more resources that are identified or restricted for certain purposes and reform the organization without creating antibodies inside it that outlast and kill the reform effort. That is my concern with really dramatic reform. It produces such a countervailing set of reactions inside an organization.

I was engaging in hyperbole when I said that there has not been change since Secretary of State Warren Christopher. There has been. Rice has had an initiative, Powell had a major initiative, and certainly it was a priority for Albright as well. Christopher would say he was improving it. Each secretary comes in and implements some reforms. Often, they are constricted by resources. Rice has gone a long way in shifting priorities within constrained resources—away from the seventeenth assignment in Paris—towards higher, more urgent priorities.

I am of the view that more resources would make all of those reforms happen faster and more easily. I do not think some of the more dramatic reforms that Speaker Gingrich was talking about would work.

1.5 HOMELAND DEFENSE

Stephen Flynn

On September 17, 2001, I had the opportunity to go to Ground Zero, where efforts had moved from rescue to recovery operations. I spent the morning talking to many people on the front lines. Then I went over to the National Security Council (NIC) for their first program event since 9/11. We called it a town meeting and opened it up to talk about 9/11. They invited me, still a Commander in the Coast Guard at the time, to sit on the panel. It was chaired by a very distinguished diplomat and another senior former Defense Department official, a former Station Chief from the Central Intelligence Agency (CIA).

There was standing room only—about 350 people were squeezed into a space designed for about 225. We talked about the state of the Middle East, issues of terrorism, and issues involved with peace in Israel. Then the moderator, the distinguished diplomat, said, "Commander Steve Flynn is on a panel with us today. Steve, we're running a bit tight on time, but I understand you work homeland security things here, and we would like you to

Dr. Stephen Flynn is the Senior Fellow for National Security Studies at the Council on Foreign Relations. He is a Consulting Professor at the Center of International Security and Cooperation at Stanford University, a Senior Fellow at the University of Pennsylvania, and a member of the Marine Board of the National Research Council. Dr. Flynn spent 20 years as a commissioned officer and commander in the U.S. Coast Guard, served in the White House Military Office, and was director for Global Issues on the National Security Council. He holds a Ph.D. and M.A.L.D. from the Fletcher School of Law and Diplomacy and a B.S. from the U.S. Coast Guard Academy. Dr. Flynn was awarded the Legion of Merit. He is the author of The Edge of Disaster: Rebuilding a Resilient Nation and America the Vulnerable.

talk." It was an extraordinary, surreal experience for me—first being at Ground Zero and then, only six miles away, watching this community spend the next hour and a half talking about the Middle East when we had this event right here that might bear some scrutiny.

My opening statement was just that. I said, "I suspect the reason you all came here today was not a sudden urge to talk about the state of the Middle East or what's going on with U.S.–Pakistani relationships. I suspect the fact that there is a very big crater just a few miles from here that may have directly or indirectly affected many of your friends and relatives is probably what motivated you to be here." How is it possible that the best and brightest of the foreign security establishment could go on talking about events overseas without acknowledging this reality right in our own front yard? I said, "Your problem is you are programmed that way. You are programmed to think about any problem that affects our security as something that can be managed beyond our shores and that we cannot or should not try to manage here."

That mindset, I am afraid, is what I still see despite the passage of time; it is a core reality of how we are struggling with this problem. The conventional national security community, the intel world, the armed services, and so forth are very much focused on this problem.

THE LESSONS OF 9/11

What is going on here? I suggest that we really have not thought through some of the central lessons of September 11th. At its essence, and with the benefit of hindsight, there are three lessons that we could have taken away from that day. The first—which I would argue we overlearned—is that there are very bad people out there who are willing to bring their battle here. The second lesson is that the new battlespace is in civil economic space. Our current and future adversaries are most likely to confront U.S. power within the civil society and critical infrastructure arenas, most of which are global so they do not necessarily have a home base. All have a transnational character, making a divide between domestic and international rather silly in functional terms.

The Unlearned Lesson

The third lesson—almost an entirely unlearned lesson of September 11th—is that the only way we will be successful at safeguarding that civil, economic space and addressing the risks associated with an adversary who wants to exploit that space is to engage as many participants as possible in the enterprise. That is the core unlearned lesson, moving towards the seventh anniversary of September 11th.

What is so remarkable about that unlearned lesson is that we got the wrong narrative out of September 11th. The dominant narrative we took away from September 11th was what happened on the first three planes—the planes that took down the twin towers and the plane that sliced through the Pentagon. I argue that the dominant narrative should have been what happened on United 93, the fourth plane. On that plane, the terrorists were cocky enough to let the passengers grab the phones in the backs of the seats and find out what the people on the first three planes did not know—the planes were going to be used as missiles.

"The almost entirely unlearned lesson of September 11th—the only way we will be successful . . . is to engage as many participants as possible in the enterprise."

Armed with that information, they did something really important. They intercepted the hijackers and prevented the plane from getting—almost certainly—to our nation's capital and quite probably to Capitol Hill. Think of the irony: our government, which we constituted to provide for the common defense, was, on September 11th, defended by one thing and one thing alone—alerted, brave, everyday citizens. In other words, the seat of government was protected by the people. All they needed was information, which we were not inclined to share pre-9/11 and still resist sharing post-9/11. We are not just avoiding the narrative of the first three planes; we are saying—and this is a great disservice to the people on United 93—that they were victims.

Our national security apparatus has to do whatever it can to protect the American people from such an event ever happening again. Think of it the way that Steve Bloom, the head of the National Guard Bureau, put it: imagine if we had the intelligence that United 93 was heading for the Capitol. Where would we be today if we had shot that plane out of the sky, killing all those innocent Americans on board? It would have created a very serious challenge for our democracy, whose core mission is to protect its citizens. There is a pretty tricky set of issues there.

THE VALUE OF ENGAGEMENT

The citizens themselves solved the problem. That is a lesson that I think this community really needs to absorb. How do we begin that process? We look to this need for engagement. I want to make the case that there is a strategic value for engagement, there is a tactical value for engagement, and there is just good old common sense civic value for engagement.

Strategic Value of Engagement

Here is the strategic value. The general assumption has been—certainly the publicly stated one—that there is no way to deter the bad guys. We are just too open; there are too many targets; basically, they are nuts. Whatever the case, the core argument here is that they cannot be deterred. I think that premise needs some rethinking.

"Think of the irony: our government, which we constituted to provide for the common defense, was, on September 11th, defended by one thing and one thing alone—alerted, brave, everyday citizens."

From a military standpoint, the adversary engages in catastrophic terrorism not because he thinks he can destroy the United States in any direct way. It is simply too big a country with too many people and too much infrastructure. The biggest danger comes not from what terrorists do to us but how we react to what they do to us and the cost associated with that reaction.

Therefore, their incentive for trying to implement a catastrophic scenario on U.S. soil is to get a big bang for their buck.

If we reduce the bang for the buck, we take away the incentive for engaging in catastrophic terror. If I am an adversary committed to confronting U.S. power, and I could do that in a number of places around the planet, why would I do it in the homeland where there would be a heavy logistics challenge? I might attack the homeland because I thought I would get a big bang for the buck, but if it is a fizzle, its strategic value is somewhat diminished.

Now, how can we remove the incentive for attack? First, we need to remove the most basic element of terrorism—its use as a tool to create overreaction. It is an effective tool, of course, because it exploits fear. Fear always comprises two elements: first, an awareness of vulnerability that was not present before and second—and most critical—a sense of powerlessness in dealing with that threat of vulnerability.

In the broader sense of civil society, Americans pre-9/11 were blithely going along, never imagining that planes could be used as missiles. After 9/11, there was a sense of powerlessness, which often leads to overreacting. Threat vulnerability is almost an educational issue, like the classic story of the child who did not know not to put his hand on a hot stove. Just as we do with our children, we need to educate society about the threat and then also empower it to be able to handle that information. Many of us have experienced that sense of powerlessness, if not personally, then certainly within our family—for example, in the case of a serious illness. The universal response is emotional at that stage, even when the illness turns out to be chronic, not terminal. When support, information, and treatment are provided, people regain their lives.

At a strategic level, we as a nation are currently far more likely to overreact than we were on September 11th. We have essentially stoked the sense of threat and vulnerability while giving Americans virtually nothing to do, almost ensuring that they will overreact in dysfunctional kinds of ways. Empowering by both sharing information and engaging with civil society is the key to dealing with the strategic appeal of catastrophic terror as a weapon of choice by our adversaries. I call this idea the notion of resilience. We need to build a more resilient society that is informed about what may go wrong and has the capacity to manage its way through that vulnerability.

Tactical Value of Engagement

The tactical level is illustrated and highlighted by 9/11, especially United Flight 93. The lesson here is that there are not enough frontline national security players to effectively police the civil economic space where the problems are most likely to emerge. For a long time, we have said that the solution was going to be in good intelligence. I suspect that it is going to be another decade or more before we get really reliable tactical intelligence. Right now, we are confronted with the reality that adapting our national security apparatus for this new threat is a work in progress that has a long way to go. These tools will run up against sheer numbers and limits, given the nature of the adversaries.

We need to draw on a few more people in that space than the professional apparatus that we have. The current situation is part of the legacy of the Cold War. During the Cold War, the security of the many was in the hands of a few. Dealing with that truly existential threat, given the nature of the adversary, required an incredibly closed and what evolved into a paternalistic system. The national security, law enforcement, and intelligence communities are having a difficult time coming to grips with the terrorist threat because it is likely to be domestic, and we are the first responders.

Civic Value of Engagement

Finally, the threat is a civic one. What we have told our young men and women in uniform, who continue to make the ultimate sacrifice beyond our shores to confront this threat, is that you have to do whatever it takes over there because we are so damned vulnerable here. We must make the case to our society that the least we can do to make this fight sustainable is make ourselves less vulnerable. We can engage and do what we can on the home front. I recommend to you the Ken Burns World War II series. It shows the juxtaposition of what was happening beyond our borders and inside our borders.

There is no downside to engagement. It is not an act of paranoia or pessimism to engage Americans in the very real hazards that confront us. It reminds us, in fact, that we came together as a community, as a nation, in the first place because we could not fend entirely for ourselves. We have to rely on neighbors, we have to rely on our emergency responders at the community level, we have to rely on the Red Cross, and we have to rely on our national security apparatus at the end of the day. We also have to be more self-reliant as a people to be better able to wrestle with this threat.

"We need to build a more resilient society that is informed about what may go wrong and has the capacity to manage its way through that vulnerability."

RESILIENCE

The broad concept I am trying to advance is moving us away from security, with all its associated absolutist qualities, and towards this concept of resilience. The core appeal of talking about resilience is that it draws on a big part of the DNA of the American nation. The folks who landed on the shores of Virginia and Massachusetts did not do so because it was an exercise in comfort. They were taking on a wilderness to pursue an opportunity. In most cases, there was a lot more challenge and adversity than opportunity. As an outgrowth of challenging that adversity, they created a spirit of optimism and confidence that they could take whatever came their way as a nation and improve it tomorrow.

Marching across the frontier, dealing with other great national calamities in our history was never done with We the People on the sidelines. We drew from that national character the sense that we can and must succeed if we were going to leave for the next generations the kind of opportunity that we ourselves were blessed with.

Robustness and redundancy

Let me define this notion of resilience very briefly in four terms. Resilience is first building robustness in critical areas, such as infrastructure or networks like public health and emergency management—the systems that we need when things go wrong. Robustness comprises an element of hardening, as with structures, and redundancy. Hardening means designing systems that will withstand unexpected forces. Redundancy means that we do not have all our eggs in one basket, which is what works best for networks. We cannot harden the networks, but we can create ways for them to bend and move.

Resourcefulness

The second part of resilience is resourcefulness. Resourcefulness is basically crisis management: the ability to recognize and understand an unfolding situation, take early action, and communicate with players. A lot of that depends more heavily on human capital than it does on technology.

Recovery and Review

The third element of resilience is rapid recovery. Critical systems have to be back up and running. Recovery is the mechanism that fixes whatever was broken and enables us to move on. The last part is review. Learn from what has happened. Review becomes essentially a feedback loop; talking about what we need to do as a nation in terms of resilience should sound a lot like what we talked about in broad terms with respect to notions of security and defense.

ENGAGE WE THE PEOPLE

Unfortunately, most of our idea of resilience has been built around hardening things up front—jersey barriers and so forth. We certainly talk about the need for recovery and response but not much about learning from the past, even though we need to draw on those skills. Building a more robust society with adequate levels of redundancy and resourcefulness and working our way through recovery requires an open and inclusive process, in contrast to the security world.

None of that capability can be developed unless we bring as many of the stakeholders as possible into the process. I want to go back to the psychology of terror: drawing people in sheds light on what seems perhaps a very amorphous and very frightening reality like that monster in the closet. You demystify it by giving people things to do, informing them, and engaging them in a participatory way.

Ultimately, we should make the threat that terrorism may pose for our society far less damaging results. In the civic context, it is part of what we should do as a nation at war. We need an open, inclusive process to build the robustness that is required, and the civic process is also necessary to stem the psychological damages of engaging terror. All that requires a much more ambitious agenda and a different kind of agenda than the one we have been pursuing for the last six and a half years.

"I do not think [the American people] will be as forgiving the next time around because we have basically told them an untruth. We have said everything that can be done is being done to make them safe and secure. All of us in this business know that essentially is nonsense."

I hope we have the benefit of being able to reflect on those years without another catastrophic attack and to make these adjustments. There are some who insist that it will take another major attack for us to get this right. I am very apprehensive about that possibility. While I think the American people were enormously forgiving of the government and the national security apparatus on September 11th, I do not think they will be as forgiving the next time around because we have basically told them an untruth. We have said everything that can be done is being done to make them safe and secure. All of us in this business know that essentially is nonsense. We raised the bar too high. When something happens, as it inevitably will, and it comes under the media spotlight, we will find that the most basic things have not been done—community command centers that have no ability to control the ventilation, generators in places where they will be buried under water if the water rises a little, no way to give showers in New York City in February to people who have been exposed to a dirty bomb. These are all the nitty gritty kinds of things that we really have not even broached here. They will create a backlash by the American people that can endanger the social contract. I do not care if there is a Democrat or Republican at the driver's seat; there is a much more severe risk here.

Let me conclude with this wisdom, which is stolen like virtually every bit of good insight. My thievery comes from a very able young lawyer, who ultimately rose to be the President of the United States—Abraham Lincoln. In his first public address, he followed the custom of the time of introducing himself to his neighbors by giving a speech. The address was given 50 years after the establishment of the Republic, and he wanted to talk about the risks to the Republic. In what is known as the Lyceum Address, delivered on January 27, 1838, he said:

> *At what point shall we expect the approach of danger? By what means shall we fortify against it? Shall we expect some transatlantic military giant to step the ocean and crush us at a blow? Never! At what point then is the approach of danger to be expected?*
>
> *I answer, if it ever reach us, it must spring up amongst us. It cannot come from abroad. If destruction be our lot, we must ourselves be its author and finisher. For as a nation of free men, we must live through all time or die by suicide.*

Lincoln was reminding us of our national faith, our national religion; the principles on which this great nation was founded are eternal. Therefore, the only way they can truly be endangered is not by an adversary who confronts them but ultimately by our losing faith in them. If we remember the words of Lincoln, we will win this battle in the long haul, but we will certainly lose it if we lose sight of the imperative to engage We the People as we move forward with this very challenging world.

Q & A SESSION WITH DR. FLYNN

Q: *Where do we invest, particularly with respect to homeland security?*

Dr. Stephen Flynn – We should invest in critical infrastructure and so forth. I gave a roadmap with my definition of resilience—robustness, resourcefulness, recovery, and ultimately response. I certainly would say that resourcefulness, recovery, and learning lessons are not high-cost items. They are capacity items that address the communities to be organized when things go wrong and the ability to coordinate with other players who can provide support.

That means basically getting a lot of adults in the room and working our way through the classic coordination issues that the military has refined. That coordination does not exist, with some notable exceptions like the wild fires in California where we saw how well these cross-community agreements can work. They spread capacity to deal with even an isolated town in Southern California.

When we actually look into hardening or the redundancy argument, it is not as costly as it may appear. Here is an example I like to use: how would you protect the Alaskan pipeline? It is an important piece of infrastructure. If it is disrupted for a period of time in the winter, we have lost it—the oil gels and sticks forever, and we would have to replace it. How do you protect it? The traditional model would be to string a lot of troops in foul weather gear along the length, which would be expensive. An alternative would be to have a backup pipeline, which would also be very costly. Another way to recover quickly if somebody took out a piece of it is to preposition pipe up and down its length and have rapid-recovery teams available that could quickly respond. What incentive would the adversary have to blow up a piece of the pipeline in the tundra if he knew the actual impact was nonexistent? When you think about protecting that network, it turns out that there are relatively low-cost or reasonable-cost measures that might serve to deter attack.

At its essence, though, recovery really is something that we can do in this society but have not done yet, in part because of the failure to engage. What we should do is ask state and local officials for a must-do list that goes to a Base Realignment and Closure (BRAC)-style commission of folks informed by the National Academy of Sciences, American Society of Civil Engineers, and so forth. They review the items that are critical and assess reasonable measures that could be put in place to safeguard them.

If we cannot protect them, maybe we need to invest in redundancy or other kinds of tools. Who pays for it? At the federal level, we argue that we are not familiar with many of these items. The private sector owns 85% of them and should take care of protecting them because we are consuming a lot of resources by taking the battle to the enemy.

When you actually get into the nitty gritty of this issue, the private sector has a hell of a problem because nobody owns all of the pieces of infrastructure. I may work very hard to fix a piece of the network, but if someone does not protect the other part of the network, I am putting myself at a competitive disadvantage without actually providing much value.

We must agree on some standards overall and on how we are going to go forward. It is nonsense to say that everything is vulnerable. There is actually only a small list of things that could kill a lot of people and profoundly disrupt our society. So let us take a deep breath, get a handle on those, and make these prudent investments. For the sake of comparison, we are spending about $300 million a day in Iraq, maybe even more, while the total amount of money that has been invested in security for the Port of New York/New Jersey since September 11th and in all the critical operations there, like refineries, is just over the $100 million mark this year. In other words, the cost of every eight hours in Iraq is what we have spent to date safeguarding the port of New York/New Jersey.

I can push the divide even further with the disconnect between the national security and homeland security worlds. We are spending more money protecting the Port of San Diego than all the other West coast ports combined because that is force protection. L.A./Long Beach brings in 43% of all the containers and 50% of all the energy west of the Rocky Mountains. If I am an adversary in Southern California, do I go south to San Diego or do I go to L.A.? By hardening the Port of San Diego, we created an incentive for the adversary to go to L.A. because the pickings look a little more promising there.

The Department of Defense, in carrying out its mission, is making civilians and critical infrastructure softer targets. Not intentionally but as an outgrowth of processes, we are focusing on our lanes and protecting our assets, and it is the job of somebody else, who remains unnamed, to take care of the rest. There is no analysis that has looked at that tradeoff issue in the six plus years since 9/11.

Q: *How do you build psychological resiliency in a civil society whose view of the world has increasingly become that any aberration is somebody's fault instead of accepting that things happen and we have to work our way through them?*

Dr. Stephen Flynn – It is really the heart of the issue. The answer, in part, is that the media are not part of the problem right now. The big screen and little screen create the illusion that we are very brittle and that we all panic and act like screaming hordes of movie extras when something goes wrong when, in fact, that is not what happens. Mostly, the initial reaction is denial; people freeze. Then, they start going through a decision-making process about what to do next. Because it is an undisciplined process, they work through about 100 options when there are only two: duck or run. Then they act based on those data.

The problem is that most of us will not have enough time to survive between the denial and the decision about what to do. What we really are doing when we give people these tools is to compress their ability to manage those events. My pitch is that for the vast majority of Americans, there is a more probable, in most cases certainly more consequential, risk than al Qaeda. It is called Mother Nature. Ninety percent of Americans today live in a place at moderate or high risk of a major natural disaster. We cannot prevent those. We can mitigate them, but we cannot prevent them. Let us mobilize Eisenhower-style around the notion that civil defense is a part of how we are building ourselves towards this goal. We need investment in infrastructure to accomplish this goal in true Eisenhower fashion.

We do need to target the young. I am actually working with some folks on this, and one of the lines we are considering is targeting younger people with the media. We would take advantage of the classic generational struggle by saying your parents are irresponsible, they have no plan, they are entirely selfish, and you need to take over. Kids resonate to this kind of message. I just did a presentation to a young high school class, and all of a sudden they wanted to sign up. It is much like the green movement. We are paying a bit of attention to the green movement now, in part because our kids are sitting in the back of that big SUV saying, "We're putting out a lot of carbon footprint here today, Mom."

If we start to target the young, we start to affect the culture. We do it around a practical set of issues. We do not do it by saying that we are all in the crosshairs. The crosshairs probably are not there, but we are in a place and in a time where we are going to be disrupted rather profoundly.

I just give them one-on-one advice: you have got to be able to camp in your home for three days. If you do that, you will not be part of the problem. Our emergency responders are limited. If you can ride out this emergency without being on the roads and have the basic supplies that you need on hand, you are relieving the pressure on those who really need help.

That is how I explain it to my 12-year-old daughter. It is not that daddy cannot protect you. We have to be responsible citizens because we live in a society where disruption is going to happen from time to time. We need to build up our basic capacity for self-reliance.

Q: Considering our fading compassion and growing cynicism, what conflicts do Americans continue to face as they deal with the post-9/11 terrorism risk?

Dr. Stephen Flynn – We need to segment what Americans are willing to do and what they are demanding versus what politicians and bureaucrats are thinking they want them to do. The reality is, of course, we fixed the 9/11 problem by hardening cockpit doors and changing passenger behavior. United 93 illustrated that. If you deny access to the cockpit, a terrorist will not be able to turn a jet into a missile and drive it into a piece of critical infrastructure. If the passengers say we are not going along for this ride, you cannot have that scenario.

That actually again illustrates the value of bringing people onboard. The bureaucracy says you are all victims, and we have got to do whatever it takes to protect you—for example, by taking nuns' shoes off as they walk through the airline check-in. As we are removing judgment, people are becoming more cynical and more passive. We have lost that 9/11 moment, and I think we can recapture it by giving people things to do.

We have to give them things to do, not just narrowly around the terrorism risk but in the other, broader collective risks that our terrorists are taking advantage of. We are a more brittle society than we used to be. We are less self-reliant than we were. We are more paranoid in a lot of ways, even though we are trying to fake it. By investing in our ability to be prepared as a society, we are accomplishing a lot of good across the board at relatively modest cost.

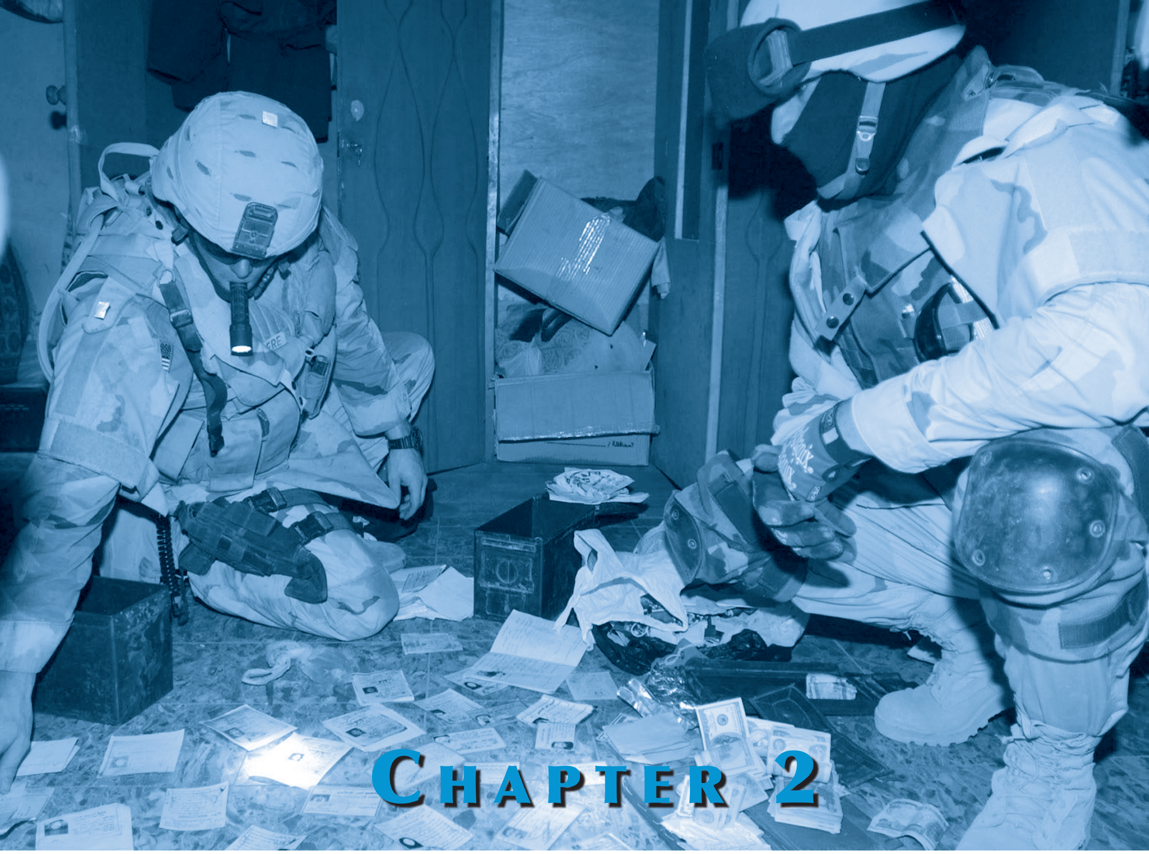
A citizen corps program that trains people around the country to be a part of this preparedness enterprise received a whopping $15 million this year, on top of the whopping $15 million we gave it last year. We are down to a half hour in Iraq for that amount. This is not an either/or case; it is just to say that we clearly made a decision, or a lot of people have just gone along for the ride to spend whatever we have to on the national security apparatus.

We are not willing to make even the most prudent investments in how we engage and draw in our civil society to be a part of the solution. Here is another illustration. My very first assignment when I graduated from the Coast Guard Academy was on a buoy tender. Buoys are traffic posts in the water. Our job was to pick them up, clean them, and put them right back where they belonged. That job introduced me to the neighborhood. Right after 9/11, something quite nice happened. The watermen of Portland said they were willing to be a civil patrol. Their proposal bubbled up to the bureaucracy, which came back and said, “We cannot get clearances for you folks, so thanks but no thanks.”

The Coast Guard has improved that situation now with a reach-out program, but that reflex to reject the watermen’s offer is automatic within the national security world. These watermen go back literally to the landing of the Pilgrims, and there is nobody more territorial than a lobsterman. If you mess with their pots, they can blow you away, and no jury will convict them in the State of Maine. They have complete maritime domain awareness, and they act on that awareness. They are great assets.

I was at a conference at Northern Command (NORTHCOM) in October, where the private sector is having a hard time. One of the members there turned out to be from Maersk, a Danish company that is the largest sea container operation in the world and the largest commercial fleet in the world. He said, “I’ve heard Admiral Mullen talk about the thousand-ship Navy. Well, we’ve got 1,600 of them. They are out there day in and day out, and they know where their ships are. They have a vested interest in keeping the sea lanes open and working.”

Our inability to tap that resource is something that is going to really cause us problems down the road.



Chapter 2

ROUNDTABLE 1

Disrupting Adversary Networks

2.1 MODERATOR'S SUMMARY

John McLaughlin

CHARACTERISTICS OF THE CURRENT WAR

We often say that we are in a long war. We do not often talk about the nature of this war and exactly what it is that we are facing. We need to think about at least four characteristics of this war throughout the conference (Figure 1). The first is that it has an unprecedented degree of asymmetry. I do not think you can find another time in history when such a small number of people can do so much damage, especially were they to acquire weapons of mass destruction. We know they have the intent to do so and the intent to use them.

- Unprecedented Degree of Asymmetry
- Global in Scope
- Proliferation of Nonstate Actors
- No Dominant Strategic Concept

Figure 1 New Kind of Conflict

Professor McLaughlin is a Senior Research Fellow in the Merrill Center for Strategic Studies at the Paul H. Nitze School of Advanced International Studies (SAIS) of The Johns Hopkins University. He has served as Acting Director and Deputy Director, and was the Deputy Director for Intelligence at the CIA, Vice Chairman for Estimates, and Acting Chairman of the National Intelligence Council. Professor McLaughlin founded the Sherman Kent School for Intelligence Analysis, and is a member of the Council on Foreign Relations and a nonresident Senior Fellow at the Brookings Institution.

Second, this is an insurgency that is global in scope. We just have to scan the years since 9/11 to see events of terror from Indonesia to Morocco, from the U.K. to Pakistan, from east Africa to the United States. There is hardly a part of the world that is not marked in some way by this conflict.

Third, this conflict takes place amidst an extraordinary and unprecedented proliferation of nonstate actors. I am not just talking about the terrorist groups; I am talking about the world that has been produced by globalization. The nation state is still here, of course, but is on the defensive. Globalization, for example, has been accompanied by growth in nongovernmental organizations and multinational corporations, and that is the environment in which we must move as we seek to combat terrorists in what is a fundamentally new conflict. It is simply a more complex international environment.

Finally, there is the absence of an overall driving strategic concept, such has we had during the Cold War period. Then, it was the simple phrase, *containment*, devised by George Kennan in the late 1940s. For all of its simplicity, it gave us a strategic concept that everyone could quickly grasp and operationalize in some way. There is no equivalent of that today. We use many words, but there is no single driving concept that quite pulls it together.

As I said at our discussion in the senior panel last year, we have yet to see the George F. Kennans, the Thomas Schellings, the Albert Wohlstetters, or the other theorists who dominated the Cold War period. We are stuck in what one another calls “the gap between strategic epochs” as we try to battle this new adversary.

DIFFERENCES BETWEEN OLD AND NEW ADVERSARIES

In this world, we need to be mindful that many of the traditional concepts that we have become comfortable with—such as deterrence—do not work quite as well. It may be possible to deter the adversary in this new conflict, but deterrence certainly is not as clear or manageable as it was against our old adversaries.

The traditional tools that we use in statecraft are also stressed by this new conflict; they simply do not work as well as they did in traditional conflicts.

Diplomacy has a role, certainly, in marshalling a coalition against this adversary; but diplomacy does not work with this adversary.

There is a role for conventional military power, of course, and certainly a role for Special Operations, but conventional military power alone is not sufficient against this adversary. That was most apparent immediately after 9/11 and after Operation Enduring Freedom, when the al Qaeda operatives scattered to places where we could not send the 82nd Airborne.

So, conventional military power has its limits. Economic policy also has its limits. Economic policy has an important role in combating terrorist financing, but it does not quite work in the traditional sense of being able to sanction an adversary. There are ways to attack their finances; but again, it is unconventional economic policy.

Finally, traditional legal norms do not work well in this environment for reasons that are generating a lot of debate in our country at the moment. In short, if we were to sum this up, I would say that the old adversary was stationary, conventional, and observable (Figure 2). His tools were planes, tanks, and missiles. The new adversary, on the other hand, is stealthy, agile, and unconventional. At a symposium at SAIS held about 2 years ago, I was struck by one of our Australian colleagues who said that the tools of the new adversary are Microsoft, machetes, Kalashnikovs, and tribal drums.

OLD ADVERSARY:

- Observable, Stationary, Conventional

NEW ADVERSARY:

- Stealthy, Agile, Unconventional

Figure 2 Old Versus New Adversaries

At the same time, global trends promise to further complicate the environment in which we struggle against this enemy. As the world approaches 7 billion people, it is noteworthy that most of that growth—approximately one Mexico per year added to the population of the world—is occurring in parts of the world that very often coincide with the origins—the recruiting centers—for terrorists. Governments come under greater stress in those areas as they seek to provide services to an expanding population. The likelihood is an increasing number of young men and women unemployed and ripe for recruitment.

Urbanization is proceeding apace, with about one-third of the world's people living in cities. In 10 to 15 years, about half of them will live in cities, giving rise to the era of the megacity of 25 to 27 million—places like Lagos and Karachi and Tokyo. A generation of terrorists trained in urban warfare is emerging from the Iraq conflict, which may have implications for the future battlefield that we need to consider.

We are very good at many parts of technology, but the same technology that is proceeding apace now will also be available to the adversary. Computer processing power per unit doubles every 18 months. While we are very good at finding, fixing, finishing, and following up—the classic intelligence/military formula—in the real and concrete world, we are not very good at finding and fixing in cyberspace. We are facing a tremendous technological challenge.

DISRUPTING THE ADVERSARY

Disrupting this adversary is very different from dealing with the old adversary. With the old adversary, we had to detect rather large objects: conventional forces and the locale of strategic nuclear facilities. Detecting and disrupting this new enemy involves finding very small things, whether it is a bomb in a suitcase or that liquid that we cannot take on airplanes, or a single packet of data that is moving through the global information network (Figure 3).

- Finding Small Things
- Secrets Harder to Get
- Drowning in Data
- Unprecedented Information Sharing
- New Data Flow Paradigm

Figure 3 Disrupting the New Adversary: New Challenges

Detecting and disrupting the old adversary meant gaining secrets that were held by thousands of people. Often, you could find them in ministries, cabinets, and embassies. The new adversaries' secrets are held by a much smaller number of people, often in very remote areas. You will not find them at embassy cocktail parties.

Detecting and disrupting the old adversary meant scrambling for data. We did not know enough. We understood capabilities but not intent. Now, we understand intent very well but do not understand capabilities as well. In a sense, ironically, we are drowning in data. Back in 1950, there were about 5,000 computers in the United States. Today there are 530 billion instant messages on the Internet every day.

Detecting and disrupting the old adversary meant compartmentalizing information and holding it tight. Detecting and disrupting the new adversary involves an unprecedented level of sharing of data across a wide array of coalition partners—data of varying sensitivity, another challenge.

Detecting and disrupting the old adversary often involved guidance, leadership, and intelligence dispensed from the top. Detecting and disrupting the new adversary requires information flowing up from special operators—intelligence officers operating in the back streets around the world—and compiling it into a database that ultimately must be shared with many other people.

COUNTERINSURGENCY STRATEGY

In this environment, what kind of strategic posture must we adopt? How do we prevail and ultimately end this conflict? Classic counterinsurgency tells us we must destroy the leadership, we must deny the leadership and the movement safe haven, and we must change the conditions that bring about this phenomenon that we call terrorism by doing the following:

- Destroy the Leadership
- Deny Safe Haven
- Change the Conditions

CURRENT CONDITIONS FOR THE ADVERSARY

From roughly 2001 to 2006, we did rather well in destroying the leadership and denying safe haven and not very well then or now—perhaps never—on changing the conditions that give rise to terrorism. So where are we today? Figure 4 provides a quick scorecard.

There was a debate on National Public Radio (NPR) this morning [10 March 2008] [1] among people across the spectrum on the degree to which there is a serious threat from al Qaeda today. I am on the side that says we still have a serious problem here. I think we can debate the degree and debate the pace and the timing, but I would describe it roughly this way. We have an adversary now that has reestablished a safe haven of sorts along the Afghanistan-Pakistan border, and it has expanded. That is why I said we had done fairly well in denying safe haven until roughly 2006. With President Pervez Musharraf's agreements with the local tribal leaders along that border and the increasing aggressive expansion of the adversary into some of the more settled areas of the tribal regions, they now have a safe haven in which they can operate with some impunity.

- Safe Haven Reestablished
- Afghan Toehold Regained
- New Global Affiliations
- Widening Breadth of Operations
- Central Leadership Reach
- Robust Propaganda Capacity
- Powerful Narrative
- Resilient After Defeats
- Memories of 9/11 Fading

Figure 4 Conditions for the Adversary Today—A Scorecard

Also, al Qaeda has reestablished a toehold in Afghanistan. They were never really at odds with the Taliban, but there was a period when the relationship between the Taliban and al Qaeda was not as close as it is today. As a result, we are seeing the migration into Afghanistan of the kind of tactics that we have come to expect in Iraq.

The number of suicide bombings rose from 21 in 2005 to 118 in 2006. I do not have the figures for 2007, but by mid-year 2007, there were 107 such bombings.

We are seeing new affiliations around the world as groups adhere to the al Qaeda mantle. Some will argue that they are simply, if you will, putting on the t-shirt, but they have a virtual safe haven that they can operate in that connects all of these people. They continue to take their inspiration from al Qaeda central. So we see groups like the Salafist Group for Call and Combat (GSPC) in Algeria taking on the name al Qaeda in the Islamic Maghreb and using classic al Qaeda tactics that we had not seen before in Algeria. There is a widening breadth of operations from Algeria to Southeast Asia and from London to Istanbul. There is a clear connection between many of the operations that at first were thought to be local.

We are now learning enough to understand that there are connections between local jihadist training camps, leaders, and assistants in those Pakistani–Afghan tribal areas. This is certainly true for the attacks that have occurred and been thwarted in the U.K. It may also be true for the attacks in Spain. It appears to be true for the attacks that were thwarted recently in Germany, and the list goes on.

Best documented are the 2005 London subway bombings, where Mohammad Sidique Khan, the lead bomber, a 30-year-old primary school teacher, recruited three colleagues between the ages of 17 and 21, all of whom committed suicide in the bombings. Mohammad Sidique Khan, who had clearly traveled to and apparently had been trained in Pakistan, appeared in a video placed side by side with another video of Ayman al-Zawahiri. I believe two of the other culprits in that attack had traveled to Pakistan as well. The connection is clear.

The propaganda capacity of the adversary is expanding, with videos and audios seemingly doubling each year.

We can take some comfort in the capture or killing of four successive chiefs of operations, starting with Khalid Sheikh Mohammad and continuing through Abu Ferag Alibi, Abu Hamza Rabia, and Abd al-Hadi al-Iraqi. Despite these fairly significant losses of leadership, the adversary appears to be resilient. They keep coming back. Meanwhile, it is not inconsequential that in our own country, memories of 9/11 are fading. We can look at the newspaper every day and come to the conclusion that the political consensus in our own country about how to deal with this adversary is beginning to fray. That is the environment in which they are operating.

ADVERSARY WEAKNESSES

They have some weaknesses, too (Figure 5). As Peter Bergen points out, they are not 12 feet tall. There are four main vulnerabilities we can exploit. For example, they have killed a lot of Muslims. Where they have done that, particularly in a place like Jordan where they attacked a wedding party, their credibility with the Muslim public has been dealt a serious blow.

- Attacks on Muslim Population
- No Positive Vision
- No Social Services
- Against Everyone

Figure 5 Adversary Weaknesses

Also, they do not have a positive vision. The whole idea of a caliphate, which existed for several decades centuries ago, is not something that I think the average Muslim is longing to recreate. In addition, they have no social services to speak of, unlike Hezbollah, which provides significant social services to about 250,000 people in Lebanon, or even Hamas, which came to power based on its record of providing such services to the Palestinian population. Apart from supporting the immediate family members of activists, al Qaeda does not have such a program.

Finally, who is not on its enemy list? They are against our European allies, they are against us, they are against most of the Middle Eastern governments, they are against the Russians—just about everyone is on their enemy list. So this is not a movement that has a lot of friends among nation states for sure, even though those countries vary in their capacity and their willingness to attack them.

REFERENCE

1. “Measuring the Strength of a Changing Al-Qaida,” Tom Gjelten, National Public Radio Morning Edition, 10 March 2008.

2.2 ADVERSARY NETWORKS

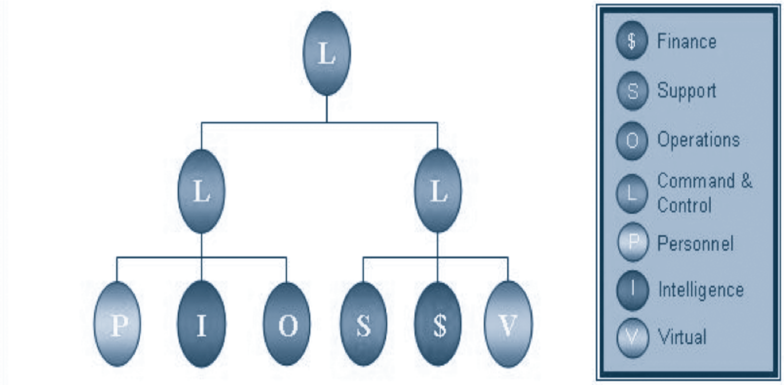
Matthew Levitt

One area where adversary networks operate is in the financial sphere. The relationships within and between the financial and logistical support networks of the Diaspora groups based in the Middle East or elsewhere tend to spread out beyond those in their home countries. It is therefore a very useful focus area for identifying covert networks. Any time people engaged in covert activity have to expose themselves to the open world, such as accessing the international financial system, we have an opportunity to identify these actors and reveal their relationships to other persons of investigative interest. Travel, communications, and finance are perhaps the three most important such areas. Therefore, when discussing adversary networks, we should refer not only to operational cells but also to the recruiters, the ideologues, and the logistical and financial support net-works that facilitate their activities.

In some cases, these roles will be discrete, especially in terms of operational security concerns. However, when we get into the typically ad hoc relationships between individual operatives and supporters, we increasingly find overlap, interconnectivity, and

Dr. Matthew Levitt is a Senior Fellow and Director of The Washington Institute's Stein Program on Terrorism, Intelligence, and Policy. He is also a professorial lecturer in International Relations and Strategic Studies at The Johns Hopkins University's Paul H. Nitze School of Advanced International Studies (SAIS). He has served as deputy assistant secretary for intelligence and analysis at the U.S. Department of the Treasury, and as deputy chief of the Office of Intelligence and Analysis protecting the U.S. financial system from abuse and denying terrorists, weapons profiteers, and other rogue actors the ability to finance threats to U.S. national security.

bleeding between the different areas, and these relationships will start to manifest themselves.



Source: adapted by Major Wesley Anderson from the unpublished work of Major Grant Morris and The School of Advanced Military Studies Program Special Operations Elective.

Figure 1 Hierarchical Structure of Terrorist Organization

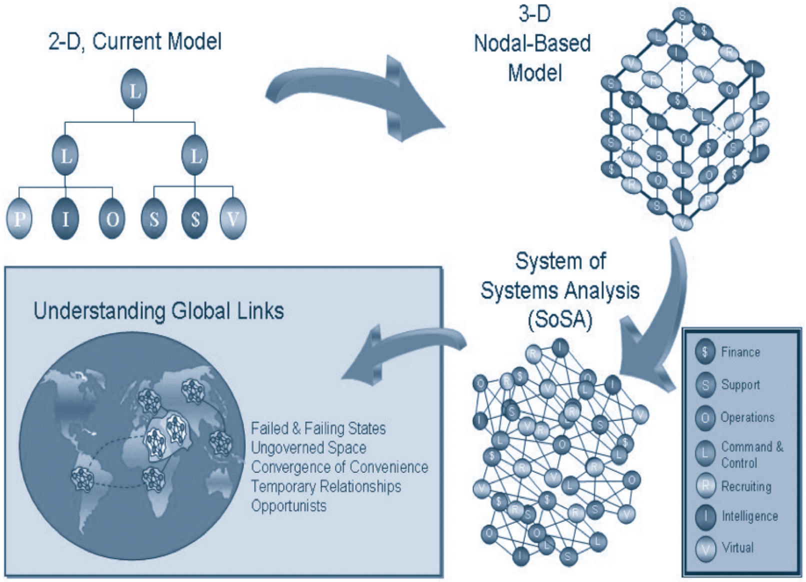
These relationships do not need to be formal. We should not expect memoranda of understanding between different elements within groups or between different groups. Sometimes they will just be ad hoc, and some-times the press will make more of ad hoc relationships than they should, but we should be paying attention because the overlaps between operatives and supporters are very important.

For example, General Nizar Ammar of the Palestinian Authority (PA) has noted that there have been many cases where the PA knew of a Hamas operative engaged in political or social welfare activities. Only the day after a bombing, however, did they discover the role the activist played in the attack. Certainly, this was the case before 9/11 in Europe, where a number of individuals were known as supporters but were not suspected of engaging in operational activity even as they supported what became the 9/11 hijackings.

Particularly in Germany, where prosecutors determine how operational resources and investigations are prioritized, authorities determined that individuals of interest were not "operatives" but supporters and did not warrant continued, full-scale surveillance.

We are not dealing today with any type of pure, simple hierarchical organization but with different types of networks intersecting and overlapping with one another.

When we look at the ever-increasing type of network structures that we are seeing, we get a sense of how complicated this area is (Figure 2). If we really want to be effective in dealing with a network of networks or a system of systems, we need to focus on relationships. You need to take advantage of every time covert operatives expose themselves by engaging in overt action, including financing.



Source: adapted by Major Wesley Anderson from the unpublished work of Major Grant Morris and The School of Advanced Military Studies Program Special Operations Elective.

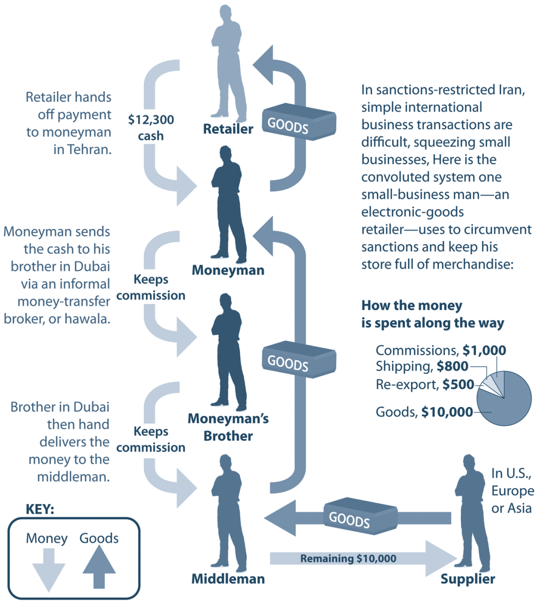
Figure 2 Network Structure

AD HOC RELATIONSHIPS

The 9/11 commission discussed ad hoc relationships between Hezbollah and al Qaeda. Hezbollah, of course, is not al Qaeda, but the existence of ad hoc relationships is telling. These interpersonal relationships are very important, whether they come from shared time in a training camp or shared connections through radical Islamist networks like the Muslim Brotherhood or Hizb a Tahrir.

A recent case in Bahrain received a lot of bad press (Figure 4). Six Bahrainians were tried for plotting what was believed to be an al Qaeda-inspired attack and were sentenced to only six months. In fact, prosecutors sought much harsher sentences, but the judge issued light sentences because no attack occurred and based on the recantations of the cell members who promised to cease engaging in violent activities in the future. However, according to Bahraini prosecutors, the cell was connected with al Qaeda networks operating in Iran. It is not clear how much the Iranians were aware of these al Qaeda facilitators within their borders, but what is clear is that the Iranians allowed them to enter the country without stamping their passports (as was the case with several of the individuals tied to 9/11, as documented by the 9/11 Commission). They were transferred from facilitator to facilitator until they arrived in the Afghanistan/Pakistan area for training. Because they were going anyway, they were sent with some funding to pass along to al Qaeda core operatives.

This is an interesting case that highlights the nature of these ad hoc relationships. In another context, Figure 3 depicts how relationships are being leveraged to evade the sanctions on Iran. It also shows how simple these relationships can be. Not every node in these relationships is going to be adversarial. Sometimes people are in this for profit, or they are helping a friend or a relative. Understanding how these relationships function is incredibly important. One of the examples I like to cite is Bank Al Taqwa, which was one of the first entities to be designated after 9/11. When the Treasury Department first publicized its designation of Bank Al Taqwa, it highlighted the bank's activities on behalf of al Qaeda. As investigative journalists and others started looking around, they discovered the bank was also involved in significant financing for Hamas as well as several North African groups. It turned out the bank was a key node being utilized by a variety of terrorist groups.


Retailer hands off payment to moneyman in Tehran.
$12,300 cash
Retailer
GOODS
In sanctions-restricted Iran, simple international business transactions are difficult, squeezing small businesses, Here is the convoluted system one small-business man—an electronic-goods retailer—uses to circumvent sanctions and keep his store full of merchandise:
Moneyman sends the cash to his brother in Dubai via an informal money-transfer broker, or hawala.
Keeps commission
Moneyman
How the money is spent along the way
Commissions, $1,000
Shipping, $800
Re-export, $500
Goods, $10,000
GOODS
Brother in Dubai then hand delivers the money to the middleman.
Keeps commission
Moneyman's Brother
In U.S., Europe or Asia
KEY:
Money
Goods
GOODS
Remaining $10,000
Middleman
Supplier

Wall Street Journal, 2/13/08

Figure 3 Following the Money

What is important here is focusing on the centers of the concentric circles of relationships among radical, violent extremists, and extremist groups. Failure to do so guarantees we will miss some key relationships between illicit actors. Law enforcement and intelligence officials have found that it is not uncommon, for example, to find that suspects affiliated with a known operative affiliated with given groups will end up being affiliated with a completely different group, especially when located in the United States, Europe, or elsewhere in the Middle East Diaspora. Connecting these dots and properly identifying the nature of these relationships is very important. Often these relationships are between individuals from different groups that one would not necessarily lump together.

OPERATIVES AND SUPPORTERS

Distinguishing between operatives and supporters is a very big problem. We can analyze attack after attack and demonstrate how people who were believed to be supporters ended up being operatives.

Hezbollah offers a good example of these relationships. Unlike al Qaeda, Hezbollah engages in domestic political activity in Lebanon, positions itself as a resistance organization, and denies that it is involved in international terrorism. In the wake of the assassination of Hezbollah's chief of international operations, Imad Mughniyah, Hezbollah is likely to carry out some form of international terrorist activity targeting Israeli or Jewish targets, as it has in the past. Some past examples of Hezbollah terrorist activity abroad show very clear crossover between supporters, such as people involved in funding Palestinian groups, and operatives, those involved in pure acts of terrorism. For example, Yusuf al-Jouni and Abu al-Foul, who were both involved in the failed Hezbollah bombing of the Israeli Embassy in Thailand in 1994, also smuggled weapons to Palestinian groups in the West Bank through Jordan. Several Hezbollah operatives were arrested by Jordanian authorities and later released there. There are many other examples of such crossover between the different "wings" of terrorist organizations.

To be sure, neither the terrorist operatives or their supporters are going to look like our preconceived notions of them. Figure 4 is a surveillance picture of three Hezbollah operatives taken by the Canadian Security Intelligence Service (CSIS). They were part of a North American Hezbollah network raising funds (primarily in North Carolina and Michigan) and procuring dual-use technologies for Hezbollah operations back in Lebanon (primarily in Canada). Here, the operatives are inspecting false identification they recently purchased to facilitate their illicit procurement activities.

TERROR FINANCING

Constricting the terrorists' operating environment encompasses the kind of tactical counterterrorism activities we in the West tend to do best—kinetic operations, kicking down doors, tapping phones. We are far less adept at engaging in the battle of ideas. If both were used together, we could have a very successful, strategic approach to combating terrorism. Focusing on the money—which is only one small tool never to be used in isolation—is very useful, both in terms of constricting the operating environment and denying funds to the various networks trying to do us harm. However, it also offers a tremendous opportunity in the battle of ideas as the information we make public when we designate terrorists and their supporters as grist for the public diplomacy mill. Focusing on key nodes—and this applies to other aspects of counterterrorism, too, but certainly terror financing—can be very effective.

© The Washington Institute for Near East Policy

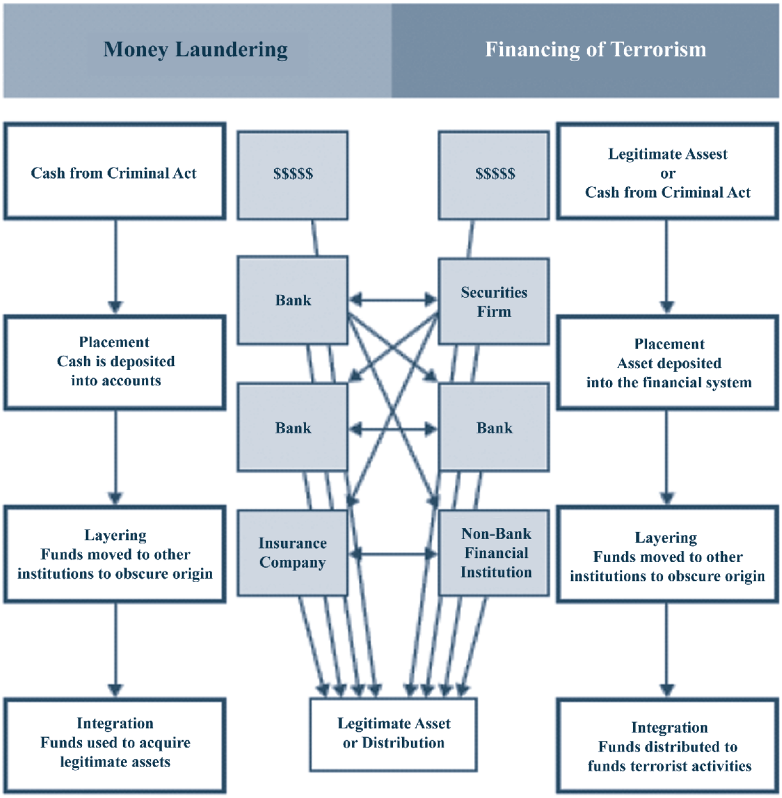
Figure 4 Hezbollah Operatives in Canada

Richard Clarke has been made into somewhat of a political lightening rod, but he is right when he says "al Qaeda is a small part of the overall challenge we face from radical terrorist groups which associate them-selves with Islam. Autonomous cells, regional affiliate groups, radical Palestinian organizations, and groups sponsored by Iran's Revolutionary Guards are engaged in mutual support arrangements, including funding." On top of this, consider the many opportunities there are for networks to present themselves and for relationships to develop—relationships that will be useful in a variety of different places for all the different activities and all the different stages of the terrorist lifecycle. Take, for example, the specific case of laundering funds. As funds move through the formal or informal financial systems, interactions occur as illicit actors place, layer, and then reintegrate their funds for future access

This money-laundering cycle is just one small part of the criminal or terrorist lifecycle; we could place it into a much larger lifecycle as well. We could also look at it in terms of the differences and similarities between traditional money laundering and traditional terror finance (Figure 5)—which present plenty of opportunities for interrelationships between illicit actors. The big difference between money laundering and terror finance is that money laundering deals with funds that started out "dirty" and need to be "laundered" for future access and use as "legitimate" funds. Terror financing is more difficult because the money is only "dirty" be-cause of its ultimate intended purpose. Looking backward over the money trail, investigators may never find dirty money. However, looking vertically and horizontally at the relationships between actors at various stages of financial transactions can be a very effective tool.

We should stress that there are two means of combating terrorist financing: freezing the money and following the money—each of which can be extremely effective. Deciding which tool to use—indeed, deciding whether the financial angle is the best course of action at all—demands a case-by-case analysis. In some cases, seizing or disrupting even small amounts of money can frustrate terrorist planning. For example, Mustapha Abu Yazid, a former al Qaeda moneyman and now a senior operative in Afghanistan designated by the U.S. and UN, has said, "We have got people to deploy, but we just do not have the money to deploy them."

Funding is important for other types of adversary networks as well. When it comes to proliferation networks, deterrence and disruption are a bit different because states are involved. However, even there, we find networks of suppliers, financiers, transporters, and others that also function as networks in their own arena.


Money Laundering
Financing of Terrorism
Cash from Criminal Act
$$$$$
$$$$$
Legitimate Assest
or
Cash from Criminal Act
Bank
Securities Firm
Placement
Cash is deposited into accounts
Placement
Asset deposited into the financial system
Bank
Bank
Layering
Funds moved to other institutions to obscure origin
Insurance Company
Non-Bank Financial Institution
Layering
Funds moved to other institutions to obscure origin
Integration
Funds used to acquire legitimate assets
Legitimate Asset or Distribution
Integration
Funds distributed to funds terrorist activities

Source: The World Bank

Figure 11 The Processes of Money Laundering and Terrorist Financing

Critically, whether focused on terrorism, proliferation, or other illicit conduct, public actions like designations and prosecutions should not be construed as the totality of our efforts to combat terror financing; they are only the most visible. In fact, our financial intelligence analysis and to a lesser extent, operations are very successful. There is also great opportunity for diplomatic engagement on combating terror finance. For example, the Qatari government is quite open about the hundreds of millions of dollars it has provided to Hamas. This presents an opportunity for diplomatic engagement with a friendly country over an issue on which we strongly disagree.

In addition, much can be done with regulatory enforcement. The biggest impact, however, may come with further public-private engagement on combating terror finance. One of the things we need to do better is develop means to provide some level of clearances to people in the financial community within the private sector so they have a better sense of what to look for and how to best protect themselves from abuse by illicit actors. We have to help them help us.

EVOLUTIONS IN TERRORIST FINANCING

Terrorists are not dangerous today because they are revolutionary; they are dangerous because they are evolutionary. You can see this in terror financing as well. As we have cracked down, for example, on global charities that were financing illicit activity around the globe, some of these charities have deferred decision making to local offices and personnel from their headquarters offices.

There is a lot of emphasis on building infrastructure, which is not only much needed but provides great cover for the transfer of substantial sums of money overseas. There is also a constant problem with NGOs operating under new names. A charity involved in illicit finance may be shut down today and open tomorrow under a different name in a slightly different location. The result is that law enforcement and intelligence investigations must start from scratch.

All this means is that we have a lot to do. If we were to focus on the networks and identifying relationships between individuals, we could position ourselves to be able to look around the corner the day after an action against, say, a terror-financing charity and see where they are going to open up the next day. This is particularly important when it comes to combating terror financing, as well as other types of logistical and financial support.

Our adversaries are limited only by their imagination. Consider a CSIS telephone intercept that was produced in open court in a Hezbollah court case in Charlotte, North Carolina. The conversation is between a person in Canada and a person in Lebanon, who are discussing taking out a life insurance policy in Canada on a person in Lebanon who would "go for a walk and never come back in the south"—presumably a suicide bomber targeting Israeli forces in Southern Lebanon (just before the Israeli withdrawal in 2000). There is neither evidence they actually carried out the scheme or that they acted on another scheme to import counterfeit U.S. $100 bills from the Beka Valley. However, it does demonstrate the scope of their imagination.

MEASURING THE EFFECTIVENESS OF COUNTERING TERRORIST FINANCE (CTF)

There is often a debate as to whether this whole effort to block terror financing is effective and whether it is worthwhile because terrorists can attack for a little money, and they are always changing names. I would argue that countering terror financing, while just one tool in the counterterrorism toolkit, is a highly effective one. Measuring its utility, however, can be difficult. People tend to apply two sets of metrics to the freezing of funds, both of which are inherently flawed: (a) How much money has been frozen? and (b) How many entities have been designated? In fact, the whole terror finance strategy is network-based, focused on targeting key nodes, or choke points, in the network of terror finance. It is wonderful if we can freeze a good deal of money going to terrorists, but that should not be the primary focus simply because if we focused on the fund-raising element, we would always be playing catch-up, like the hamster running in the wheel in his cage. Indeed, there are many more terror financing entities out there that have not been designated because designation is only one tool; it is not only the best tool. The equities of various interagency partners and foreign allies and the availability of actionable intelligence limit the ability to designate all appropriate targets. Moreover, law enforcement or intelligence operations—or diplomatic engagement or capacity building—may be a more appropriate tool for different cases. Trying to figure out how much money has been frozen and how many entities have been designated misses the point. Are we focused on the right chokepoints? Have we identified the right nodes and the key relationships in the networks so that we can have as much of a disruptive effect as possible?

Designations can work if used appropriately. When applied against the right targets, they can name and shame, they can constrict the operating environment, and they can have a very disruptive impact on terrorist plotting. There are many declassified anecdotes where terrorists say, as Abu Yazid did, that they lack access to the funds they need and are therefore operationally constrained. This is one of the few areas in modern day counterterrorism where deterrence can have an impact. True, the average suicide bomber is unlikely to be deterred. However, the major donors financing al Qaeda are people who have spent their lifetimes building up financial empires. They are not sending their children to die as suicide bombers, and they do not want to put their financial empires at risk. Repeatedly, after being exposed, they pull out and become less active.

It is very difficult to measure the impact of efforts to combat terror finance. There is no "Jack Bauer" moment. However, there are some telling anecdotes that have been declassified, mostly for congressional testimony. The FBI has talked about attacks they have successfully thwarted abroad by following the money at home. Much has been said about the utility or the effectiveness of the sanctions on the Hamas government in Gaza. Treasury officials have talked about cells complaining that they lack funds to carry out their plans. There are even cases that have been partially declassified by allies like the UK on their success combating terrorism by following the money.

FOLLOWING THE MONEY: VALUE OF FINANCIAL INTELLIGENCE

It is important to stress how effective financial intelligence can be. It has proven extremely important post-blast in almost every investigation from Ramsey Yousef [the man who plotted the 1993 attack on the World Trade Center] on down but also in preventive efforts to foil ongoing terrorism plots. In the words of then Chancellor of the Exchequer (now Prime Minister) Gordon Brown, "Just as there be no safe haven for terrorists, so there be no hiding place for those who finance terrorism." Brown called for a "Bletchely Park" style effort to combat terror finance styled along the lines of the effort that eventually broke the Nazi communication code in World War II.

When the 9/11 commission evaluated efforts to implement its recommendations, the only A grade it awarded was an A- to the government's efforts to combat terror financing, especially the financial intelligence aspect of it.

Financial intelligence is an extremely effective tool, particularly in identifying the kind of relationships we have discussed here. Following the money as it travels between people enables investigators to identify previously unknown contacts. In some cases, following financiers or supporters leads to the operators planning attacks.

Consider the case of Dhiren Barot, who was originally known to British intelligence only as Esa al Hindi. Following the financials of their subject, British authorities identified him and his accomplices as they plotted attacks in Great Britain and the United States.

Following the money is also an extremely useful tool in the battle of ideas, an area in which we need significant improvement. When Treasury started designating individuals and entities right after 9/11, they simply listed names. Eventually, they realized they needed to explain why they were doing these things. No less important, they needed to provide information so that financial institutions would actually know who these people and entities were. This designation provides a treasure trove of declassified information that should be publicized in an effort to actively engage in the battle of ideas instead of ceding the entire narrative to our adversaries' propagandists.

Focusing on the financial angle alone will not solve the critical national security problems we face today. However, used wisely and sparingly, and in the right situations, combating terrorist and proliferation finance can be extremely effective when combined with other tools. It can be effective in denying illicit actors access to the money they need to conduct their various operations. Even more important, it can be effective in identifying the relationships within and between these networks. This must be our primary objective because what makes terrorists, proliferators and other illicit actors so dangerous is not that they are revolutionary, but they are evolutionary. They are difficult to identify, which means it is critical we take advantage of those instances when covert actors are forced out into the overt world. Nowhere is this more pronounced than in the areas of travel, communication, and finance.

2.3 STRATEGIC, ANALYTIC, AND TECHNOLOGICAL DEVELOPMENTS IN DISRUPTING NETWORKS

Paul Pillar

I will start with Matthew Levitt's last point, which is that the disruption of terrorist finances is only one of a menu of tools for disrupting terrorist networks. In turn, the disruption of terrorist networks is only one facet of counterterrorism at large.

TOOLS FOR DISRUPTING TERRORIST NETWORKS

Per the title of this panel, I will confine myself to the topic of disrupting networks. Let me remind you of some of the other tools:

- The military tool, which occasionally can apply its kinetic methods to truly disrupt networks
- The capabilities of our law enforcement agencies, such as the FBI, which mainly investigate but sometimes arrest and prosecute

Dr. Paul R. Pillar is a Visiting Professor and member of the core faculty of the Security Studies Program in the Edmund A. Walsh School of Foreign Service at Georgetown University. His distinguished career in U.S. intelligence included National Intelligence Officer for the Near East and South Asia. He has served as chief of analytic units at the CIA and on the National Intelligence Council. Dr. Pillar served the U.S. Army Reserve in Vietnam, and he was head of the Assessments and Information Group of the DCI Counterterrorist Center, and a Fellow at the Brookings Institution. Dr. Pillar holds a bachelor's degrees from Dartmouth College and Oxford University, and an M.A. and Ph.D. from Princeton University. He is the author of Negotiating Peace and Terrorism and U.S. Foreign Policy.

- The capabilities of our intelligence agencies, which are primarily collection and analysis of information, occasionally include covert action.
- Diplomacy, which John McLaughlin touched on briefly earlier, is an important part of disrupting networks.

No matter how much information gathering, preliminary work, instigation, and organization goes on inside our government, in the end, disrupting a foreign terrorist network usually entails the actions of some foreign government—for example, a police or internal security service conducting a raid and arresting someone. Even a knock on the door can have a very disruptive effect if it sows concern, fear, and distrust inside the terrorist organization. We have seen on many occasions where just the knock on the door and perhaps some questions by the local police or security service were sufficient to cause a major disruption to the planning and operations of a terrorist cell.

LIMITATIONS OF TOOLS

Most of the important means of disrupting terrorist networks have not changed in recent years. The tools listed are the same ones that have been in our kit for quite some time. Each of them has inherent limitations. With the financial tool, for example, we have to make sure that we have identified the right accounts. Is an IRA account an individual retirement account, or does it belong to the Irish Republican Army?

Perhaps the most basic limitation is that terrorists can do a lot of harm cheaply. Much of what our law enforcement agencies can do is limited by whether a crime or a suspected crime is being committed, despite the attempt by Director Robert S. Mueller to redirect the efforts of the FBI to intelligence gathering and not just law enforcement.

Intelligence has multiple challenges. With diplomacy, we are dependent on the good will and capabilities of a foreign government. As far as military tools are concerned, the great majority of activities by terrorist cells and networks do not provide good military targets—for example, inside apartment buildings in western cities, U.S. flight schools, etc.

"We have seen on many occasions where just the knock on the door and perhaps some questions by the local police or security service were sufficient to cause a major disruption to the planning and operations of a terrorist cell."

WHY DISRUPTION HAS BECOME MORE DIFFICULT

Before I discuss how strategic, analytic, and technological developments may be enhancing our capability to disrupt networks, I want to note some of the reasons disruption has gotten more difficult.

Increased Decentralization

One is the increased decentralization of the jihadist movement, which has concerned us over these last several years. Mark Sageman makes the point that larger developments in the jihadist world will shape the degree of terrorist threat that we face for the next several years, at least as much as anything al Qaeda central does. To use the title of Sageman's book, there is a leaderless jihad, with individuals acting independently and being swept up into this movement and ideology in a very undirected, uncentralized way.

Dr. Sageman cautions that we should bear that in mind as we are fighting the al Qaeda central target, and that we should not conduct that fight in a way that exacerbates the decentralization problem. This division multiplies our intelligence problems because there are more independently operating nodes of activity and more directions from which threats may emanate, creating more difficulty for our intelligence services in detecting and keeping track of the activity.

Terrorist Use of Technology

Terrorist use of technology has also become more challenging. It is not just that the terrorists can make greater use of it in the future; we have already seen increased, very effective operational use of technology for planning, for internal communications, and for research to formulate operations. If it works for legitimate businessmen and scholars, it works for terrorists as well. Some technology, of course, expands the terrorist vulnerabilities, but it also expands their capabilities.

Cooperation of Foreign States

The third limitation is the lack of willingness or capability among certain states to fulfill their part of this task. I am thinking particularly of Pakistan with its wrenching political difficulties that have, at a minimum, severely distracted the Pakistani leadership from the counterterrorist tasks on which we would like them to focus.

That last observation goes beyond the strategic, analytical, and technological arena and gets into the political. If I were to revise the subtitle for the panel, I would put "political" in there as well. Indeed, looking on the positive side, much has been accomplished, especially since 9/11, in disrupting foreign terrorist networks, and a huge factor has been the increased willingness of foreign states to be more cooperative. The demands of the American people for action since 9/11 have made it possible for us to send formidable people like Richard Armitage to these foreign states and tell them to cooperate with the program. So, in terms of positive developments that will enhance our ability to disrupt networks in the future, the political side is important too.

TECHNOLOGY AND ANALYTIC TECHNIQUES FOR DISRUPTING NETWORKS

Limitations

Political and Legal Issues

For the most part, the relevant technology and analytic techniques have been here all along. A little over 10 years ago, I was involved in one of the Defense Science Board's summer studies looking at transnational threats, which mainly meant terrorism. I was attached to the science and technology subpanel, and what I mainly heard from the panelists, including a lot of senior experts in the private sector in telecommunications and information technology, was that there are all kinds of technology (even a decade ago) to do very sophisticated data mining and others that are applicable to the task of detecting and disrupting terrorist networks. The main problem is not the technology; it is the legal and the political issues associated with accessing the information and using it.

Look at the controversies in recent years over the Patriot Act or, more recently, the interception of communications, the courts' role in such intercepts, and the most recent legislation that the White House and Congress have been debating. What the National Security Agency (NSA) can or cannot do is not a technological issue; it is the old question of balancing security interests in the name of counterterrorism with privacy or personal liberties.

There are probably some additional advances to be made in information-handling technology with respect to mining of large and diverse sorts of data that could further enhance our capability to disrupt terrorist networks. I am thinking of a program that could somehow mimic the mind of a very capable counterterrorist analyst, look at the data, and draw conclusions about whether they indicate a bad guy. But I would not expect major advances in applying any of this to counterterrorism or in seeing major counterterrorist results because of the political and legal problems in accessing information.

Terrorist Decentralization

The terrorist decentralization that I mentioned earlier is a major limitation on what we can achieve through the sort of link analysis that counterterrorist analysts perform in trying to decipher and make sense of terrorist networks. One person is connected to somebody else because of a phone call or financial relationship, and that second person is connected to someone else, who is connected to someone else. The more independent or would-be jihadists there are who are not under the umbrella of a Hezbollah or an al Qaeda, the more difficult the task, no matter how sophisticated the analytic techniques and technology.

". . . we do not yet have the capability to technologically mimic what a really good analyst would do."

Successes

Despite all these limitations, disrupting networks is, in my judgment, the single most important counterterrorist task that we can address. It has resulted in most of the biggest counterterrorist successes that have been achieved. The kind of archetypal success that the public most often expects and demand—thwarting a planned terrorist plot before it can be executed—will always be rare because of the inherent difficulty of discovering the tactical details of that next plot. We will be able to prevent terrorist attacks by finding out more about the networks, about the personal relationships, about the suspected bad guys, even if we are unable to identify exactly what attack it was we prevented.

"There are probably some additional advances to be made in information-handling technology with respect to mining of large and diverse sorts of data that could further enhance our capability to disrupt terrorist networks. I am thinking of a program that could somehow mimic the mind of a very capable counterterrorist analyst, look at the data, and draw conclusions about whether they indicate a bad guy."

This kind of disruption is inherently even more effective than the kinds of defensive security measures that have been so much of our homeland security focus over the last several years. If you focus on safeguarding any one potential target, you have protected just that target or class of targets. If you focus on any one particular method, like unconventional weapons versus conventional bombs, you have protected yourself against only that one method. But if you disrupt a terrorist organization that could attack any target with any method, then you have prevented a lot more. That is why the topic of disruption of networks is so important.

2.4 QUESTIONS AND ANSWERS HIGHLIGHTS

Transcripts

Q&A

Q: *What are our financial institutions doing to cut money off to terrorist networks?*

Dr. Matthew Levitt – Well, not a whole lot. But what can be said is that there are people looking into this. There are a reasonable number of people in the financial community, particularly in New York, who have clearances. The operation is not organized yet, and it has not proliferated out as far as we need it to be. It is not a question of reinventing the wheel. DoD has been doing this in many different ways and in many different places for a very long time.

People who have clearances and are able to work in Secure Classified Information Facilities (SCIFs) and people in other parts of the world who are able to come into a SCIF can have access to some information and go back to their regular places of business. I think the vast majority of this operation can be done at the secret level. Therefore, it is really important to try and build it up.

There is a conference next week where some of the right people in the Washington area are bringing in some of the right people from New York and other places to look into this. I think it needs to be done and done quickly. However, I do not think organizing this kind of operation should be difficult to do.

I will just give you one anecdote from a good friend of mine, Bob Werner. Bob is the only person who has served as both the Director of FCEN—the Financial Crimes Enforcement Network, which is the American financial intelligence unit at Treasury—and also as Director of the Office of Foreign Assets Control, where he administered the U.S. sanctions program against criminal enterprises and terrorists. He is now a senior anti-money laundering

(AML) compliance person at a major bank in New York. He has said, "Look, I will be honest. I put most of these regulations on the books, and I guess I assumed in the back of my head that the private sector had all these really sexy tools at its disposal, but they do not. There is a tremendous lack of training, and we do not yet have the capability to technologically mimic what a really good analyst would do." The result is either significant underreporting or, more often, significant overreporting, which creates, as John McLaughlin pointed out, a situation where we are literally drowning in data with all kinds of false positives. That makes it much, much more difficult for the FBI, in particular, to have really useful real-time access to Bank Secrecy Act data. Some small fixes could do a lot in that regard.

Q: Is al Qaeda in Pakistan trying to attack some preexisting networks: the preexisting tribes and then, at the other end of the spectrum, organizations such as Hezbollah?

Prof. Paul Pillar – Al Qaeda has been doing that sort of thing in various guises for quite some time. This is not quite what you are talking about, but the acquisitions of franchisees in the form of existing organizations like the GSPC [Groupe Salafiste pour la Predication et le Combat (Salafist Group for Preaching and Combat)] group, which now calls itself al Qaeda and the Maghreb, or Zarqawi's organization in Iraq, which became al Qaeda in Iraq, are examples. It is partly an organizational infiltration that is taking place here, but, more important, it is an ideological infiltration.

Al Qaeda central and al Qaeda itself and Osama bin Laden and Ayman al-Zawahiri expound a particular transnationalist ideology that involves attacking the far enemy, mainly the United States. Over the last decade, this ideology has not had majority support among jihadists as a whole. Most of them are more concerned with specific national causes like overthrowing the Egyptian government. To the extent that this sort of infiltration, in the form of individuals who have cross memberships between organizations, can spread the transnationalist ideology of bin Laden and Zawahiri, those leaders will be very satisfied. It does broaden the particular threat that al Qaeda represents.

Prof. John McLaughlin – Matt Levitt made the point that these different groups are organizationally distinct to a degree. They are not like American organizations. They are not like corporations. They do not have a line and block chart that they all follow. They do not have membership cards. They use certain common facilities. For example, it is not at all uncommon for al Qaeda in Pakistan to borrow a safe house from a group like Lashkar-e-Taiba, one of the Kashmir-oriented groups.

I do not know what you can do other than attack the networks, the logistical and financial and communications nodes that they all draw on and use in common, even though each of them has their own kind of focus and separate part of it. So damaging one set will actually inflict trouble on the other guys as well. I do not know of a strategy other than that because they borrow from each other.

What unites them is a common enemy. It is a little harder when you are talking about groups outside of al Qaeda because, with groups like Hamas and Hezbollah, policy issues get more complicated just by virtue of where they are located and how they are protected and how they are woven into their societies. With groups that are fundamentally oriented around al Qaeda's ideals, I think you can get at them that way.

Q: *One of the basic assumptions of U.S. policy that Dr. Mahnken reiterated here today is that time is on our side. Given the inherent resiliency of networks and the difficulties we have in attacking them, combined with other issues such as demographics in Europe, the costs of the Global War on Terrorism, and challenges to our position as the world's only superpower from countries like China, is time on our side? And if that is not the case, how does that affect our strategy?*

Prof. John McLaughlin – I would not necessarily say that time is on our side. I think this will be a long effort. In a sense, we are impatient; we expect results; we do things in 1-year plans, 3-year plans, 5-year plans. The debate always arises around the time of a significant holiday. It is the Fourth of July—are they going to attack us now? It is the anniversary of 9/11—are they going to attack us now? They do not attack on anniversaries—they attack when the time is right, which means they take their time. In that sense, as long as they have a safe haven, I think we are at a disadvantage timewise. That is why I put so much emphasis on denying safe haven when I presented the three elements of counterinsurgency: deny them safe haven, destroy the leadership, change the conditions.

I know that the Pakistanis have thrown conventional power into the tribal areas, and Predators operate there, and so forth, but as long as they have got a place where they are relatively undisturbed, we have to assume that they are planning to attack us or our allies, that they are planning to try to do something in the United States at least on the scale of 9/11. In that sense, time works for them. I think having a safe haven is the key factor that affects the time variable here.

Prof. Paul Pillar – My answer to that question is time is on our side if we do not screw it up. It is on our side for one of the reasons John McLaughlin mentioned in his earlier briefing: the bankruptcy of the ideology being offered. There have been other scholars, especially a couple of French ones—Gilles Kepel, Olivier Roy—who have studied this topic in depth and basically made that same point: the failure of radical political Islam is eventually going to cause it to die away.

Another scholar, David Rappaport, whose work I admire, has looked at previous waves of terrorism of different ideologies—such as anticolonialism and the leftist movement—we were worrying more about in the 1960s and 1970s. He observed that each one died out, usually after about 40 years, largely for reasons other than specific counterterrorist efforts directed against it.

Here, I am going to have to agree with Mark Sageman: We can screw up in ways that extend the appeal of people like Osama bin Laden and Zawahiri by playing into their game of a war of civilizations, of a U.S.-led, Judeo-Christian West against the Muslim world. That is entirely the wrong approach. If we avoid mistakes like that, then time is on our side, and this too will pass.

Prof. John McLaughlin – To clarify what may sound like a contradiction between what Paul said and I said: Paul is saying that, strategically, time is on our side; I am saying that, tactically, it may not be. In other words, time may not be on our side for stopping the next attack. The question that always arises here is how will we know when this battle is over if it is a long war? There will not be a signing on a battleship. We will never stamp out terrorism, but we will know it is over when it is at a nuisance level—not that loss of life is ever really at a nuisance level—when it is at a level that is not as widespread, as global, as catastrophic, as it is now. Communism still exists, but very few people believe in it any more.

In a sense, time may not be on our side in that we do not control certain things. Go back to what I said about population increases and urbanization. The conditions that give rise to this phenomenon will continue to spawn new recruits unless we change the conditions—the third of my three points in counterterrorism strategy. There is probably a no more complicated problem in the world at this point.

Dr. Matthew Levitt – The only thing I want to add is an answer to what do we do if time is not on our side. Obviously, we have to continue to constrict the operating environment. We have to continue to engage in tactical kinds of counterterrorism because I agree that time is not on our side for that issue. But we have to be very sensitive in every move we make to make sure that we are not causing further alienation.

I believe that there is a strategic element to a tactical kind of counterterrorism in terms of how we shape the dialogue about the larger battle of ideas and do not engage in a tactical counterterrorism that will lengthen the period over which the ideology dies out. I do think the ideology will eventually die out on its own, and I do not think that we will completely shoot ourselves in the foot, but we should never underestimate our ability to do so. We will certainly make this struggle much longer and more complicated if we are not careful.

Politically, it is hard for us to avoid shooting ourselves in the foot. Just recall what happened to Senator John Kerry when he said almost exactly the same thing about needing to bring terrorism down to where it is a nuisance.

Q: *You have all worked in the intelligence community at a very senior level and spoken about the importance of diplomacy. Obviously, among the many counterterrorism tools out there, there are tensions that must be worked out in the interagency every day. With the recent National Intelligence Estimate (NIE) on Iran and weapons of mass destruction (WMD), clearly some would argue that the publication of that unclassified assessment complicated international diplomacy with respect to further financial sanctions in the third U.N. Security Council resolution. With all of your years of experience, could you comment on the prudence of continuing to publish unclassified NIEs?*

Prof. John McLaughlin – One of the big problems in the intelligence business right now is that our country does not have a common expectation of intelligence. The public generally has a cartoon image of it. I think it is wrong and ill advised to publish the judgments of National Intelligence Estimates.

We are caught in a vicious cycle, and it illustrates my first point. Those key judgments on Iran were published only because there was a conviction that they would leak. Once you yield to that conviction and say we better publish them so that at least we have some control over how they are presented, you take an important tool out of the hands of the world's sole surviving superpower.

The other problem is the way the key judgments of that estimate were written. The people who wrote them did not know they were going to be released for public consumption. Even if they had been written in a different way, the key point, made with high confidence, was that the actual weaponization program in Iran had been put on hold in 2007. If you read the fine print, that did not mean that anyone was complacent about Iran's nuclear program, which would be an important card for U.S. government decision makers to have up their sleeves in the kind of carrot–stick diplomacy that we ought to be engaging in with Iran. So, it is not the fault of the intelligence community; it is our whole system, which does not use intelligence in the kind of mature way that a superpower ought to.

Dr. Matthew Levitt – I am sitting between two people who have been intimately involved with this particular issue much more than I have, although in my time as Deputy Chief of Treasury Intel, I was on the National Intelligence Board that went through these estimates for a brief period. More to the point, at Treasury, we were at the center of the drafting of the Iran strategy. I personally could not agree more that this is the wrong product to declassify. I think that there is utility in declassifying information in the right way, in the right products, when it is not hurried, when it is thought out. The biggest problem with this was that it was declassified for fear of leaks.

When I was still at the FBI, leading one of the analytical teams up through 9/11, certain members of Congress came through FBI headquarters to give us all a pat on the back for the insane hours we were putting in. A whole bunch of us did not go because these were the same individuals who had just told Osama bin Laden about a certain satellite phone that we had been listening to, and I did not want to have anything to do with them. It is a real problem when you have to worry about people, especially Congress, leaking highly classified information. There is a time and a place and a means for engaging in declassifying material for the purposes of discussion.

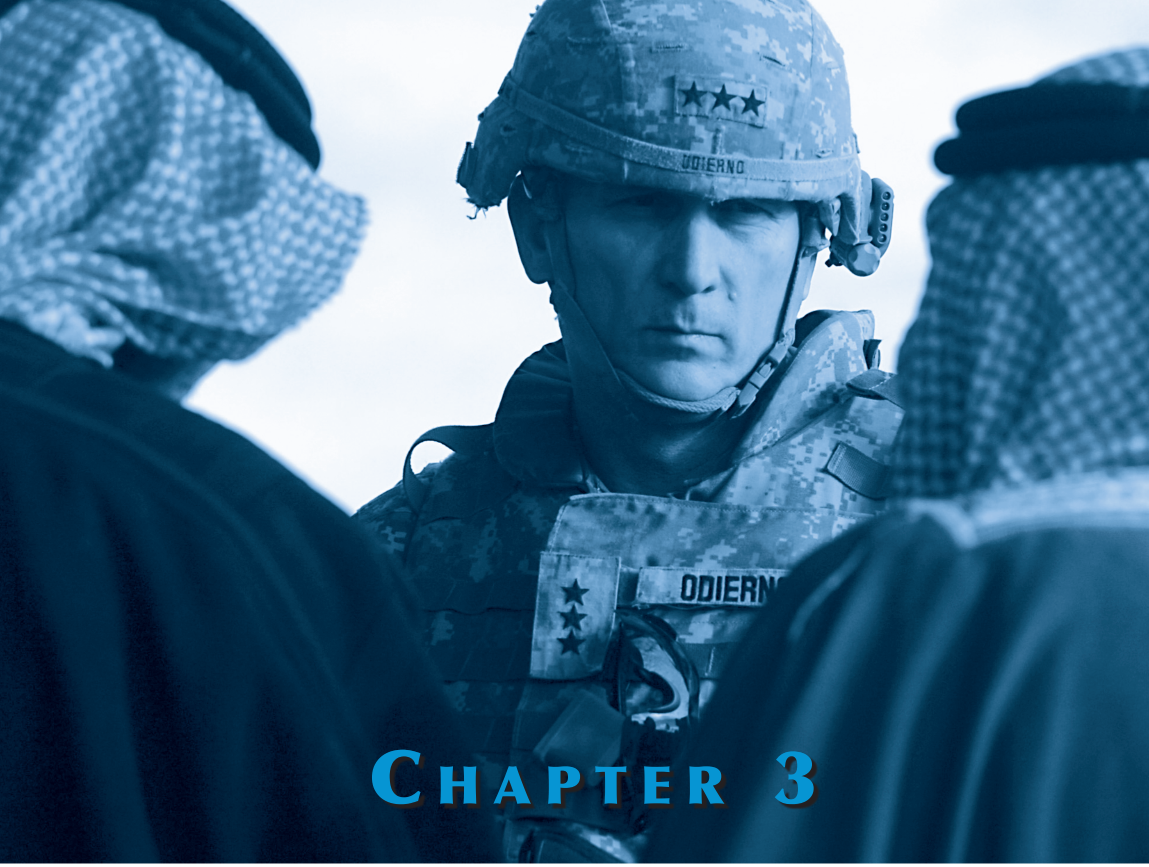
The timing could not have been worse. Our European allies had just met in London and Paris. They were pushing the third U.N. Security Council resolution harder than we were at that time. We completely cut them off at the knees, and they said to us, “You made us look like fools.” There is absolutely a very clear connection between this type of activity and the nature of diplomacy. That disclosure made our diplomacy much more difficult, gave Iran a lot of meat to use in its propaganda, and really complicated things for our allies. There is a time and a place for declassifying material, but this was not it.

Prof. John McLaughlin – The other problem, of course, is that once you publish that material, in this particular case, Iran begins a counterintelligence scrub. Where did this come from? How did this get out? How did they know that? So the likelihood of the intelligence community discovering when the program is turned back on is reduced. The groundwork is laid for another intelligence failure. That is one of the reasons that I say people do not think systemically about our intelligence system.

Prof. Paul Pillar – We do not have time to explore all of the ins and outs of this recent episode with the Iranian nuclear program. I would just make two other points. One, the Director of National Intelligence (DNI), Admiral McConnell, had already expressed his preference—even before this episode with the Iran nuclear estimate—to cut back on—if not cut off entirely—declassification of these documents. No doubt, this unhappy experience will solidify his views and probably those of his deputies as well.

Two, although I do not disagree with any of the points that my colleagues cited as the downside of the declassification, it is not a cut-and-dried issue. There are legitimate arguments that can be made for the other side, two in particular. First, leaks are inevitable. They are not going to go away. (By the way, the record of the Congress has been pretty good.) If documents are going to be of any use and be as broadly distributed in the Executive Branch as they are, we are going to have more leaks.

Second, there is an issue of the public's right to know. The public is entitled to say, "If we are spending $43 billion or whatever on our intelligence, shouldn't we, who are supposed to form opinions on things like policy towards Iran and elect leaders who are going to do smart things about it, be entitled to know the judgments on these issues by the people consuming those billions of dollars?" I think that is a legitimate position.



Chapter 3

ROUNDTABLE 2

Denying Access to and Use of WMD

3.1 MODERATOR'S SUMMARY

L. Dean Simmons

This panel focuses on denying our adversaries access to—and ultimately use of—weapons of mass destruction (WMD). The following is an overview of the problem and a preview of the roundtable discussions. Panelists Dawn Scalici, Peter Nanos, and Jim Hillman provide perspectives on how the United States is prepared to deal with this extremely severe threat.

THE THREAT

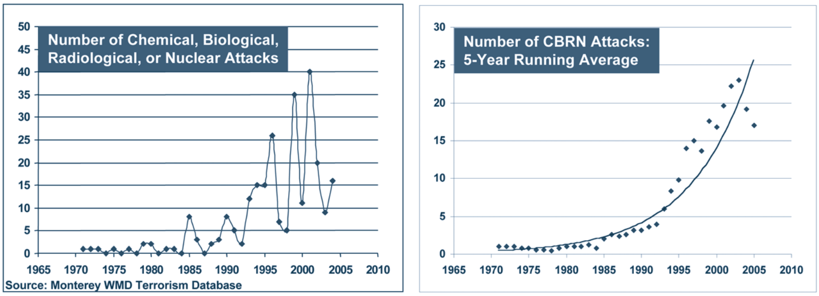
As we know only too well—given our experience on September 11, 2001—the threat posed by weapons of mass destruction, whether chemical, biological, radiological, nuclear—or in our tragic case, high explosives in the form of manned aircraft—is indeed a serious one. The human, environmental, and economic devastation that result from the use of such weapons in any American city—the prospect of which conjures our worst possible nightmares—provides justifiable cause for a concerted effort to do everything we possibly can to prevent those who would use WMD from access to these weapons and, failing that, to thwart their ability to employ WMD in any form.

Dr. L. Dean Simmons is a National Security Fellow in the National Security Analysis Department at The Johns Hopkins University Applied Physics Laboratory. A former Assistant Director in the Institute for Defense Analyses and the Center for Naval Analysis, he has expertise in systems evaluation of manned and unmanned tactical aircraft, rotary wing aircraft, surface ships, combat lessons-learned assessments for air operations in Bosnia and Kosovo, and national command and control. Dr. Simmons holds a PhD in Physics from Purdue University, Masters degrees in Physics and Operations Research, also from Purdue, and a BS in Physics from Kansas State University.

President Bush gave voice to the potential devastation in his address on the first anniversary of September 11th, when he said our enemies are actively seeking WMD and the United States is committed to preventing these efforts from succeeding:

> *"The gravest danger our Nation faces lies at the crossroads of radicalism and technology. Our enemies have openly declared that they are seeking weapons of mass destruction . . . The United States will not allow these efforts to succeed."*
>
> *— President George W. Bush, September 17, 2002*

This panel discusses some of the steps that the United States is taking to back up the President's promise. Figure 1 provides some convincing evidence that use of WMD is not an empty threat but an ever-increasing reality. The graph on the left shows the number of chemical, biological, and radiological attacks that have occurred between 1970 and 2005. The data are from the Monterey WMD Terrorism Database that the Center for Nonproliferation Studies maintains at http://cns.miis.edu/wmdt/ [1]. Although the year-to-year data show considerable variability, they clearly show a gradual upward trend. That trend is much more apparent in the graph of the five-year running average on the right; the increases are clearly exponential when plotted this way.



Number of Chemical, Biological, Radiological, or Nuclear Attacks

Number of CBRN Attacks: 5-Year Running Average

Source: Monterey WMD Terrorism Database

Number of CBRN attacks globally is increasing exponentially, although year-to-year values show substantial variability.

Figure 1 The Threat: Increasing Exponentially

THE NATIONAL STRATEGY

The national strategy to combat WMD—which the White House released in December 2002, just over a year after September 11—outlines America's approach for dealing with the WMD threat, and it declares that these types of weapons are one of the greatest security challenges facing the United States. The strategy outlines a three-pillar approach: counterproliferation to combat the use of WMD, nonproliferation to combat the spread of these weapons, and consequence management should the worst case actually happen. Roundtable IV on deterrence discusses the arguments for nonproliferation and how to accomplish it—at least partially. This roundtable focuses on counterproliferation. The National Strategy to Combat Weapons of Mass Destruction (December 2002) has three pillars and identifies three counterproliferation capabilities:

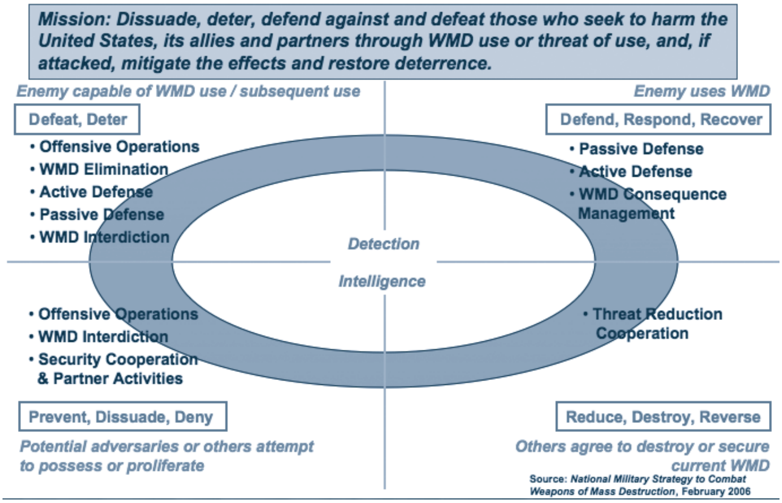
- **Counterproliferation Capabilities:**
  - **Interdiction:** prevent the movement of essential materials, technology, and human expertise to hostile states and terrorists.
  - **Deterrence:** discourage acquisition with strong declaratory policy, effective military forces, and the prospect of overwhelming response.
  - **Defense and Mitigation**: detect and destroy weapons and materials before they can be employed against the United States or our allies, mitigate effects.
- **National Strategy Pillars:**
  - Counterproliferation to Combat WMD Use
  - Strengthened Nonproliferation to Combat WMD Proliferation
  - Consequence Management to Respond to WMD Use

As Ron Luman and Admiral Olson discussed, combating WMD is a very important part of DoD's Global War on Terrorism

(GWOT). Denying access and use of WMD is one of the major lines of operation in the campaign concept.

THE MILITARY STRATEGY

The National Military Strategy to Combat Weapons of Mass Destruction [http://www.defenselink.mil/pdf/NMS-CWMD2006.pdf (Reference 2)], which the Chairman of the Joint Chiefs of Staff released in February 2006, outlines the DoD plan for combating WMD in more detail. Figure 2 summarizes the key elements of that strategy. To defeat or deter adversaries who are capable of WMD use, the United States plans to employ offensive operations, active and passive defenses, and steps to eliminate or interdict any weapons held by those adversaries.


Mission: Dissuade, deter, defend against and defeat those who seek to harm the United States, its allies and partners through WMD use or threat of use, and, if attacked, mitigate the effects and restore deterrence.
Enemy capable of WMD use / subsequent use
Defeat, Deter
• Offensive Operations
• WMD Elimination
• Active Defense
• Passive Defense
• WMD Interdiction
Enemy uses WMD
Defend, Respond, Recover
• Passive Defense
• Active Defense
• WMD Consequence Management
Detection
Intelligence
• Offensive Operations
• WMD Interdiction
• Security Cooperation & Partner Activities
Prevent, Dissuade, Deny
Potential adversaries or others attempt to possess or proliferate
• Threat Reduction Cooperation
Reduce, Destroy, Reverse
Others agree to destroy or secure current WMD

Source: National Military Strategy to Combat Weapons of Mass Destruction, February 2006

Figure 2 Military Strategy to Combat WMD

Should an adversary actually employ WMD against the United States, we will defend, respond, and recover using active and passive defenses and consequence management. Should adversaries attempt to acquire or develop such weapons, we will take action to dissuade them. If that fails, we will have the resources and strategies to prevent or deny their success. Finally, should adversaries offer to destroy or otherwise secure weapons already in their possession, we will be glad to assist them in realizing their goal.

REFERENCES

1. Center for Nonproliferation Studies, Monterey WMD Terrorism Database: http://cns.miis.edu/wmdt/

2. Military Strategy to Combat Weapons of Mass Destruction, Chairman of the Joint Chiefs of Staff, 13 February 2006: http://www.defenselink.mil/pdf/NMS-CWMD2006.pdf

3.2 WHAT IS CAMPAIGN X? — THE ROLE OF ANALYSIS IN ENHANCING COUNTER-WMD CAPABILITIES

James Hillman

A STORY

I will start by telling you a story, and then I will illustrate it by describing the work we are currently doing to analyze the problem of lost or stolen—I will call them "loose"—nuclear weapons.

First, the story: There was a couple who lived in Wyoming. They had a hunting dog, and that hunting dog was nationally famous as one of the smartest hunting dogs ever bred.

The couple decided towards the end of their lives that they wanted to go to Africa, and they decided to take their dog with them. Now, this dog was getting a little long in the tooth as well.

So, they all go to Africa, they get to where they are going to live, they settle in, and the dog decides he is going to explore the area and make sure he understands what his surroundings are like. Off he goes into the jungle, and he trots a little ways through the trees and runs into a clearing. In the middle of this clearing is a big tree, and underneath this tree is a big old pile of

Colonel James L. Hillman, USA (ret.) supervises the Advanced Technology and Concept Analysis Group in the National Security Analysis Department at JHU/APL, exploring and developing analysis tools and processes for asymmetric warfare. He served 27 years in the U.S. Army and has led development and evaluation studies in C4ISR. Colonel Hillman has partnered with the Defense Threat Reduction Agency to conduct analytic wargames to counter WMD. He received a master's degree in operations research from the University of Arkansas and a bachelor's degree in mathematics from Arkansas Tech University. He is a graduate of the Infantry Basic and Advanced courses, the Command and General Staff College, and the Army War College.

bones—they look to be lion bones. He goes over to check them out, sniffs around a bit, and as he is walking towards the bones, out of the corner of his eye he sees a tiger emerge from the edge of the jungle.

Now, the dog has been the top predator most of his life, but he recognizes a dangerous predator when he sees one. He says, "Oh my goodness, what am I going to do?" He thinks real quick, moves over to the bones, sits down, snatches up one of those bones, and starts gnawing on it. The tiger comes up behind him on his silent tiger paws—sneaking up—thinking, "I'm going to have me a bite of dog." The dog waits and waits—and just as the tiger is ready to jump, he says, "Boy, this lion is good, but what I really would like to have is some tiger."

The tiger stops and says, "Whoa," and runs out of the clearing back into the woods. Now, in this tree above these bones—way up in the top—is a monkey. The monkey has been watching all of this, and he says, "Wow, what a dumb tiger. If he only knew that dog made a fool out of him. I'm going to go tell that tiger what a fool that dog made out of him."

So the monkey gets down from the tree, runs across the clearing, goes into the woods, and chases after the tiger, who has gone deep into the jungle. When he catches up with the tiger, the monkey says, "Hey tiger. Wait a minute." The tiger turns around and in one motion snatches the monkey up by the neck and says, "I'm going to have me a bite of monkey head."

The monkey says, "Stop! I know you like monkey, but dog is much tastier—and you know, that old dog sitting back in that clearing, he made a fool out of you. He told you a story and you believed it. He made a complete fool out of you."

The tiger says, "Rrrr, that's not good. That makes me angry! Get on my back, monkey. We will go back and get that dog." So the monkey gets on the tiger's back and they track back through the jungle, back to the clearing, where the old dog is still sitting by the bones, soaking up the sun and relaxing, but with one eye open.

The dog spots the tiger with the monkey on his back as they emerge from the jungle. He says, "This is bad. Two times now. That tiger is going to attack again." He wonders, "What can I do this time?"

The old dog sits back down, turns his back to that tiger and the monkey, picks up the bone, and begins gnawing on it again. That tiger comes sneaking back up on those big old tiger paws, and just as the tiger is ready to jump, the dog says, "Where is that monkey? I'm hungry for some fresh tiger meat. I sent him out to fetch me a tiger an hour ago."

The moral: The old dog was able to dodge another attack because he recognized that the circumstances—that the world had changed a little bit.

BACKGROUND

What does this have to do with the role of analysis in defeating the threat of lost or stolen ("loose") nuclear weapons? Let me continue to set the stage with some background.

JHU/APL is working with the Defense Threat Reduction Agency (DTRA) on a project that DTRA calls Campaign X (Figure 1). DTRA—a combat support agency supporting the United States Strategic Command (STRATCOM), which has the primary Counter-WMD (CWMD) mission—has assembled a "team of teams" to combat WMD. Campaign X employs a multidisciplinary team that is conducting a cross-enterprise effort—both within JHU/APL and outside with other talented agencies—using advanced analysis methods to understand how to bring technologies to bear in an operational context to counter the potential threat of loose nuclear weapons in the hands of terrorists.

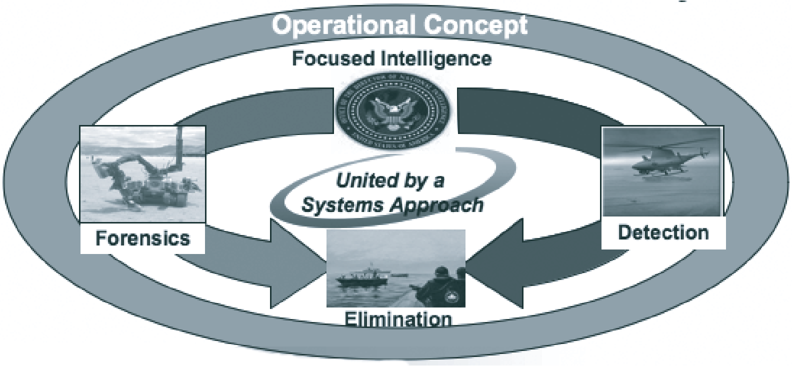


Figure 1 DTRA's Campaign X

DTRA's Campaign X combines R&D and operational expertise to create an integrated, end-to-end solution to the problem of loose nuclear material. The campaign coordinates activities, programs, and projects to provide improved intelligence, detection, forensics, interdiction options, and operational capability.

My role at JHU/APL is to construct an operational understanding of how technologies could be employed to counter this threat and how effective they would be compared with the development effort required—to determine whether or not "the juice would be worth the squeeze."

As Dr. Simmons mentioned, President Bush summarized the problem we face in his September 2002 address, worth repeating here:

> *"The greatest danger our Nation faces lies at the crossroads of radicalism and technology. Our enemies have openly declared that they are seeking weapons of mass destruction, and evidence indicates that they are doing so with determination. The United States will not allow these efforts to succeed . . ."*

To define that mission, the Quadrennial Defense Review and Strategic Planning Guidance [1, 2] laid out the following priorities for developing capabilities for countering WMD:

- Detect fissile materials at stand-off ranges
- Provide a Render Safe capability
- Provide capabilities to locate, tag, and track WMD

Campaign X is developing key enablers for the three pillars of the National Strategy on Combating WMD: nonproliferation, counterproliferation and consequence management.

CRITICAL CHALLENGES

Figure 2 summarizes the challenges we face with nuclear materials; it shows material getting lost, moving across a set of pathways labeled as proliferation pathways, and ultimately being employed for nefarious purposes—in the worst case, in the United States. The analysis problems center around identifying where the materials are, and once they get loose, where they are going.

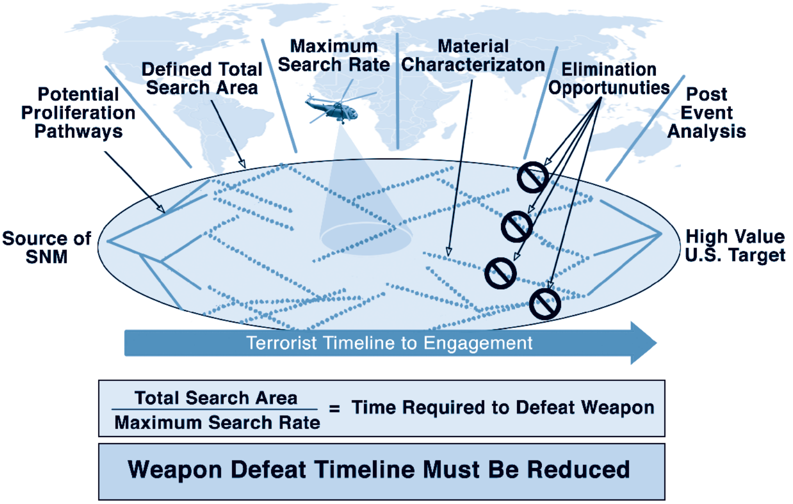

Maximum Search Rate
Material Characterizaton
Defined Total Search Area
Elimination Opportunuties
Potential Proliferation Pathways
Post Event Analysis
Source of SNM
High Value U.S. Target
Terrorist Timeline to Engagement
Total Search Area / Maximum Search Rate = Time Required to Defeat Weapon
Weapon Defeat Timeline Must Be Reduced

Figure 2 The Critical Challenge

The objective is to improve the currently limited capabilities to provide comprehensive monitoring of the location and status of nuclear materials outside the continental United States. Limitations that constrain the operational effectiveness of current CWMD technologies and methods include:

- Detection range (meters) of detection equipment
- Maximum search rate
- Number of personnel
- Weather and terrain

Current Concepts of Operations (CONOPS) rely on focusing intelligence on the "proliferation pathway," combined with maximizing equipment in the area of interest. Coping with the uncertainty creates the need for a layered approach directed at key links and nodes in the proliferation pathway to produce a system shock that causes the targeted network, node, or link to catastrophically fail, rendering it incapable or unwilling to perform its WMD enabling function.

THE CAMPAIGN X APPROACH

It is a big world, and the kinds of technologies that are available to us do not work as well as we would like or provide the coverage we need. So, what CONOPS and Tactics, Techniques, and Procedures (TTPs) can we use to help improve the chances of being able to intercept these materials? First, how do we render these materials safe? Then, if the very worst happens and there is a detonation, what can we do to recover? How do we conduct the post-detonation analysis?

Although these challenges involve a multitude of technologies, our analytic focus is not the specifics of the technologies, but rather how we can combine the operational imperatives with the technology to determine whether developing a particular set of technologies might be worth the investment. Alternatively, given a particular technology, how can we make sure that we get the best use out of that technology?

Figure 3 provides an overview of the Campaign X approach. In Campaign X, JHU/APL is applying new analytic techniques that were not previously available for conducting threat analyses. Campaign X is implementing an analytic framework to facilitate the integration of roles and responsibilities for the CWMD effort. It intends to break traditional stovepipes and focus on responding to the warfighter's needs. It considers technologies in the 2014 timeframe employed in operationally realistic scenarios to develop a full range of solutions with particular focus on technology. Campaign X analysis focuses on key capability gaps with the objective of delivering a comprehensive, integrated, end-to-end capability that eliminates the threat from loose nukes.

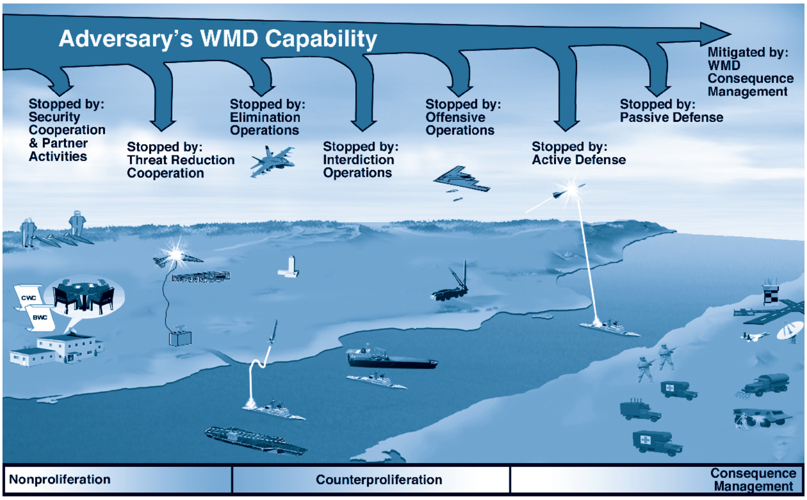

Adversary's WMD Capability
Stopped by: Security Cooperation & Partner Activities
Stopped by: Threat Reduction Cooperation
Stopped by: Elimination Operations
Stopped by: Interdiction Operations
Stopped by: Offensive Operations
Stopped by: Active Defense
Stopped by: Passive Defense
Mitigated by: WMD Consequence Management
CWC
BWC
Nonproliferation
Counterproliferation
Consequence Management

Figure 3 The Campaign X Approach

THE TIE-IN

Here is the tie-in to the story of the dog, the tiger, and the monkey. As a threat analyst, I see myself somewhat as the old dog (also a little bit long in the tooth). I would like to think that all of us analysts who are in that long-of-tooth category—or even those fresh-faced analysts who understand the traditional analysis techniques, tools, and procedures—can adapt traditional methods to the newest tools that have been developed recently and apply them to the rapidly changing circumstances of CWMD.

On the proliferation pathway against the adversary's WMD capability—from nonproliferation all the way through consequence management (Figure 3)—one of the most essential tools is the ability to game the outcomes. We are at a fortunate technology juncture because the gaming community now offers games that were originally designed for entertainment but are now sophisticated enough to allow us to adapt them quickly to a serious gaming construct.

Experts in the gaming industry now offer us the opportunity to represent our problems using the latest multimedia gaming applications. If we can help them understand the problem, they will help us represent that problem in the game. They are not interested in doing the analysis, but they offer us the ability to visualize that analysis to frame the problem. Once we have framed the problem, we can turn to the more traditional tools to address the problem from that perspective.

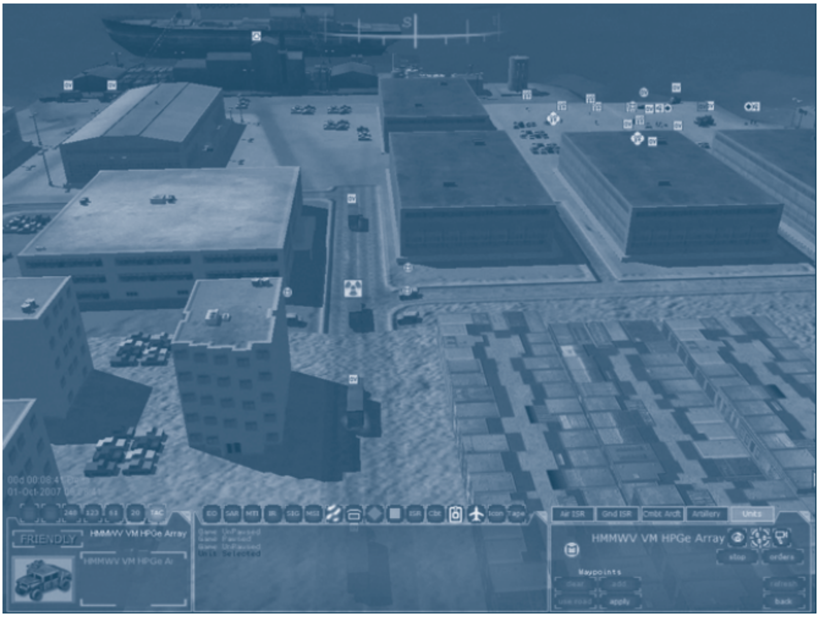
In that context, the Campaign X team is conducting a series of tabletop exercises intended to drive discussions and examine the operational contributions that candidate technologies could make if fielded. These seminar and analytic games are set in DoD-approved planning scenarios that provide analysts with:

- A forum in which to explore CONOPS for forces executing CWMD missions,
- Venues within which analysts can develop and evaluate specific TTPs, and
- Methods to develop potential operational contributions made by individual or composite groups of candidate technologies for subsequent detailed analysis using appropriate Modeling and Simulation (M&S) tools.

Ultimately, the objective of this analysis process is to determine what is the best operational contribution we can get from the technology. Alternatively, if we employ our technologies the way they exist "today" (i.e., at a particular moment in evolutionary time) given their performance capabilities, what other decisions do we need to make? We are not just asking, "How well does the technology perform in detecting nuclear materials?” We are also asking, “Given a technology that performs in this particular way, how can I optimize my ability to detect the movement of this material before it gets to the United States of America, and certainly before it can be detonated?”

Given the way that we have to employ the technologies, what kind of problems and limitations does that entail? Figure 4 displays what would happen when we detect and interdict a shipment of nuclear material in a port that is an international shipping hub. The analysis goes on to examine questions such as:

- How does it affect traffic in the port?
- What might happen if we had to shut that hub down?
- What are the economic effects?



Game UnPaused
Game Paused
Game UnPaused
Unit Selected

Figure 4 Interdiction of Radiological Materials in an International Shipping Port

CONOPS centering on how to employ the available technologies to keep an interdicted nuclear shipment from getting out of the pier. Many other CONOPS could be pursued in a similar way. This is an example of how to frame the analysis. The follow-on necessarily has to be the detailed representation in an M&S environment using tools and procedures to begin the tradeoff analysis that examines what is the best technology in which to invest to implement the capability depicted in that CONOPS. With the new tools we are using today, we are better able to conduct agile analyses that readily adjust to rapidly changing technologies, world circumstances that might affect the availability of WMD, and the adversaries that would exploit them.

3.3 CWMD RESEARCH AND DEVELOPMENT OVERVIEW

Peter Nanos

INTRODUCTION

Before I give you my overview of the R&D work we are doing at the Defense Threat Reduction Agency (DTRA), I want to thank Jim Hillman for his perspective on the counter-WMD analytical challenges we face. The most important thing to remember is that understanding how the various technologies play together—and more importantly, which ones are going to work and are worthy of investment and how to distribute that investment, particularly in the dollar-constrained world we now face—is extremely important.

The R&D challenge—like the analysis challenge—must consider all aspects of the CWMD mission: Chemical, Biological,

Dr. G. Peter Nanos, Jr., is the Associate Director of Research and Development at the Defense Threat Reduction Agency (DTRA), where he is responsible for combating Weapons of Mass Destruction (WMD) by providing R&D capabilities to reduce, eliminate, counter, and defeat the threat of WMD and mitigate its effects. Previously, Dr. Nanos served as Director of Los Alamos National Laboratory. A retired Navy Vice Admiral, Dr. Nanos commanded the Naval Sea Systems Command and was the Director for Strategic Systems Programs. A Trident and Burke Scholar graduate of the U.S. Naval Academy, Dr. Nanos received a bachelor's degree in engineering and a Ph.D. in physics from Princeton University. His awards and decorations include the Navy Distinguished Service Medal and the Legion of Merit.

Radiological, Nuclear—including dirty bombs and improvised nuclear devices—and High Explosives (CBRNE):

- Chemical Weapons – cheap and easy to make, not very effective
- Biological Weapons – use available technology and are potentially catastrophic if properly used
- Radiological Devices – dangerous to assemble with high contamination impact
- Nuclear Weapons – difficult to acquire, devastating in use
- High Explosives – easily available materials with many ways to deliver

To conduct R&D in countering the CBRNE threat, DTRA has established the R&D Enterprise. This briefing provides an overview of DTRA's R&D Enterprise, including:

- Mission and Organization
- Investment Strategy
- Top Challenges and Major Programs
- Technologies Transitioned to the Warfighter
- Future R&D

The fundamental mission of DTRA's R&D Enterprise is to identify, conduct, and deliver innovative science and technology (S&T) through systematic, risk-balanced processes that enable America to combat WMD. DTRA's system engineering activities provide for Research, Development, and Acquisition (RD&A) to support the needs of Combatant Commanders (COCOMs), the Services, and DTRA. The Agency conducts 6.1 basic research (in DoD terms); at the same time, DTRA has a combat support mission supporting combatant commanders in the field in country.

RESEARCH STRATEGY

DTRA's research strategy is to focus on four technology areas through the following organizations:

- **Basic and Applied Sciences (RD-BA)** – conducts basic research to reduce, eliminate, counter, and mitigate the effects of WMD by advancing fundamental scientific knowledge and applying the best practices in system engineering. RD-BA's top S&T challenges are to cultivate world-class research talent and promulgate systems engineering practices throughout DTRA. As DTRA's basic research arm, the RD-BA organization not only fosters basic and applied science, but it also funds systems engineering, determining where the investment needs to go and how to approach counter WMD problems systematically.

- **Chem/Bio Technologies (RD-CB)** – manages and integrates the development, demonstration, and transition of timely and effective chemical and biological defense solutions for DoD while serving as the focal point for S&T expertise. The entire S&T investment in the DoD outside of the Defense Advance Research Projects Agency (DARPA) in chem-bio defense is in this organization.

- **Counter WMD Technologies (RD-CX)** – focuses on developing innovative technologies to actively counter the full spectrum of CBRNE threats. Its top priority is achieving an effective level of lethality in WMD counterforce weapons while minimizing collateral effects. Interdicting and defeating WMD agents is a complex challenge. For example, RD-CX recently conducted tests to determine how to destroy a Scud missile launcher loaded with chemical or biological weapon agents without disbursing the agents and killing innocent populations. The challenge is not only to destroy the delivery vehicle but to prevent collateral damage so we do not lose the hearts and minds of the innocent citizens who populate the areas near the threat.

- **Nuclear Technologies (RD-NT)** – researches, develops, and demonstrates technologies that mitigate the threat and effects of nuclear and radiological attacks and enhance the safety, security, survivability, and performance of U.S. nuclear assets and facilities. Its top challenge is standoff nuclear detection. Its mission encompasses consequence management—understanding how to mitigate the effects of nuclear devices—detecting nuclear materials, and conducting the large-scale simulations, computing, and modeling necessary to support the enterprise.

In addition, DTRA sponsors the R&D Innovation Office, which is the hunter-gatherer of innovative technologies and capabilities. DTRA devotes funds every year to pinpoint technologies that are ready to transition, to find out what other research organizations are developing, to spur small business innovations, and to foster international collaboration by surveying worldwide capabilities and identifying opportunities to fill DTRA technology gaps. This year, the Innovation Office has created a virtual laboratory where we can post fundamental research questions and get scientists from all over the world responding to unclassified scientific issues. The Innovation Office is also scrutinizing where the next Silicon Valley might arise—whether it is in this country or overseas—to be the first to recognize cutting-edge technologies that are going to succeed.

Innovations that have transitioned from this program include:

- "Pixel interrogation" technology that enhances images to provide the ability to see a pistol in a metal box
- A chemical detection device that can be swiped over materials to determine what type of chemical agent might be present in, for example, a variety of different robots and detectors
- Rubber-cased explosives that will shred an improvised explosive device (IED) without actually detonating the explosive

The COCOMs provide the technology requirements "pull," which DTRA augments with M&S studies and operations analyses. The technology "push" comes from universities, laboratories, and many industrial partners, including small companies. The systems engineering strategy takes a holistic approach to mesh with the national strategy of nonproliferation, counterproliferation, and consequence management. Systems-engineered concepts develop into campaigns that aim to deliver warfighter capabilities.

THE R&D CAMPAIGNS

DTRA investments include research organized into the following six campaigns:

- Improving Situational Awareness
- Controlling WMD Materials and Systems Worldwide
- Defeating the Threat from Loose Nuclear Weapons
- Deterring the 21st-Century WMD Threat
- Enabling Others to Protect the Homeland
- Eliminating WMD as a Threat to the Warfighter (Campaign X)

DTRA R&D takes an integrated approach to conducting these campaigns. As shown in Figure 1, combating WMD spans all of the adversary's means of delivering WMD threats, from detection, interdiction, and elimination to consequence management, particularly in the chemical/biological area.

Security cooperation and nonproliferation are also essential areas in which we invest R&D resources. If we do not pursue efforts to suppress the sources of chemical/biological weaponry through security co-operation, virtually everything COCOMs do in the global initiatives to combat nuclear terrorism can be jeopardized because trouble can arise in too many places to control. The partnership with the intelligence community is extremely important as well. No matter how good our detectors of WMD are, the Eurasia land mass is a huge place. (Think of antisubmarine warfare in the 1940s with a 2,000-yd-range sonar.)

1. Situational Awareness

End State – Improve knowledge and information to permit execution of successful courses of actions

R&D Investments – Common Operating Picture for interagency connectivity and an integrated architecture; Decision support/predictive CBRNE decision support tools; Strategic assessment; CBRNE and Protection & Mitigation Assessment tools

2. Control WMD Materials and Systems Worldwide

End State – Provide effective tools to prevent proliferation of WMD and WMD related capabilities

R&D Investments – Nonproliferation training tools for Arms control/ Confidence and Security Building measures; Regional training tools (customs, culture, language); Doctrinal and planning support tools; Sensors and detectors; Train-the-trainer systems

3. Eliminate the Threat of WMD to the Warfighter

End State – Provide an integrated capability to eliminate the WMD threat to the Warfighter

R&D Investments – Personal Protection Equipment; System Survivability in environments where WMD use has occurred; Response, mitigation and restoration in contaminated areas; Technology and subject matter expertise to identify vulnerabilities

4. Protect the Homeland from WMD

End State – Provide an integrated capability to eliminate the threat from loose (lost or stolen) nuclear weapons

R&D Investments – CBRNE decision support tools; Bio-surveillance; Radiation hardening technologies; Blast mitigation technologies; Bio-medical prophylaxes; CBRN treatment technologies; CM and restoration technologies

5. Transform the Deterrent

End State – Establish DTRA role in supporting USSTRATCOM as it transforms the nuclear deterrent.

R&D Investments – CBRNE Decision Support Tools; Sensors and Detectors; Experimentation Facilities; Test/experimental instrumentation; M&S of Weapons Effects; Specialized Weapon Designs for Combating WMD; Advanced Energetics

X. Defeat the Threat of Loose Nuclear Weapons

End State – Provide an integrated capability to eliminate the threat from loose (lost or stolen) nuclear weapons

R&D Investments – Common Operating Picture; Sensors and Detectors, fixed sites and portable applications; Specialized Weapons Design; Doctrinal Support; Strategic Assessments; CBRN Neutralization and Destruction Technologies

Figure 1 DTRA R&D Campaigns

Situational Awareness

The campaign to improve situational awareness means cultivating a creative partnership with the intelligence communities. To meet the end state of improved situational awareness that permits successful counter WMD actions, we need to know where to look; a Common Operating Picture (COP) that provides interagency connectivity and an integrated architecture is essential. DTRA is also investing R&D resources in developing tools needed for decision-support, strategic assessments, and protection and mitigation assessments.

Controlling WMD Systems Worldwide

Controlling WMD systems worldwide requires not only sensors and detectors but also nonproliferation training tools for arms control and measures to build security confidence; regional training tools for understanding the customs, culture, and language; and doctrinal and planning support tools, as well as systems to train the trainers.

Eliminating the WMD Threat

Eliminating the threat of WMD to the warfighter requires R&D investmenting:

- Personal protection equipment
- System survivability in environments where WMD have been used
- Response, mitigation, and restoration in contaminated areas
- Technology and subject-matter expertise to identify vulnerabilities

Protecting the United States from WMD requires R&D investment in improving defense support of civil authorities through shared training, planning, tools, and technologies. Tools must be developed to support CBRNE decision-making, bio-surveillance, and biomedical prophylaxes. We are developing technologies for radiation hardening, blast mitigation, CBRN treatment, and restoration.

The 21st century mantra for deterrence is transforming the deterrent. In Campaign 5, DTRA is supporting USSTRATCOM in the transformation of the nuclear deterrent by investing R&D resources in new CBRNE decision-support tools, sensors, and detectors; experimentation facilities including new testing instrumentation; M&S on weapons effects; specialized weapon designs for combating WMD; and development of advanced energetics.

The campaign to limit the threat that Jim Hillman described, Campaign X (defeating the threat of loose nuclear weapons), focuses on integrating tools to limit the threat of lost and stolen nuclear weapons and materials and solving problems if our troops in the field have to face WMD. DTRA investments focus on developing a COP, sensors and detectors (both at fixed sites and portable), specialized weapons, strategic assessments like the analyses Jim Hillman described, and CBRN neutralization and destruction technologies.

TOP CHALLENGES AND PROGRAM AREAS

The complexity and evolution of the threat demands that we change our investment to meet the most pressing challenges. In response, DTRA is concentrating its efforts in areas such as:

- Deployable Technical Intelligence
- National Technical Nuclear Forensics
- Active Nuclear Interrogation
- Hard and Deeply Buried Targets
- Advanced Energetics for Weapons
- WMD Threat Research and Analysis Center (WTRAC)
- Chem/Bio Applied Technology Development
- Transformational Medical Technologies Initiative

I will not go into detail on all of these, but some of the highlights are the Deployable Technical Intelligence Laboratory and the National Technical Nuclear Forensics efforts.

Deployable Technical Intelligence Laboratory and National Technical Nuclear Forensics

When DoD needed laboratories to identify the makers of weapons and track them back to their hiding places, DTRA created labs that could go forward into Afghanistan and Iraq. DTRA has since also built weapons forensics laboratories for the Department of Justice and others who wanted a mobile laboratory capability.

The National Technical Nuclear Forensics mission in DoD is to provide rapid identification: if a weapon goes off, get the sample, get it to the laboratory, find out who did it, and be able to support the attribution mission. A rapid-response forensics capability is essential for knowing who the enemy is and responding appropriately and swiftly.

A robust forensics capability is even more important if there is a chance that there might be another attack coming out of the same supply chain. We have to be able to respond quickly but accurately in possibly ambiguous circumstances. For example, say there were 10 possible sources for a nuclear or radiological event. It is a daunting challenge to search for 10 possible sources the morning after. We need to winnow them down to a few very rapidly so we can adequately deploy our assets. In this case, getting an answer within 24 to 48 hours to define the battlespace is extremely important.

Developing an accurate, rapid, and reliable capability to characterize post-detonation materials and provide prompt data for a nuclear or radiological event requires:

- Prompt data collection
- Ground-based gamma collection and alternative signatures for yield determination

- Improved personal protection equipment for manual collections
- Sample debris collection
- Automated collection systems
- Ground sample Advanced Technology Demonstration
- Sample debris analysis
- Deployable analytical and screening capabilities
- Rapid analytical technologies
- Data evaluation and knowledge management
- Database development
- Prompt phenomenology data evaluation

Active Nuclear Interrogation

Accurate detection of nuclear materials is one of the greatest technical challenges we are facing. Right now, our nuclear detectors are point detectors that have a range of a few tenths of a meter at most. If the radiological source is shielded, the range is considerably less than that. If you think about what you would do if you had to find a weapon somewhere in the Eurasian land mass, your best option, without prior knowledge of exactly where it is, is a million men with Geiger counters walking fingertip to fingertip down the Eurasian land mass.

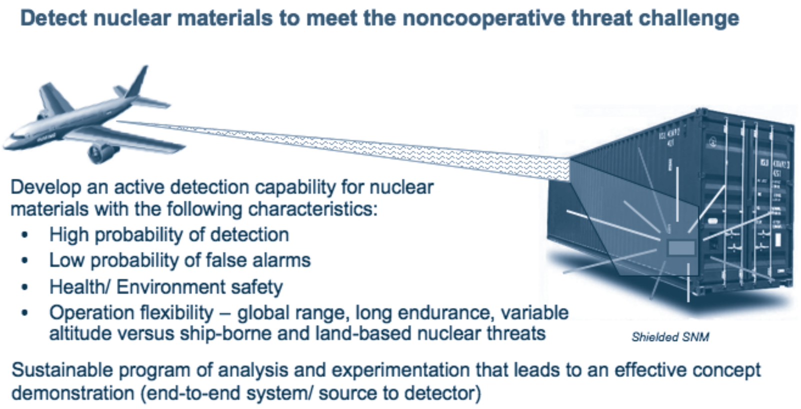
We do not have standoff, high-search-rate detection capability for fissile material right now, and this is an important area for us to invest in and get into our arsenal. The good news is there are technologies that are promising, and DTRA is pursuing several different active technologies. The challenge is to develop an active detection capability for nuclear materials with the following characteristics:

- High probability of detection
- Low probability of false alarms
- Health/Environment safety

- Operation flexibility – global range, long endurance, variable altitude versus shipborne and land-based nuclear threats

Three different approaches DTRA is taking have a goal of 5-km detection capability (Figure 2):

- Bremsstrahlung Interrogation
- Muonic X-ray Detection
- Proton Interrogation



Detect nuclear materials to meet the noncooperative threat challenge

Develop an active detection capability for nuclear materials with the following characteristics:

- High probability of detection
- Low probability of false alarms
- Health/ Environment safety
- Operation flexibility – global range, long endurance, variable altitude versus ship-borne and land-based nuclear threats

Sustainable program of analysis and experimentation that leads to an effective concept demonstration (end-to-end system/ source to detector)

Figure 2 Standoff Nuclear Interrogation

Advanced Energetics For Weapons

You just cannot blow up a 55-gallon drum full of anthrax. The heat capacity of anthrax is too great. Defeating the agent in cases like that is a hard technical problem. In the Advanced Energetics effort, DTRA is looking for a way to increase the energy content of devices to increase their effectiveness in defeating WMD, especially in hard and deeply buried WMD facilities.

Because we are interested in defeating WMD agents, DTRA has become the major DoD organization focusing on energetics, developing advanced weapons systems like thermabaric hellfire, thermabaric skip bombs, and the massive ordinance penetrator.

Energetics is really the key to defeating WMD—actually killing the agent and not disbursing it. Very little basic research in energetics is being conducted anywhere else; DTRA has taken on a major role in that responsibility and is pushing forward with it—just one example of the initiatives DTRA is taking.

WMD Threat Research and Analysis Collaboration (WTRAC)

DTRA is initiating an effort to start up a partnership with the intelligence communities to develop new techniques to characterize complex proliferation threats. Through intelligence sharing, the thrust is to develop a collaborative capability that combines intelligence collection and all-source analysis expertise with national science and engineering R&D capabilities; the goal is to:

- Integrate DTRA, the Defense Intelligence Agency (DIA), and other expertise in a multidisciplinary effort to address adversary WMD developments
- Develop innovative collection and analysis strategies and technical capabilities to understand adversary WMD
- Refine the capability to detect, characterize, and counter adversary WMD, using DoD's Hard Target Research and Analysis Center (HTRAC) as a model

The significance of this effort is that DTRA is not part of the intelligence community; it is a Title X activity. However, DTRA can contribute its skills in modeling, simulation, high-end computing, and knowledge of the technologies associated with WMD. DTRA is taking those assets inside the intelligence community to help them do their job; intelligence experts can combine DTRA's expertise with their information to achieve better real-time information for the pursuit of WMD. DTRA's philosophy is if we have knowledge assets that will help, we must take the initiative to put those assets to work within the intelligence community.

Transformational Medical Technologies Initiative

This major initiative focuses on revolutionary technologies to counter emerging biological threats, in anticipation that our adversaries will engineer pathogens as WMD. Scientific thrust areas include genomic identification, small-molecule discovery, protein-based therapeutics, nucleotide therapeutics, and human immune enhancement. Through a process of integrated cross-cutting technologies (Figure 3), including microarray technology, bioinformatics, proteonomics, and genomics, DTRA and the Chemical and Biological Defense Program are pushing for deliverables such as broad-spectrum treatments for hemorrhagic fever viruses and intracellular bacterial pathogens as well as genetic identification and analysis.

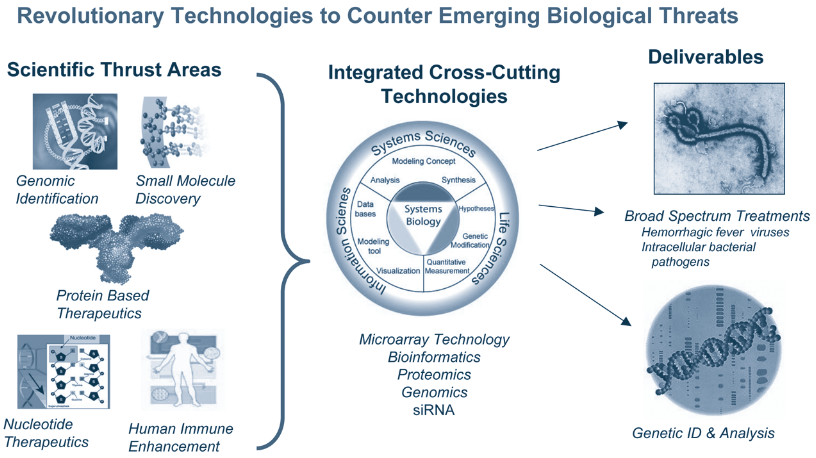


Figure 3 Integrated Cross-Cutting Technologies

Out of the Human Genome Project came computational biology and large-scale simulation. These technologies are enabling people to develop methods to turn nonpathogens into pathogens, making production of biological weapons relatively much easier once the technology is understood. Given that it can take years from the time we identify a pathogen to when we get a new drug for it in the system, DTRA is accelerating a double-pronged initiative: (1) speed up the fundamental process of drug development and (2) create drugs that are proven against a range of pathogens within a given class to provide some capability before the threat really materializes. This is an aggressive initiative, in which DRTA is inviting the whole spectrum of the medical community to participate—large and small pharmaceutical industries, universities—any person or organization with a good idea can answer one of DTRA's Broad Agency Announcements (BAAs) and have a reasonable shot of being part of this process.

Basic Research

DTRA is sponsoring fundamental research that is needed to reduce, eliminate, counter, and mitigate the effects of WMD. DTRA is investing in high-payoff S&T, balancing resources between evolutionary and potentially revolutionary advances. In this regard, DTRA is developing strategic partnerships and forging long-term alliances with universities to train the next generation of scientists and revitalize the skill base and programs that increase the flow of new ideas.

As mentioned previously, very few developed technologies will produce large game-changing increments of performance improvement in combating WMD. Therefore, DTRA's biggest challenge is to leave no technology unturned. In this area, if people have wild ideas on how to help the problem, DTRA will listen to them seriously.

TECHNOLOGIES THAT HAVE TRANSITIONED

Among the technologies that DTRA's R&D Enterprise has transitioned into service are the following:

- Electromagnetic Pulse (EMP) Radiation-Hardened Chip
- Thermobaric Weapons (BLU-121 A/B)
- Smart Threads Integrated Radiation Sensor (STIRS)
- Massive Ordnance Penetrator (MOP)
- Angel Fire & Constant Hawk Wide-Area Persistent Surveillance Programs
- Biological Combat Assessment System (BCAS)

WHAT IS ON THE HORIZON?

Considering that our current nuclear detectors provide only alertment and not tracking as well as our much higher capability in missile defense and the antiair warfare missions, where we can track 2,000 or 3,000 objects, we need to apply that technology to WMD problems. If we include all the large port area background traffic, all the vehicles in a crowded downtown metropolitan area, we are looking at 30,000 to 40,000 tracks to discern and watch all the time. This is probably two or three orders of magnitude greater than what we have demonstrated in our overall ability to manage track files and do battle management.

WMD scenarios, such as the port detection mission, represent an urgent need for a major upgrade of our capability over the next several years. It will bring with it the need for high-performance computing to do major simulations and agent-based modeling, particularly for consequence management. Once a device goes off, or a major disaster happens, we have to be able to make the calculations to find out what happens to the infrastructure, and conduct the agent-based simulations to find out where the people go. It is a huge computational problem. Therefore, the challenge is to provide the warfighter with an enhanced WMD threat analysis and assessment capability for a persistent adversary. This will require two major thrusts:

- **Integration of the Three Combating WMD Pillars (CP, NP, CM)**
  - Integrate the intelligence, surveillance, reconnaissance, and consequence management activities
  - Produce common operational picture with net-centric interfaces
  - Implement integration of sensors and taggants
  - Monitor numerous adversary tracks, sensors, and movements to predict hostile intent
- **High Performance Computing for Science-Based Applications**
  - Develop integrated modeling and simulation solutions to CWMD threats

- Create decision support alternatives for CWMD operations
- Provide predictive analysis and consequence management

CONCLUSION

Although DTRA's focus is on the warfighter, it fully supports cooperative work across all agencies. As we have seen, DTRA's major initiatives include nuclear detection, forensics, medical technology transformation, large-scale computing for weapons effects, energetics, and penetrators. The next major thrusts are information integration and fusion, the ability to track 100,000 objects in major parts of the world all the time, and the application of large-scale M&S to provide advanced, real-time battle management.

3.4 NCTC ROLES IN EDUCATING OUR ALLIES AND PARTNERS TO DETER/DETECT/DENY TERRORIST ACCESS TO WMD

Dawn Scalici

THE WMD CHALLENGE

As discussed in the previous session, one of the greatest security challenges we face is WMD in the hands of terrorists. We know the threat is real because terrorist groups have already demonstrated their capability to carry out at least small-scale CBRN attacks using poison and improvised chemical devices. Not surprisingly, al Qaeda and al Qaeda in Iraq appear to have dedicated the most effort to obtain a sophisticated CBRN capability, given that these groups are trying to deliver shock, awe and headlines around the world. It is also crucial to understand—as John McLaughlin noted in Roundtable I—that al Qaeda thinks and acts strategically with a very long-term view. It acts with a great deal of patience and resolve, a case in point being the long time span between the first attack on the World Trade Center in 1993 and its tragically successful attack in 2001. Given the history of al Qaeda's plotting in the WMD arena, we must assume that it retains the intent to gain a true WMD capability.

Ms. Dawn Scalici serves as the Deputy Director for Mission Management at the National Counterterrorism Center (NCTC). A career CIA officer, she has served as Chief of the Al-Qa`ida and Sunni Affiliates Group and the Director of Central Intelligence Representative to the National Security Council and briefer to the Deputy Secretary of State while concurrently serving as the Special Advisor to the Ambassador-at-Large for the New Independent States. She has expertise in political, military, economic, and leadership analysis for countries within the European and Eurasian spheres, and high-technology industries, Soviet strategic forces, arms control, and nuclear security issues. Ms. Scalici has an educational background in Marine Science and Biology.

BACKGROUND

Documents recovered in Afghanistan show that al Qaeda prior to 2002 had launched a sophisticated biological weapons program, aimed primarily at gaining the capability to launch mass casualty anthrax attacks. In addition, documents indicate that al Qaeda had trained Mujahideen and produced and tested mustard agents, Sarin, and VX. Moreover, statements by Osama bin Laden and his senior deputies indicate that they have a strong intent to gain a nuclear capability, either by developing that capability on their own or acquiring a weapon.

Since those documents were discovered in 2002, Mujahideen associated with al Qaeda have continued their CBRN-related activities abroad, including in Europe, although many of their plots have been disrupted. The poisons handbook that has been on the Internet for years appears to have provided some of the instruction for the simplistic CBRN type plotting that we have seen to date.

We successfully disrupted Iraqi extremists operating in Iraq in late 2003 and early 2004, but the al Qaeda leader in Iraq, Abu Ayyub al-Masri, in a statement issued in late 2006 on the Web, implored physicists, chemists, nuclear scientists, and explosives engineers to come to Iraq to test the "unconventional bombs of the so-called germ or dirty [variety]" against American forces.

Given the kind of technical expertise available in the scientific community and openly available on the Web, we must assume that the prospect of a true WMD attack in the future is one that we have to guard against.

When considering al Qaeda's capabilities today, we have to examine it within the framework of how it has re-consolidated its position in the last two years. As discussed earlier in this symposium, by consolidating much of its leadership and plotting within the federal tribal areas of Pakistan, al Qaeda has been able to reestablish a safe haven of sorts—a safe haven from which it is recruiting, training, and dispatching operatives to the West. While Al Qaeda has scored many successes in metastasizing its organization and ideology in many areas around the world, its most sophisticated plotting against the West is guided by a small cadre of extremists operating within the frontier areas of Pakistan.

NCTC'S ROLE

Given the severity of the threat, the U.S. government is pursuing a comprehensive strategy to counter WMD terrorism in all of its dimensions. NCTC plays a key role in this regard because of its leadership in the area of strategic operational planning for the U.S. government to prosecute the Global War on Terrorism.

Vice Admiral Joseph Maguire, who provides his perspective in the Session VIII panel on integrating strategy, analysis, and technology in support of the U.S. war on terrorism, will provide much more detail on the role NCTC is playing in strategic operational planning. For this panel, the following is a summary of the key tenants of the strategy NCTC is carrying out in cooperation with other partners in the U.S. government, as well as with foreign partners, to address the threat of WMD terrorism.

INTELLIGENCE GATHERING

Step one of the strategy is determining the terrorist groups' intentions, capabilities, and plans to develop or acquire a WMD capability. Much of our activity currently lies within the Intelligence Community, using open source as well as clandestinely acquired information. The Intelligence Community is working on this issue more closely and collaboratively now than probably at any time in our history. An example of this is the unique partnership recently formed between NCTC and CIA to pool our expertise on WMD terrorism. By pooling our efforts, we are better able to inform the policy makers and support the operators.

We face many challenges in addressing terrorism, including WMD terrorism, not the least of which is the fact that the terrorists are using our own technology against us. So, one of our greatest challenges is keeping up with the terrorists—and optimally getting ahead of them—on the technology front.

DENYING ACCESS

The second key tenant of our strategy is denying the terrorists access to WMD materials and expertise and the enabling technologies they would need to gain a WMD capability. Along with our foreign partners, we have done a lot of work to try to secure WMD-relevant materials around the world and to monitor the proliferation of WMD expertise. As a government, we have extensive experience working with foreign partners to try to secure fissile materials around the world. No doubt, many of you in the audience have been part of those efforts at some point in your career.

As the threat of terrorism has loomed, we have worked even harder to try to secure a range of materials—including pathogens and toxic industrial chemicals—to better protect our interests at home and abroad. However, this has been a challenge in part because of the dual-use nature of many of these materials—the chlorine tank attacks in Iraq being a good example of this. To respond to this challenge, we have established a layered defense–securing materials at their point of origin; blending classic counterproliferation and counterterrorism activities to identify and disrupt terrorists' attempts to acquire relevant materiel and technology; and shoring up our defenses along our borders as well as at key infrastructure sites around the United States.

DETERRENCE AND PERCEPTION

Along with these activities, we also must help to deter terrorists from employing WMD. In this regard, we must not only shore up our defenses, but we must also demonstrate our resolve in doing so. Terrorists' perceptions of our security posture help drive their actions. They operate, it appears, hoping for a high probability of success. Therefore, the deterrence effects resulting from building up our security probably have thwarted some of their plotting to date.

Part of our job is to eliminate the element of surprise, because that is the realm in which terrorists like to operate. Consider what al Qaeda could have achieved in the 2001–2002 timeframe if they had attempted to carry out—or carried out—a mass casualty anthrax attack: We would have been unprepared as a nation. In response to the anthrax letter attacks of 2001, as well as our discovery of al Qaeda's dedicated anthrax program in Afghanistan in 2002, we built up our defenses by educating our medical community and stockpiling antibiotics.

Moreover, we advertised our actions loudly and clearly. By doing so, we took away some element of surprise from the terrorist enemy but also, importantly, built up our own ability to mitigate the consequences of a WMD-type attack in the future. So, our range of deterrence strategies must take into account our ability to mitigate the effects of a terrorist attack using WMD and to ensure our capacity through both analysis and technical forensics to determine the perpetrator of any such attack to help prevent follow-on attacks, as well as to inform U.S. response options.

We must also make clear that our determination to respond overwhelmingly to any such attack is never in doubt. This is an essential part of our strategy, in addition to maintaining our capability to work with partners at home and abroad to detect and to disrupt any terrorist plot to use WMD once it gets underway.

INFORMATION SHARING

I want to conclude with a discussion of the importance of sharing our information—and sharing our information relatively broadly—in contrast with the conventional handling of intelligence. To counter the terrorist WMD threat, we must disseminate the knowledge that we acquire on terrorist WMD intentions and activities to foreign governments, to the military, to first responders, and to industrial security experts so that they are better aware of the indicators of CBRN or WMD activity to help protect our interests. On this point, I posit that this is not just a game of secrets. Just as it is important for us to try to identify and to disrupt terrorist plotting with WMD, it is also our responsibility in the Intelligence Community to share information on how the terrorists think and how they operate so that we can better respond, not only here in the United States, but also with our partners against terrorism worldwide.

A case in point was our discovery in 2003 of al Qaeda affiliates that were planning an attack with an improvised chemical device–a cyanide-based chemical weapon that could have proved quite effective, at least within closed spaces such as subway cars. We took that knowledge and we informed the community openly and broadly. We built mockups of the devices, and we shared the information with federal, state, and local partners. The impact of that was that we built up our defenses in many of our major subway lines, including installing chemical detectors and making other modifications to subway cars. It is an example in which we translated intelligence and intelligence analysis into actions on the ground to help protect our interests.

We have been sharing information in a variety of other ways as well. In concert with CIA, NCTC has developed handbooks that provide information on threats such as radioactive sources. We have translated these handbooks into 15 languages; they are part of training programs to a number of foreign governments, to their first responders, and to their law enforcement agents, to instruct them on the indicators of terrorist activities in CBRN so that they can better respond.

We have also assembled a variety of kits that contain CBRN simulants that we can use to train law enforcement officers and first responders on how to identify chemical, biological, radioactive, and nuclear materials. For example, these kits can demonstrate what impure sulfur mustard looks like, its range of colors, and its smell to help identify threats.

If you were to conduct a raid on an apartment and discover possibly hazardous materials that could be used as terrorist weapons, the kits help in identifying them. In addition, the kits are helpful in identifying materials such as red mercury, which has been part of many scams that have taken place in the terrorist arena.

We have also prepared flip charts that we have shared with customs and border officials to help them identify the kind of materials one might see in a trunk of a car coming across the border, or perhaps even in suitcases, as well as the kind of questions one may ask sources regarding CBRN materiel and activity. We have shared these training materials broadly–providing them, for example, to 911 operators to include as part of their call log so they are prepared to ask questions relevant to CBRN activity.

CONCLUSION

In addition to coordinating intelligence from a variety of sources, we must deny terrorist access to WMD through a layered defense that secures materials, borders, and key infrastructure sites; and clearly demonstrate to the terrorists the deterrence measures we are putting in place. A significant part of our effort also lies in information sharing. NCTC has been working to find the means to share the knowledge that we have gained through intelligence; filter it to focus on detecting, deterring, and denying access to WMD; and share it broadly amongst federal, state, and local partners so that as a nation we are better able to respond. We also share that information with key foreign partners around the world. NCTC has gathered intelligence, put it into an unclassified forum, created counterterrorism tools, and distributed them to our allies and partners who can use them to secure CBRN materials and deter and disrupt terrorist efforts to obtain weapons or materials.

3.5 QUESTIONS AND ANSWERS HIGHLIGHTS

Transcripts

Q&A

Q: *In a scenario in which you have confirmed that terrorists have planned a series of attacks with WMD, and one of the attacks has already occurred, what are the challenges in comparing the intelligence; deciding on the appropriate countermeasures; assembling the appropriate forces; and determining whether, where, and when to respond to the next terrorist attack with a WMD? Do you consider a nuclear response?*

Dr. Peter Nanos – This is a difficult one to discuss because it depends on how much pain we are willing to accept. Particularly right now, it is a difficult conversation to have. After the first one goes off, we are probably more willing to have it. The truth is, when you are dealing with a terrorist who has a WMD device, if he decides to activate it—particularly if he is a suicide agent—wherever he is, you have to respond to the event.

DTRA's RD-CX [Counter-WMD Technologies] research enterprise is tackling the issue of, "Where do you hit a Scud launcher loaded with chemical or biological agents? How do you make the countermeasure effectively lethal with the minimum amount of collateral damage to innocent people?" Some of that can be answered with new technologies, but everything about the response has risks. Almost every act you take has to be measured in terms of gain versus consequence. Frankly, that is something we have really just started to think about in the whole issue of battle management: How do we tee up all the information to the decision-makers so that they know the consequences of action and the consequences of inaction? Perhaps the most important aspect is the timeline decision-makers are dealing with so that they do not make a decision by not making a decision.

Q: *How do you prepare for the political fallout of a WMD counterattack?*

Dr. Peter Nanos – Well, you are asking a technical geek a policy question. That is always dangerous, but I will try to answer. I think it is a tradeoff. One always has to deal with the consequences, particularly when we find in many cases that terrorists have set up shop in areas where any sort of counteraction is designed to produce as many innocent casualties as possible. You really have to have a firm grasp on what you think the adversary has, what you are going to employ, how you are going to employ it, and what the consequences are.

That is one of the reasons why our massive modeling and simulation effort is so important—and one of the reasons to have the joint cell with the intelligence community: We are starting to be able to construct fairly sophisticated simulations of what might happen given the combination of intelligence and physics models—and all of the other aspects such as social and economic effects—that will allow us to make informed decisions. Unfortunately, it is not a clean, clear-cut process; it will never be pristine. We may get lucky in some circumstances; we will most likely be faced with an ambiguous situation and will have to make a choice based on imperfect knowledge about the outcome.

COL James Hillman – Let me offer a personal observation to that. Back during Operation Desert Storm, I had a similar situation with a battalion. Command had to decide whether to destroy a suspected cache of chemical-biological weapons, and I was personally hoping that they would decide not to do that. When you put the force into the kind of protective gear that you would need to operate in that kind of environment—given that we did not have the ability to render the chemicals neutral—it creates stresses and limitations that I really did not want to have to deal with. I preferred that we find a way to destroy them without having to blow anything up.

In the example of a terrorist with WMD, if the terrorist is sitting there on a trigger and we approach him and he blows it, he wins. Unless we can bring about some change in the way we think about and respond to such situations, the terrorist wins because he is able to create an event that then gets all of the news.

Although I do not want to overstate it, the answer truly does lie in the ability to render the weapon safe in a way that mitigates—as much as can be done—the effects of the device. That is really where we need to be trying to go.

Ms. Dawn Scalici – I would just add that intelligence analysis also can pay some dividends in this regard, considering both risk management as well as the consequences of a particular type of attack. We are looking at the problem from all angles to try to find out what impact a particular response might have on terrorist enemies as well as what positions would enable them to exact retribution, perhaps outside that particular area. What would be the blowback in terms of public opinion in the area if we were to undertake those actions?

The intelligence community is increasingly called upon to provide the kind of analysis that deals with the consequences of our actions—or the potential consequences of our actions—and to look at these kinds of problems in new and different ways, for instance, using Red Cell analysis and alternative analysis. It does not always answer the questions, but it can help the decision-makers think through a problem in terms of the potential consequences of their actions.

Q: *Given al Qaeda's stated intention of carrying out a WMD or CBRN attack, why haven't they been able to do one anywhere in the world so far? Is it lack of expertise, lack of materials, or some other factor that is entering into the equation?*

Ms. Dawn Scalici – Although we do not know for sure, the consensus opinion is that acquiring the material is probably the longest pole in the tent for them. We certainly have had extensive conversations with our WMD experts about why we have not seen a WMD-type attack on our soil. Although plenty of technical information is available to terrorists—many recipes are out there on the Web, in books, and among scientists who may be willing to work with them—the information available does not always provide the kind of expertise that would be necessary to teach them how exactly to carry out that kind of an attack. For instance, what would you have to do to position the device and carry it out? The terrorists' biggest obstacle seems to be acquiring the material necessary to develop this kind of capability as well as the full knowledge of how to carry out such an attack that would have some probability of success.

Q: *The concern about technical expertise was apparent on September 11th, considering that terrorists were able to get the technical training—the flight training—to learn how to fly the passenger jets by going to school in the U.S. Is the nation now paying attention to who is getting training in other areas that could be used for terrorist ends, for example, molecular biology or chemical engineering, especially given the threats that Peter Nanos mentioned for genetically engineered diseases?*

Ms. Dawn Scalici – Many people in the audience could provide a fair amount of background on this. Certainly, we are giving a great deal more scrutiny to student visas and to people coming into the United States to study technologies that potentially could be useful for developing the kind of capability that would be necessary for WMD. Scrutiny of those who are coming into this country to study—examining the backgrounds and contacts of those people who are working at our laboratories—is much greater today than it has been in the past, particularly focusing in fields of study that may pay high dividends to the terrorists if, in fact, that knowledge should get into their hands.

Dr. Peter Nanos – One troubling issue is that, because of the free flow of information through the press and scientific publishing—for example, in the pharmaceutical industry—almost everything produced for legitimate uses can somehow be subverted. We are going to have to live with the fact that the technology will become available, and the fundamental materials are not all that difficult to obtain. The terrorists' ability to operationalize that expertise is the aspect that we are really going to have to consider carefully.

It is not just a matter of being able to close our borders to foreign students or scientists because the message of the transition to the new century is that the pre-World War II distribution of centers of excellence and science are reestablishing themselves, and many others have been added worldwide. We are going to find that a good part of the science necessary for our national health is going to be occurring overseas. Our ability to exploit it, know its sources, and tie into it is going to be very important. We are going to have to maintain a broad spectrum of people with expertise in the scientific realm who know where the knowledge originates. We are going to have to work hard countering this threat, but I do not see any easy way to insulate ourselves against it.

Dr. Dean Simmons – I want to reiterate a point I noted earlier: fissile materials are one thing when you are talking about trying to acquire the kind of material that would be needed for a WMD-type attack, but many of the materials that would be needed for biological or chemical attacks are dual-use materials for which there are many legitimate uses. We are not always going to have very clear indicators as to whether or not these materials are being used for nefarious purposes. In the majority of cases, they are going to have perfectly legitimate uses in our society. We have to look at the intersection of where the terrorists come in contact with those who can provide the kind of technology and the materials, and that is a complex problem.

Q: *This question is about resource allocation at the national level. We face at least two tiers of threat: weapons of mass destruction and weapons of mass disruption. From a national perspective, is anyone looking at how resources are allocated to these different types of threat; for instance, which has the higher probability or lower consequence? Who is making those types of decisions? Are we just engaged in capabilities-based planning where we are making certain assumptions about intent and then just attacking capability across that entire spectrum?*

Further, as to who is making these decisions at a national level, is the Office of Management and Budget (OMB) talking with DTRA or with NCTC? Is one individual or one agency coordinating all of this? Is it the National Security Council, DTRA, or the Domestic Nuclear Detection Office (DNDO)? Who is in charge?

Ms. Dawn Scalici – I will give you the NCTC perspective on this. As I noted earlier, NCTC has the lead for strategic operational planning. The broad, so-called "war plan" for the Global War on Terrorism is encompassed in the national implementation plan for GWOT. There are a number of key pillars to that effort; WMD terrorism is just one of them. What is very important is not just to have a strategy on the shelf, but also to make sure that it is appropriately resourced.

NCTC also has responsibility working with all the relevant departments of the U.S. government, as well as with OMB, to make sure that the plan is appropriately resourced. We look at what our gaps and our shortfalls are in any one of those areas and try to make sure that we are appropriately surging resources to try to fill those gaps. It is a fairly new effort. NCTC is still a fairly new organization overall. It is a broad effort to marry the strategy with the budget and to make sure that we are filling our shortfalls.

Dr. Peter Nanos – I can speak about DoD just briefly. Clearly, there are many national plans and strategies, and assignments have been made of who is responsible for various areas. One example is nuclear detection. The DNDO in the Department of Homeland Security has responsibility for establishing the global architecture for nuclear detection. It also has the responsibility to secure our borders and to conduct nuclear detection domestically. The Department of Energy (DOE) has the responsibility to develop nuclear protectors for securing stockpiles of nuclear material and other assemblies, both as part of their responsibility inside the United States and in their contributions to securing other nations' stockpiles of material.

The Department of Defense has the responsibility to play the "away game." In other words, DoD is called on to respond to hostile actions of any sort involving weapons or materials overseas, including issues of theft of WMD materials. Each one of these agencies has a specific set of responsibilities. Although DNDO establishes the overarching architecture, each agency has a particular focus area for technology, and some agencies share focus areas.

We have a detailed Memorandum of Agreement (MOA) right now between DoD, DTRA, DNDO, DOE, and the Director of National Intelligence S&T office that coordinates our programs in nuclear detection—and it is a living document. We revise it every year. We are approaching our third annual conference to align and deconflict our programs, making sure we are managing them correctly.

I believe that we will receive as much in the way of resources as we can prove to the government that we need. If we can prove that we can make progress, I think we will get as many resources as we need to make that progress. This is an area of intense concentration—one that I would say is not lavishly funded—but as we prove the value of technologies, the funding is being made available to pursue them. I feel very good about that.

Q: One of our attendees was particularly impressed with the training kit that Dawn Scalici showed and wondered whether similar materials were provided for the military or law enforcement in the U.S. Is that the case?

Ms. Dawn Scalici – I know NCTC has shared these kits pretty broadly, including with national, state, and local as well as foreign agencies. I do not have a list of everybody, but I believe the military has benefited from these kits. I know the FBI has used the kits for law-enforcement training, including overseas. As I mentioned, NCTC has translated many of the materials for use by foreign governments. NCTC helps to train our foreign liaison partners to ensure their safety because it is in our interest for them to be able to recognize the indicators of CBRN activities so that they are better positioned to try to react to CBRN threats themselves.

Q: Can you highlight some of the challenges and risks we face when it comes to gathering information about WMD threats and deciding how to share that information with our partners?

Dr. Peter Nanos – I would say the challenges in information sharing are multiple but manageable. We have come a long way in that regard, but if you get a group of counterterrorism experts in a room, the whole conversation will quickly devolve towards how we still have many areas we need to make up for and to improve upon in terms of information sharing. Another challenge is the considerable difficulty in gaining the intelligence we need.

As mentioned earlier, leaks have occurred. When we have significant leaks—here or by our foreign partners—about the means by which we track terrorist groups and gain our intelligence, it just educates the terrorists all the more, and they improve their own tradecraft. It makes it that much more difficult for us to gather the kind of intelligence we need to be able to understand what they are up to and how best to counter them.

Another challenge is the compartmented nature of many of these terrorist activities, even within the terrorist groups themselves. When we talk about WMD activities or relevant activities by al Qaeda or others, we would consider these to be highly sensitive operations—even within those groups themselves—information that they would not share broadly within their own community, much less with sources that could give us a sense of their capabilities or what they are planning. Many of the challenges we face in terms of intelligence work on terrorism are magnified many more times in the area of WMD.

Chapter 4

ROUNDTABLE 3

Enabling Partners to Combat the Enemy

4.1 MODERATOR’S SUMMARY

Tom Keaney

This is the last panel of the day, but it is the first panel in the second phase of Admiral Olson’s diagram for the Global War on Terrorism (Figure 1). The “Isolate the Threat” lines are the direct means that we talked about in the first two roundtables. Starting this afternoon and continuing tomorrow, we are going to talk about the three “Increase Friendly Freedom of Action/Reduce Enemy Freedom of Action” lines. As Admiral Olson noted, the latter lines are going to be primary over the long term. The first of these lines, enabling partners in the Global War on Terrorism, is particularly important.

Professor Thomas A. Keaney is the executive director of the Foreign Policy Institute at the Paul H. Nitze School of Advanced International Studies (SAIS), The Johns Hopkins University. He also serves as the executive director of the Merrill Center for Strategic Studies and is an expert in defense policy, arms control, military power and strategy, air power, military history, and security issues. Professor Keaney taught at the National War College, and served the military teaching at the U.S. Air Force Academy and as a B-52 squadron commander in Vietnam. Prof. Keaney is a prolific writer, and holds a Ph.D. in history from the University of Michigan.

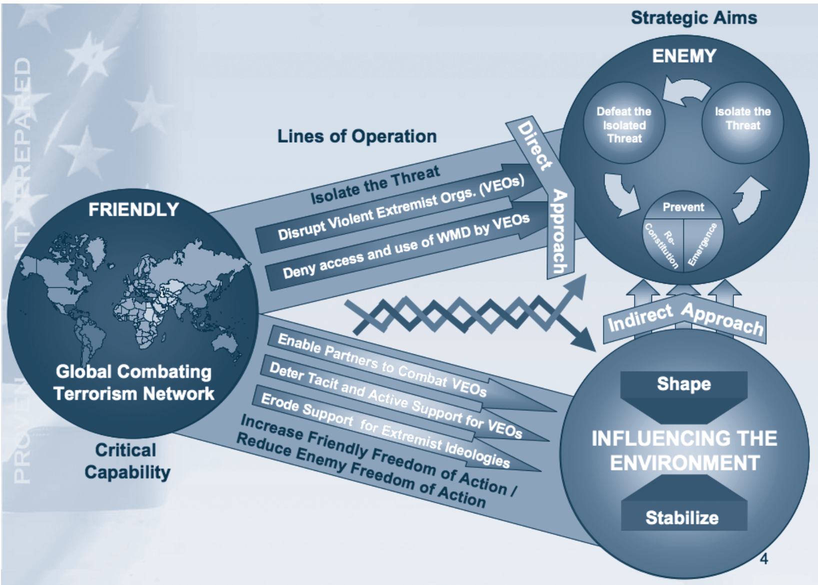

Strategic Aims
ENEMY
Defeat the Isolated Threat
Isolate the Threat
Prevent
Re-Constitution
Emergence
Lines of Operation
Direct Approach
Isolate the Threat
Disrupt Violent Extremist Orgs. (VEOs)
Deny access and use of WMD by VEOs
FRIENDLY
Global Combating Terrorism Network
Critical Capability
Enable Partners to Combat VEOs
Deter Tacit and Active Support for VEOs
Erode Support for Extremist Ideologies
Increase Friendly Freedom of Action /
Reduce Enemy Freedom of Action
Indirect Approach
Shape
INFLUENCING THE ENVIRONMENT
Stabilize
4

Figure 1 Diagram for Global War on Terror

Note also that Admiral Olson reversed the sequence in terms of priority. He is actually pointing out that the "Increase Friendly Freedom of Action" arrows represent operations that Special Operations Command is not in charge of. In other words, Special Operations Command becomes supporting here, and other people, mainly nonmilitary, are responsible for operations to enable our partners.

Admiral Olson gave us all the information we need on why enabling partners is important. He mentioned that Special Operations Command has teams in 61 different countries. Both he and Tom Mahnken emphasized the importance of these kinds of measures, not only in terms of dealing with allies, but dealing with our own interagency.

That is what this roundtable is going to talk about today. We have three superb speakers on this topic. Mr. Robert Grenier will talk about how the Global War on Terrorism is being fought and, specifically, what the roles of partners should be and how to get them to that point. For our purposes, we define partners not only as people from other countries, but also from other departments such as Departments of Defense, State, and Treasury; the U.S. Agency for International Development (USAID) within State; and any number of others. Henry Nuzum will talk about the interagency and how organizations need to work together in one very specific instance. One of his points is going to be that interagency cooperation is not enough—we need to do more than cooperate.

Our final speaker will be Brigadier Rod West, a military attaché from the Embassy of Australia, who has extensive experience dealing with both U.S. civilians and the U.S. military. He will give us a look from the other side of the fence, i.e., the view of a partner.

4.2 ENABLING PARTNERS TO COMBAT THE ENEMY

Robert Grenier

NOT YOUR FATHER'S WAR

Let me start by making a fairly broad and flat statement of fact. I say this advisedly, knowing that it is probably not going to be terribly popular in this room. The Global War on Terrorism, although a so-called war (and there are those who would disagree), is not and cannot be led by military forces. The reason was best summed up in a speech General Michael Hayden, Director of the Central Intelligence Agency, gave a number of months ago. He made this point by contrasting the war that he spent most of his lifetime preparing to fight (and fortunately never did) with the war that is being fought now.

Most of his career was spent preparing to fight a war with the Warsaw Pact in Western Europe. That enemy was very easy to find. The military knew precisely where he was: in mass formations east of the Fulda Gap between East and West Germany.

Mr. Robert Grenier is a Managing Director of Kroll, Inc., a risk consultancy firm. Previously, he served 27 years in the Central Intelligence Agency, where he developed his expertise in global intelligence, security, and foreign affairs. Mr. Grenier served in foreign assignments in CIA's Clandestine Service for 14 years as an operations officer, and was Deputy National Intelligence Officer for Near East and South Asia. As Chief of Operations, he conceived and organized CIA's Counter-Proliferation Division and was Chief of CIA's basic training facility. He has directed the CIA Counterterrorism Center and has expertise in Iraq, Pakistan, and the Global War on Terrorism. Mr. Grenier received an AB in Philosophy from Dartmouth College and did several graduate studies at the University of Virginia.

However, that enemy was going to be very hard to kill. Terrorists, on the other hand, are fairly easy to kill or to capture, but they are very hard to find. That is what makes the Global War on Terrorism inevitably an intelligence-led war.

COUNTERINSURGENCY EFFORTS

That is not to take anything away from the excellent and vital work being done by the military in Iraq and Afghanistan. The part of those very complicated struggles, particularly in Iraq, that is of primary concern to us today in the war on terrorism is fundamentally a counterinsurgency operation in Anbar province and other Sunni-dominated parts of the country.

Only U.S. Has Required Intelligence Capacity

Counterinsurgency efforts are extremely important for occupying otherwise unoccupied and uncontrolled space, denying safe haven to the enemy. Even after we have concluded our efforts in Iraq and Afghanistan, the fundamentals of the war on terrorism—the bread and butter of what we do day in and day out—will be intelligence-led, with U.S. intelligence playing a unique and a central role for quite simple and obvious reasons: nobody else has both the capacity and will to do what we do. No other intelligence community in the world is able to collect the vast amounts of intelligence that we do from all sources, to sift that intelligence, to analyze it, to winnow out what is actionable, and to provide that actionable information to both domestic and international partners. Along with that capacity comes a unique network of international relationships with intelligence and security services all around the world—relationships that have been established and nurtured in most cases for decades.

So, if we have a terrorist suspect who is traveling from country A to country B, we will share that information with our sister services in country B. We hope that they do a proper job, that they surveil that individual. We hope that they do not arrest him too soon. We hope they will wait until they have determined his network and patterns of activities, so that they do not arrest only him but arrest others who are associated with him.

Arresting and interrogating those individuals will, in turn, generate tens, dozens, maybe scores of further leads. In most cases, those leads are going to lead outside that country to other countries. Our friends in country B may or may not have relations with those other countries, and they may or may not be willing to share that information, but we are in a position where we can.

The result is dozens and dozens of simultaneous investigations all around the world, where the U.S. is the glue in that system. But for all of our capabilities, we cannot begin to duplicate what a modest security service operating on its own territory can do because they control that space. I can tell you from my experience in Pakistan, where we worked for two years clandestinely trying to do what a competent security service could do very easily on the ground, it does not work very well unless you have the active cooperation of the country.

Gaining Active Participation of Foreign Partners

That kind of situation is what makes this conflict a Global War on Terrorism. It is not because the United States is conducting this campaign by itself all around the world; it is because this effort is literally global, and we cannot begin to succeed without the active cooperation of those foreign partners. They do not do it because they like us; they do it because it is in their interest. For the most part, it is not a matter of motivating; they have every reason to cooperate.

The Dilemma of Intelligence Sharing

We need to nurture and encourage the relationships that will facilitate that cooperation. How do we maintain that tactical struggle? As we have just been saying, it is primarily through intelligence sharing, specifically, sharing actionable intelligence. Sharing of actionable intelligence is hard. Most people who do it for a living, even when they are actively cooperating, do it with a great sense of trepidation. If somebody actually takes action based on that intelligence, they may take the wrong action, or they may take it prematurely. They may take it in a way that causes the loss of the sources and methods that are responsible for the actionable information that was shared in the first place. The sharing of actionable information is a very difficult proposition.

The way that we share intelligence is enormously inefficient because we do it in the context of bilateral exchanges. To share information freely, we have to have a tremendous amount of trust in the people with whom we are sharing, and more often than not, our degree of trust is somewhat limited. So the information that we share is somewhat limited. Maybe we share it only when it is going to be too late for the recipient to use it, which may mean that they probably will not use it as effectively as otherwise. Consequently, we tend to share it in a bilateral manner: we share it with country A, which shares it with country B, which shares it with country C, and country C shares information with us.

We almost never put everything that we all know collectively on the table. There have been a few instances when we have attempted to do that, particularly with our European allies. Even then, it has succeeded only to a very limited degree because of a lack of trust. You put a bunch of spies in a room together and—surprise, surprise—they do not trust each other very much. Yet, where at all possible, we need to overcome that impediment.

Building Capacity for Our Partners

If this war on terrorism is a global effort, and we rely absolutely on the efforts of our global partners, capacity building for our partners becomes an extremely important—if not the most important—part of the overall equation.

I can tell you from my own experience, capacity building is probably the most underfed part of the overall effort. Yet, given our responsibility in acting as the glue in the system, in generating the information, in sharing the information, in trying to conduct so-called intelligence operations properly at the same time that we are doing what really amounts to international police work, we do not have anywhere near the number of qualified, experienced personnel that we need to help our allies increase their capacity.

For the most part, helping them increase their capacity means helping them to form dedicated counterterrorism units. They often do pretty well with the same units that are doing everything else, but they can do it much more effectively if they have a dedicated unit with upgraded training, upgraded intelligence systems, upgraded means of storing and analyzing information, and upgraded means of communicating both internally and also with us and other foreign partners.

Providing the required resources is very, very difficult. The task may not require a large number of people, but the people who do it have to be highly experienced. They have to be able to act as senior intelligence leaders and mentors to our foreign partners, and we do not have anywhere near the resources required to do that in the dozens of countries where we need to do it. Further, part of capacity building is also building up the military and paramilitary capabilities of our partners. There again, we have to be very, very careful about priorities and where we as a government are putting our resources. Simply because we have the opportunity to build up paramilitary capabilities in a particular country does not necessarily mean that we ought to be putting our resources there. If there is unoccupied space that we need that partner's help in occupying, then absolutely. But, frequently, we can end up confusing our allies by putting resources where we think we can rather than where we should.

STRATEGIC FIGHT DEPENDS ON OUR PARTNERS

An Islamic struggle

So much for the tactical fight. What about the strategic fight? Since 9/11, we have had quite a lot of tactical success in the Global War on Terrorism. We and our allies have captured or killed a great many terrorists, from simple fighters all the way up to major cadres. Yet, when the last National Intelligence Estimate on the counterterrorism effort was issued, the conclusion was that we are probably seeing the creation of more terrorists than we are killing or capturing. With the establishment of a renewed safe haven in the Pakistan-Afghanistan corridor and the continued threat of a terrorist safe haven in the western parts of Iraq, it is pretty clear that, strategically, we have not begun to turn a corner on this struggle yet.

So, if we are dependent on foreign partners, how do we make this happen? At the end of the day, this is not our struggle. I cannot tell you how many meetings I have attended in Washington with people who ought to have known better and think this is an American fight. It is not. We have a huge stake in the outcome of this struggle, but fundamentally, this is a struggle for the future of the Islamic world, and it is going to be decided within the Islamic world.

Provide Indirect Aid

The people who have the greatest stake in this struggle are those in the Muslim world. Make no mistake, we have huge equities tied up in this battle. But because, fundamentally, this is not our struggle and has to be fought through others, the means at our disposal are primarily indirect rather than direct. Further, consider that one of the prime unifying issues for our enemies is opposition to us, that we are seen as the enemy by many in the Muslim world who are not otherwise motivated to fight against us, still less to use terrorist means against us. Consequently, when we aid our partners, we have to do it indirectly rather than directly. We can help them at a tactical level. In fact, if we think of the struggle against Islamic extremism as a global counterinsurgency, a lot of very good counterinsurgency work is being done by our allies at a tactical level, particularly in the Middle East and elsewhere in the Muslim world. We can help them with that work if we maintain a very low profile by giving them resources and advice and helping them to share best practices among allies who do not otherwise talk with each other very effectively.

Project An Image of Supporting Justice

There is also something for us to do at a much more strategic level. There are many who tend to think that our problems and image in the Islamic world are a matter of misunderstanding. Yes, there is much we do that is misunderstood, but their problem is with their perception of U.S. policy. Rather than taking measures or actions to try to make Muslims like us who would otherwise be opposed to us, we need to focus especially on trying to reduce the degree to which our allies, in whose success we are so invested, are harmed by their continued association with us.

". . . fundamentally, this is a struggle for the future of the Islamic world, and it is going to be decided within the Islamic world."

This issue is a much longer conversation for another day, but I would argue that we need to focus primarily on projecting an image of supporting justice in the world. Whatever else you might say about the overall outlines of U.S. foreign policy, people in most parts of the world do not see our primary preoccupation as being justice. What tends to motivate Muslim populations to oppose us is their view that they are getting a raw deal in a world that is largely controlled by the United States.

They have fundamental difficulties and fundamental political issues that have been around for many decades and are not about to be solved, whether we are talking about Kashmir or Chechnya or Palestine. Those are the issues that we need to be prepared to deal with. Unless and until we do and are seen as being on the right side of history, we are not going to be able to turn a corner in this struggle.

INTERAGENCY COOPERATION

Let me just say a couple of things about what I would call the bureaucratic underpinnings of success. In my limited experience, the best model that I ever saw for how to bring about interagency cooperation was the effort during acts of hostilities in Afghanistan. We had intelligence personnel linked up with military personnel fighting alongside the Afghans. Everybody knew what everybody else was supposed to do. Everybody had a common perception of the strategic aim. CIA people were not trying to be soldiers, soldiers were not trying to be intelligence people. The soldiers called in air strikes when they needed to, and the intelligence officers maintained the relationships that we had long established with the indigenous forces. Everything worked as it should because everybody understood what everybody else was supposed to do. We did not try to duplicate one another's efforts, and we had a common understanding of the strategic goal.

". . . we need to focus primarily on projecting an image of supporting justice in the world."

That, I would argue, is what we need to maintain. In my experience, that is what we have at a tactical level. Where we do not have it is at much higher bureaucratic levels in Washington. In my experience, the bureaucratic imperative often ultimately outweighs common sense. People are trying to aggrandize themselves bureaucratically—people with sharp elbows trying to say I am in charge—when we all should understand the comparative advantages and how we need to bring the effort together.

4.3 THE STRUCTURE OF UNITY OF COMMAND

Henry Nuzum

INTERAGENCY FIELD COMMAND AND COUNTERINSURGENCY

I am going to talk about partnerships within the U.S. government, specifically interagency field command and counterinsurgency. Counterinsurgency is certainly a prominent component in our response to URW. Furthermore, as Mr. Grenier said, terrorism is the dominant tactic of the insurgencies we face in Iraq and Afghanistan.

There is little dispute that counterinsurgency demands a coherent strategy that integrates political, military, economic, and governance programs to promote the capacity of the local government, as well as an appropriate organization to guide that strategy. Unfortunately, American counterinsurgency efforts use the loose construct of unity of effort rather than the structure of unity of command, which is a fundamental principle of warfare.

Mr. Henry Nuzum works in the Office of the Under Secretary of Defense for Policy, Special Operations, and Low-Intensity Conflict (SOLIC). Previously, he was in Iraq with the International Republican Institute (IRI) as the Chief of Staff, Bagdad, and then Director of the Basra Office. He has also served on the House Armed Services Committee. Mr. Nuzum has served aboard the USS John S. McCain in Yokosuka, Japan, and in Persian Gulf deployments, leading boarding operations and Tomahawk strikes. He was a Navy Reserve Officer Training Corps (NROTC) midshipman and captain of the Varsity Crew at Harvard University who later rowed in two Olympic Games and World Championships while in the Navy. Mr. Nuzum will receive an MA at The Johns Hopkins University School for Advanced International Studies (SAIS).

I will address three topics:

- A brief discussion of counterinsurgency operations (COIN) and the COIN program of Viet Nam, where we did to some extent achieve unity of command over our counterinsurgency campaign
- The U.S. government's current framework for approaching counterinsurgency, which is combined warfare via joint warfare, and some of the problems created by the unity of effort construct
- Observations from a recent trip to provincial reconstruction teams in Iraq, which showed the real power of co-location in the absence of unity of command

Counterinsurgency Operations in Viet Nam

First, let us examine how we approached our last major interagency COIN: the effort in Viet Nam. From the early 1960s, Presidents Kennedy, Johnson, and their administrations promoted an integrated response to insurgency, but the departments fighting the war successfully resisted.

Through 1966, pacification, as it was called then, followed two parallel tracks: a military track and a civilian track. The civilian track was further divided into activities by the constituent departments and agencies. Several problems arose because of the lack of unified management:

- A proliferation of poorly coordinated programs, resulting in 60 separate pacification programs in the field in South Viet Nam as late as 1965
- A peacetime approach to funding, resources, and management, which did not have sufficient flexibility to respond to the demands of the environment
- The Army, which, although it had its own counterinsurgency programs, saw counterinsurgency as primarily the responsibility of the civilian agencies dominated resources and personnel

Civil Operations and Revolutionary Development Support

Meanwhile, the anemic civilian side had difficulty achieving its programs because of lack of security. Consequently, in 1967, President Johnson initiated the Civil Operations and Revolutionary Development Support (CORDS) program, whose mission was to pacify and bring the provinces under Saigon's control. The new organization's command structure put a civilian, Robert Comer, in charge of all personnel and programs, civilian and military, involved in counterinsurgency.

Comer served not as a coordinator or as an advisor, but as a component commander directly under General Westmoreland, with three-star equivalence. Civilian and military personnel were interspersed throughout the chain of command in the new organization. The program had three basic goals:

- Increase the resources, both manpower and money, devoted to counterinsurgency.
- Bring to the civilian agencies the benefit of the vast resources, both personnel and physical, of the military.
- Impart an appropriately civilian flavor to the counterinsurgency effort, even though the civilians were ultimately under military command, and, at the very top, Comer reported to Westmoreland.

Comer ran the counterinsurgency show. Below Comer were four regional CORDS directors, and below them at the operational level were 44 provincial teams, who, in turn, supervised 250 district teams. Throughout the command structure, all military and civilian members, no matter their parent agency, reported up this chain of command.

The new organization dramatically increased the performance of pacification and resources. From 1966 to 1970, the number of personnel devoted to pacification increased sevenfold, and the budget tripled. Participants praised the new program, specifically, the real power of the provincial senior advisor, who was a Provincial Reconstruction Team (PRT) leader or a senior foreign service officer. This single leader was able to direct all pacification programs within the province and ensure that they were coordinated in an integrated fashion. Previously, some of these programs had undermined one other. This authority included writing performance evaluations.

I interviewed a deputy provincial senior advisor, an XO of one of these province teams, who worked for the U.S. Agency for International Development (USAID). He told me that he would grab an M1 and spot check the district teams, which were all five-man military teams, on their night patrols. I asked if he had any military experience. He said, "No, but I was better at bushwhacking than soldiers because I was a Boy Scout."

There were some problems with the program, specifically reporting requirements and integration at the operational and tactical levels; at the national level, we were still fighting two wars. The vast majority of the military command reported directly via General Abrams to Comer and was not integrated. Also, the civilian agencies maintained many of their national programs—USAID, CIA—and were not integrated through the CORDS program.

Current Framework for Counterinsurgency

There are obvious differences between the conflict today and Viet Nam: the nature of the role; the conventional aspect of the war in Viet Nam, as represented by the North Vietnamese Army (NVA), a very competent conventional force; and the great power sponsorship enjoyed by the communists in Viet Nam.

However, I believe that these differences—chiefly the absence of the conventional component in the current conflict—make the lessons of CORDS especially applicable today. Because insurgency is the only war in Afghanistan and Iraq, it is all the more imperative that we approach it with a unified management. However, the United States seems to have forgotten the interagency command lessons of Viet Nam. Today, the government seems to have unconsciously conceded that it cannot bring unity of command to its departments and, instead, is settling for a proxy unity of effort.

In all the discourse explaining our difficulties in Iraq and Afghanistan, the lack of unity of command is seldom cited, and we fail to apply this fundamental concept of war—unified authority—to insurgency. That failure is especially surprising because of the nature of insurgency. All war is political, but insurgency is political at the micro level and at the level of the checkpoint, the home, and the street.

Security activities have an immediate political effect and vice versa. Conventional military doctrine holds that unity of command is a prerequisite for unity of effort. Joint Publication (JP) 1, "Doctrine for the Armed Forces of the United States," the capstone document of U.S. military doctrine, states, "Unity of command must be maintained through an unambiguous chain of command, well-defined command relationships, and a clear delineation of responsibilities and authorities."

Furthermore, the purpose of unity of command is to ensure unity of effort under one responsible commander for every objective. But the guidelines for multiagency operations replace directive language with accommodating language. In JP3-08, "Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations, Volume 1," the language relies on coordination, harmonization, and cooperation, and the prerequisite of unity of command has disappeared. Unity of effort, an end in JP1, becomes a means in JP3-08. If you combine the two citations shown in Figure 1, you approach totality: "Coordination and cooperation toward common objectives ensures that all means are directed towards a common purpose."

JP 1: "Unity of command must be maintained through an unambiguous chain of command, well-defined command relationships, and a clear delineation of responsibilities and authorities."

JP 3: "The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective."

Figure 1 Unity of Effort Alternatives

Let us contrast the language between joint conventional doctrine and interagency doctrine. Figure 2 shows a chart comparing the frequency of terms in the JP1 conventional doctrine and the interagency doctrine. Both documents are similar in length. “Unity of command” is used 23 times in the conventional doctrine and only twice in JP3-08 and then only tangentially. “ Authority” appears 350 times in JP1, 73 times in JP3-08. “Responsibility” occurs 250 times in JP1, fewer than 100 times in JP3-08. “Accountable” appears 9 times in JP1, zero times in JP3-08. “Consensus” appears 12 times in JP3-08; JP1 was never concerned about consensus. There are twice as many instances of “coordinate,” “coordination,” etc., in the interagency doctrine as the conventional one.

	JP 1	JP 3-08
Total Pages	**155**	**103**
Unity of Command	23	2
Authority	350	73
Responsibility, etc.	250	<100
Accountable, etc.	9	0
Consensus	0	12
Coordinate, etc.	268	378

Figure 2 Doctrine Diction

If we look beyond the text, it could be said that this contrast in language is appropriate because JP3-08 applies to international actors, which brings up a larger issue. Policymakers seem to follow a combined versus a joint model for counterinsurgency, even though all the players play for the same team. Consider the ponderous title of JP3-08. Clearly, to the military, other departments are as foreign as international actors.

It is not just the services; DoD as a whole subscribes to this same model. DoD 3000.05, which directs the Department to give stability operations the same primacy as conventional combat operations, repeats the phrase “U.S. departments and agencies, foreign governments and security forces, international organizations, NGOs, and members of the private sector" 11 times in an 11-page document.

The defense community is combining interagency partnership with international partnership. Interagency partnership is relegated to the foreign realm. The defense community is not alone in embracing this model. There is no vocal objection from the civilian agencies to being relegated in this way.

Directive NSPD44, signed by the President, guides stabilization and reconstruction efforts and repeats the soft language of JP3-08. Absent again is directive language. "Coordinate" and "cognate" appear 24 times, and "authority" appears 3 times but only in a final paragraph with caveats. "Responsible" and "responsibility" occur 4 times, "accountability" once. Cooperation and coordination are now appropriate routes to combine warfare. When the U.S. negotiates with allies, over whom it has no authority, using these same tools of loose collaboration to unify multiagency efforts, it demonstrates that policymakers have lost hope for the tight command structure that guided our efforts in CORDS.

Provincial Reconstruction Teams in Iraq

The unity of effort framework has three potential problems:

- Remote management
- No system of dispute resolution
- Effects of insurgency bleed into all spheres

First, I will look at these obstacles generally with respect to Iraq and then go into more detail on the performance of PRTs in Iraq. For some background, provincial reconstruction teams are multiagency teams designed to enhance the capacity of Iraq's provincial and municipal governments. PRTs and brigade combat teams, aka brigades or BCTs, are responsible, respectively, for the political and economic aspects of the counterinsurgency and the security aspects. They frequently work in concert.

The first problem is remote management. There is no onsite oversight of the brigade commander and the PRT team leader.

The result is an inefficient parallel system of recourse that deters appeal on any local disagreements. If you ask a PRT leader or brigade commander how this command structure works, the answer is invariably, it depends on the personality.

The second problem with the unity of effort arrangement is that with no system of dispute resolution, some issues are not even vetted. Leaders question whether it is worth the time, effort, capital, or the conflict with the people involved. They tend to retreat into their respective civilian and security spheres of responsibility, impeding integration.

The final and most serious obstacle created by this former multiagency management structure is a separation between authority and responsibility for effects. In the unity of effort construct, the brigade commanders and the PRT team leaders each have their own arenas, with the PRT responsible for political and economic operations and the BCT commander responsible for security. But insurgency does not respect our government's artificial departmental borders. The brigade's actions in security and the PRT's actions in the political and economic arenas impact each other because of the intimate nature of insurgency. Effects, but not responsibility, bleed over into all the spheres. If a manager is not responsible for an area—even if he has supporting responsibility—he is not going to dedicate as many resources to that issue. This link between responsibility and resources was one of the primary motivations for Comer's consolidation of command.

PRT Performance in Iraq

I will wrap up with an analysis of how PRTs in Iraq have performed. First we will consider some fundamentals. Among other improvements on Afghanistan's PRTs, Iraq's PRTs have a single leader rather than the three-leader construct of an aide, a State, and a military staffer, as was done in Afghanistan.

The single leader has a fair degree of authority over team members and civilian programs, but the PRT and the military chains of command are still bifurcated, which fuels the problems of remote management, personality, and segregation of authority from responsibility.

There are some issues with the first two, but the most common problems involve the separation of authority from responsibility. I will cite two examples. The first is with resources, particularly transportation. The brigade and the PRT are theoretical equals. However, because of the brigade's preponderance, the PRT must request assets, which puts them in a subordinate position. One of Comer's prime goals in uniting the chain of command was to give the civilians ownership of vast resources.

In 1968, a CORDS representative said that one of the great outcomes of CORDS was the ability to demand military resources and expect them to be made available. The brigade rarely says no to these requests, but the simple act of making the request by the PRT sets up a dynamic of suppliant and benefactor. Hence, many requests go unmade.

There are two types of PRTs in Iraq: paired PRTs, which have province-wide responsibility, and embedded PRTs with a smaller area of responsibility, usually at the municipal level or slightly larger. Especially for the province-wide PRTs (paired PRTs), transport is a real currency, even more so than funding, especially now that the Baghdad government is disbursing some funds to the provinces. Most of the PRTs rely on the host brigades for daily movement. They are generally able to go from the forward operating base (FOB) to the provincial capital, and they are usually co-located. If there is a government center in the provincial capital, the FOB will be just on the outskirts of the capital. The result is that they are rarely able to leave the provincial capital to monitor projects or assess government performance in the districts, which degrades their province-wide responsibility mission.

As an example of a typical dynamic, I would be told by a brigade staffer that the PRT has enough movement assets, and I would be told by the PRT leader that the PRT has enough movement assets. Then, I would go one level lower to the economic, governance, infrastructure, agriculture leads of the PRT, and they would say. "No, we can't get out of the capital, we can't get out into the districts."

There is an interesting story related to this situation. When I talked to the brigade staff, I was dealing mainly in Multinational Division (MND)-North. They reported that the MND-North commander had said that transporting the PRT team members took priority over combat ops. A few minutes later, I asked a brigade staffer how many movement teams the brigade had dedicated to PRT, and he said one platoon. Then, I asked how many movement teams the brigade had. The answer was about 60. When I asked if the brigade could provide more teams if the PRT requested them, the staffer said that they could do it as soon as they got more troops. This was at the height of the surge, and no more troops were likely. I said, "What about right now? " He answered, "We can't do it without taking away from our responsibilities, combat ops." So, despite the guidance (this was the same staffer who had told me that PRT movement should take priority over combat operations), the brigade is still responsible for combat operations, and the PRT is responsible for political and economic operations.

The brigade had only supporting responsibility there. So, the PRT ended up augmenting movement with its own civil affairs personnel, who could be doing PRT-specific work. Joint Multinational Forces, Iraq (MNFI) and Embassy guidance directs the military to support three concurrent PRT moves, but in reality they usually get one, or possibly two, moves simultaneously.

A second aspect of the separation of authority and responsibility is the different conceptions of mission duration. The PRT focuses on building the capacity of the local government and is wary of dependency, so it prefers not to execute programs but, rather, train and assist Iraqi officials in planning and monitoring. The BCT wants to quickly improve the security of its area of responsibility (AOR) in a finite tour of 12 or 15 months, and it may often lead an initiative if local officials seem incapable. The BCT will claim the project merits spending money from a humanitarian and infrastructure fund because the project will immediately lower violence, which is generally true. But it will also inhibit the development of provincial government capacity, which is the responsibility of the PRT.

Lowering violence and increasing the capacity of the government are certainly laudable. The problem is that they act against each other, and there is no single responsible arbiter onsite in the provinces who can balance these competing interests and make a decision. Furthermore, it is very difficult in Iraq, even today with the improving security situation, to maintain that anything is independent of security. Therefore, the military can be involved in areas that might ostensibly fall within the PRT sphere.

I did find these expected obstacles, but I also found something encouraging—that co-location was even more powerful than I had previously believed. Even if there is no formal organizational link, it is very difficult to completely ignore the concerns of a compatriot in a wartime environment if you see that person daily. It is a lot easier to do it over e-mail, however. I do not want to exaggerate the tension between the civilian and the military sides. Generally, the BCT listens to the advice of the PRTs regarding political and economic matters. This cooperation is also helped because of the frequent contact between the PRT and the BCT, which are usually on the same FOB.

However, being on the same base is not the same as co-location. These bases are big—four, eight, nine square miles—and the PRT and the brigade headquarters are often on opposite sides of the base. If the personalities do not match, the BCT commander and the PRT leader might not see each other for a week or two. When the personalities mesh, the PRT/BCT team works fairly smoothly, and I do not think that unified authority would add a lot to it. However, the clarity of responsibility affected by a CORDS-like structure would certainly help when the PRT and BCT leaders have different conceptions of how to wage a war.

4.4 COALITION PARTNERSHIP PRINCIPLES

Rod West

I have a good deal of experience working with coalitions. I have worked in five different coalition operations around the world, twice in command of Americans. I have worked in different sorts of situations and with different sorts of military posture in East Timor, in Kuwait, in Iraq, in Bogenville, and Cambodia, and also in a number of defense cooperation and engagement activities. What runs through all of those particular operations is that each is unique and requires a different, often first-principles, approach. While a good doctrine, TTPs [tactics, techniques, and procedures], communications plans, and so forth are very handy, they cannot be relied upon to provide a templated solution for future conflict resolution, particularly in the present complex and persistent conflict.

Brigadier Roderick J.S. West commanded the Joint Headquarters Transition Team in Iraq, a multinational team of senior military officers, civilians, contractors and Iraqi personnel providing mentorship and policy guidance to improve the institutional capacity of the Iraqi government and security forces. His distinguished military career spans more than 20 years in the Australian Army and the Corps of the Royal Australian Engineers in various command, instructional, and staff roles. Brigadier West holds a Master of Management degree from the University of Queensland, a Master of Science (National Security Strategy) from the United States National Defense University, and a Master of Defence Studies degree from the University of Canberra. His reconstruction support to the Itape tsunami in Papua, New Guinea, won him the Conspicuous Service Cross.

LEGITIMACY AND HOPE

I do not propose to dazzle you with answers today about how to empower your partners. I come to you from the point of view of a coalition partner, a planner, and a commander from my own army. I approach my own planning from the point of view of two important principles:

- No one starts a war without first being clear of mind about what he intends to achieve by that war and how he intends to conduct it.
- The purpose of war is to secure a better peace.

The former quote, attributed to Carl von Clausewitz [1], relates to legitimacy, and the second quote, from Sir Basil Liddell-Hart [2], relates to hope. Legitimacy and hope are the two elements that will bring coalition partners into play. Without those two important factors, it is unlikely you will get a coalition partner of any endurance to stump up for the operation. The von Clausewitz approach is very direct, while the Liddell-Hart approach is more indirect. It extends from his experience in World War I.

Trenchcoat Analogy

As I reflect on recent operations, we could wonder if we have asked the right question here. If we have not, then it is going to be hard to achieve legitimacy or hope from the operation. Coalition operations is a very difficult area to work in. I have often heard Professor Bob Sharpe at the National Defense University describe coalition operations as rather like an Englishman wearing a three-button trenchcoat. The top button is usually done up high and tight and always looks very smart. He likens this to unity of intent. That is, all the nations that sign up to the adventure generally speak with a similar voice and are on message.

The second button he refers to as unity of effort, and this button can be a little untidy. It could be done up, or it may be undone, but it is quite nonspecific and may not generally support the whole unity of intent. And rarely does the action or the effort match the rhetoric.

The final button, the third button, is generally very untidy, allowing the coattails to blow around in the wind. This button he refers to as unity of effect. Very rarely do we get the specified effects in the operation right at the start as we talk about unity of intent. For example, we estimated that we would need about $40 billion to solve the problem of Iraq. So far, we have got commitments of about 10% of that sort of figure.

Realism About Military Might

The trenchcoat is an interesting analogy because it tells me, as a military planner, that almost always I am not going to get all of the resources that I need to achieve the specified end. This realization would generally cause military planners to be cautious, to underpromise and attempt to overdeliver. I think the trick here from a planner's point of view is to be realistic about what can be achieved by the military instrument.

In the context of the overall government approach or coalition approach, one has to be realistic about what the military can bring to the overall mechanism to get you to where you need to go. This issue is important as the U.S. moves to its new doctrine under FM3-0 [3] and starts to look at stability operations along with the other phases of war: offense, defense, and support operations.

In my view, the new plan does not go far enough to address this issue. I want to a look at some of the issues of operational weaknesses, as I identify them. These are trends that I have noticed in operations, not necessarily any sort of doctrinal approach or an Australian government approach.

OPERATIONAL WEAKNESSES

Institutional Capacity

The first issue is that of institutional capacity, which is the ability of a host nation or a country's military or security services to manage their organization. It includes institutions and processes, such as strategic planning, budgeting and financial control, force management, equipment and capability acquisition, an institutional training base, logistics and sustainment, modernization, and military law. Most nations are strong in some of these issues, but no nation is strong in all of them, including the U.S. military. Each of those functions must be audited to identify the critical vulnerabilities where investment is needed to bring the country's capability up to a level that will empower them to take on this global war.

Combat Effectiveness

The next issue is the combat effectiveness of each of those nations. There is great variation from nation to nation. But the important point is to look at how a military can actually apply its combat power, how it is informed for the commitment of that combat power, how it is controlled, how it is equipped, and how it is trusted or viewed by the international community and its own people. The results of this assessment will be very different for each partner.

Information Sharing

The ability to conduct intelligence-led operations is fundamental to this sort of global warfare. The key to ISR [intelligence, surveillance, and reconnaissance] is information. In the coalition environment, information gathering, processing, and sharing should be a continuous loop that we all undertake on an international level. The difficulty is that the U.S. is traditionally very reluctant to share information and is understandably very protective of that information. The question is: Can the U.S. find ways to share actionable intelligence with its allies or partners in ways that will not compromise its own security or competitive edge?

This area is very difficult. No nation has a better intelligence or security relationship with the United States than Australia. In 2006, the President signed a directive to allow Australia and the U.K. to share Classified Information Procedures Act (CIPA) access. Sharing has occurred in some instances, but it certainly has not occurred in accordance with the intent of the President.

Further down the command chain at the level of a foreign disclosure officer, the grassroots level is bound by rules and regulations that cannot be sidestepped, even with a Presidential citation. If information sharing is very difficult for us, it is certainly going to be very difficult for nontraditional partners or for partners who do not have the same sort of security relationships built up over many years that we do. It is going to be tough, but it is an area that needs investment and analysis.

"Can the U.S. find ways to share actionable intelligence with its allies or partners in ways that will not compromise its own security or competitive edge?"

Values and Ethics

The next issue is values and ethics, which is as much about cultural friction as it is about ideology. The question here is: can the U.S. cooperate with societies that do not share its values of freedom, democracy, and the pursuit of happiness in the same way? We live in an area where we have to get along with our neighbors. Even if we do not share the same values as some of those neighbors, we know that we must cooperate, operate, and share information with them if we are all going to be secure within our own region. Again, it is a very difficult area, and a lot of people will say you cannot do this or that, or there are regulations to prevent you from doing what you want to do or going where you want to go. Somehow, they have to be circumvented.

Reliability

The final issue on the operational side of the house is reliability. How reliable are those that you are working with—the leadership, the commanders, the whole of government leadership? Can they be trusted? Are they working in the best interests of their own nations, their own people, the coalition? We have been trying to assess the reliability of the leadership in Iraq and Afghanistan and other places, and it is very tricky assigning any sort of metrics to it. Somehow, we have got to come to grips with those that we can trust and those that we cannot.

TECHNICAL GAPS

Modernization

Coming down to the technical level, there are a number of gaps that need work. Many of our allies who are crucial to this persistent conflict have been very slow to adapt their own doctrines and their own systems to this new environment. Counters to unrestricted warfare cannot be conducted with old industrial age or Cold War-era TTPs, equipment, and information systems. Many of the nations whose support we need do not understand that there is a Global War on Terrorism. They are very loath to invest, to modernize their systems, to modernize their intelligence gathering, or to modernize their linkages to Western partners because they are just not motivated to do so.

> *"Can the U.S. cooperate with societies that do not share its values of freedom, democracy, and the pursuit of happiness in the same way?"*

We have to attack that particular issue. The crucial issue comes back to information and information sharing, particularly in the form of actionable intelligence. Many of our allies rely solely on human intelligence. Although human intelligence is very important, it is rarely extensive enough and very rarely timely enough to provide the precision effects required by counterterrorist operations.

Counterinsurgency or Counterterrorism?

I also have one problem with what I have heard today: the intermixing of counterinsurgency and counterterrorism. They are two completely separate issues, and the tools that work for one will not necessarily work for the other. We need to be very precise in the use of these terms. If we get confused, we are likely to apply the wrong tool to the wrong problem.

Common Operating Picture

If we really want our forces to interoperate at the technical level in the field alongside each other on a dark and dangerous night, we have to build a common operating picture of what we are doing, what the enemy's doing, and what the noncombatants are doing. As Sir Rupert Smith said, "This is a war among the people." [4] We have got to acquire that picture, develop it ourselves, and then disseminate it so that everyone involved is seeing the same thing. We have been after this holy grail for decades. Having just finished in Iraq in September, I can tell you that we are still a long, long way from that common operating picture.

Tactical Mobility

The next technical gap that I see is tactical mobility. Many nations still have foot-mounted militaries. They have not learned the lessons of protected mobility and the ramifications of coming up against a smart enemy who uses improvised explosive devices (IEDs), land mines, and other such devices.

It has taken us 5 years to get into a position where we can ensure mobility by upgrading the protection on our land-based mobility systems. A lot of nations are going to need help with that.

Force Protection Standards

The next issue relates to force protection standards. Many nations have much lower force protection standards than we do. We have to reach agreement on a common standard if we are going to be operating together. Counter-IED and electronic warfare standards must be included as well. Interoperability in basic communications and radios and the ability to speak together on a tactical radio network is still something that eludes us. The difficult questions are what degree of interoperability is actually required, and who is going to fund it? It may be that the U.S., as the last great superpower, has to come up with the coalition junction box that all nations can plug into for commonality of communications or a common operating picture.

CONCLUSIONS

Kinetic action cannot solve the underlying issues and often works to gain new recruits for our enemies. We have known that for a long time, but we are still doing it.

Military action can buy time and can certainly help reduce passions. But by itself, it is highly unlikely to be decisive in this war. Militaries must be adaptable. From what I have seen of the new FM3-0, there is a real attempt to make the U.S. Army, in particular, far more adaptable than it has been in the past.

Right now, the Australian army is conducting operations across the spectrum of conflict and in three of the four global hemispheres. After about a decade of these operations, we are now in a position where we can implement our own doctrine of adaptive campaign. We can do it because we are small and agile.

The lesson is that all militaries have to do that. We have soldiers in Iraq who are currently conducting full-spectrum operations. In Timor, we are conducting peace support operations with a highly visible military presence. In Afghanistan, we are conducting provincial reconstruction tasks, supported by the Dutch and by local security operations. In the Solomon Islands, we are supporting the regional assistance mission through presence without posture—that is, we have a combat team of soldiers there but without visible weapons.

Our soldiers need to be able to rotate through that spectrum, as do yours. That takes a certain agility of mind, not to mention equipment, techniques, and procedures.

I will leave you with a thought that persistent conflict among the people knows no boundaries and cannot be defeated by a single nation alone, no matter how omnipotent seeming. The solution to unrestricted warfare will require an unprecedented international cooperation, an unprecedented exchange of information, and perhaps the subordination of some traditional national interests to empower friends, allies, and even nontraditional partners to counter this global phenomenon.

REFERENCES

1. Carl von Clausewitz, *Vom Kriege (On War)*, 1832; Penguin Classics: London, 1982.
2. Sir Basil Liddell-Hart, *Strategy*; Faber & Faber Ltd.: London, 1954.
3. “Operations,” Army Field Manual FM3-0, Department of the Army, 14 June 2001.
4. Rupert Smith, *The Utility of Force: The Art of Warfare in the Modern World;* London, Allen Lane: 2005.

“The solution to unrestricted warfare will require an unprecedented international cooperation, an unprecedented exchange of information, and perhaps the subordination of some traditional national interests to empower friends, allies, and even nontraditional partners to counter this global phenomenon.”

4.5 QUESTIONS AND ANSWERS HIGHLIGHTS

Transcripts

Q: *General West, would you expand a little on your comment that counterinsurgency and counterterrorism are very different given our context today?*

BRIG Rod West – I will answer the easy part first. Counterterrorism is a kinetic effect. Terrorists sit under the banner of what I have heard General Patraeus describe as the irreconcilables. Generally, the only answer to that kind of adversary is a kinetic effect, that is, destroy them or disrupt them or kill them.

In contrast, when you talk about counterinsurgency operations, you are talking about an operation that is focused on the minds of the people in that particular area. The focus moves away from the enemy to the people. The more you come back to focus on the enemy, the more you isolate the people, and the effect is quite the reverse of what you want. Henry [Nuzum] mentioned some very good examples of the lessons learned from Viet Nam. You have to start directing your operations, possibly not led by the military instrument. Those are the two important distinctions.

Q: *Could you comment on the intel aspects for each, if they are different?*

Mr. Robert Grenier – I am not sure that there are different intelligence aspects. I would just add my voice to Rod West's that counterterrorism, as narrowly defined, and counterinsurgency are very different. Perhaps the best example that makes the distinction clear is the situation in the tribal territories in Pakistan. We are pushing our Pakistani allies to take effective action against terrorist targets under circumstances where doing so further inflames the local population against them and, by inference, against us. At the same time, we want to conduct a counterinsurgency campaign there to deny safe haven to the very terrorists that we are trying to kill or capture. In other words, we are trying to do two things simultaneously that work directly against each other.

Q: *How difficult is it to get our allies to cooperate with us?*

Prof. Thomas Keaney – Quite frankly, when I was still in government, I was amazed every day that people cooperated with us as much and as effectively as they did. In their place, I am not sure that I would have acted quite as vigorously.

Q: *An associated question for Rod West. Has there been some reluctance either by the Australians or anyone else to being seen as an ally to the U.S because of how U.S. actions are viewed abroad?*

BRIG Rod West – Specifically from Australia's point of view, the answer is no. We are our own nation, and we make our own judgments and decisions. Australians would not be swayed by *The Washington Post* because very few read it. They would be persuaded by what they read in the *Camber Times*, and that is something different.

The issue for other nations is that they see a difference between what the Administration is saying and what people are reading or seeing on CNN. People have a level of tolerance to that kind of disconnect, but each time it happens and each time people observe it, another small layer of trust is lost until there is no going back.

Q: *Mr. Nuzum referenced the CORDS program in his Viet Nam example. From your experience or from your research, can you tell why there has been reluctance to look at the lessons from Viet Nam and apply them?*

Mr. Henry Nuzum – I am a true believer in this unity of command concept. It took half a decade to apply it in Viet Nam, so it required continued and persistent executive attention for an appreciable period. President Johnson picked up on President Kennedy's attention to the subject in November of 1963 when he took over. Still, CORDS was not implemented until May of 1967, almost four years later.

Part of the immediate reason is that we assume these wars will be very quick. The quiet period of 2001 to 2003 or 2004 in Afghanistan only confirmed that optimism. We also assumed that Iraq was going to be quick, so why reorder the mechanics of government when you are going to be in and out in a hurry? CORDS is being applied now in Iraq. There is a country team concept there, but the level of the authority of the Ambassador on the country team is fairly variable. The bureaucracies are being taken out of their peacetime construct, reporting up their own chains to Baghdad and from Baghdad back to DC, which unifies power at a national level in Baghdad, a provincial level, and eventually a district level.

The broader reasons have to do with different bureaucratic cultures. USAID State, and the military are the three main players, and all approach these things differently. Societal conceptions of war play a part, too. American society still thinks of World War II as the paradigm of war, whereas it was probably more anomalous than anything else. The narrative of World War II is that military commanders had freedom of action. I think the memory of that is exaggerated. We were striving for unconditional surrender, so commanders probably had more latitude. Again, the memory is of a grand conventional conflict—we do not remember the messier, insurgency aspects. It is difficult to escape that conventional paradigm. As a society, we are uncomfortable with both insurgency and the reforms that are necessary to properly address it.

Finally, I do not believe those lessons have received the attention from the Executive Branch or the Congress that they might have gotten during Viet Nam, which ties into the societal conceptions.

Q: *Bob Grenier mentioned the need for intelligence sharing, but specifically at the tactical level, and Henry [Nuzum] talked about the need for unity of command. Would that apply to intel people at the tactical level, or is there a special province for that? How successful will intel sharing between countries be at the tactical level?*

Mr. Robert Grenier – Intel sharing does apply, particularly in a war zone where we have intelligence personnel, intelligence assets, and capabilities deployed in the same theater with military assets and military capabilities. Those of us who leave government live in deathly fear that our experience will become irrelevant. This discussion has been enormously reassuring to me because I can see that we are still having the same discussions now that we were having a year and a half ago when I was still in government. It does not appear as though we have made any forward progress whatsoever. I think people could easily read my comments as an impassioned argument for unity of effort, when Henry is arguing passionately in favor of unity of command. The issue for me is not so much who is in charge, or who is deciding if there is going to be unity of command and who the commander is going to be, as it is my concern that the question itself is irrelevant. It is irrelevant to the extent that in many cases, an argument over unity of command and who should be in charge is actually masking a more fundamental question that has not been resolved.

From Henry's recounting of his direct experiences with the PRTs in Iraq, what jumps out is that the job of the BCTs is not just to work together with the PRTs—they actually have wider responsibilities that require somebody at a more senior level to decide the priority at any given point in time. It seems as though somebody has not made a fundamental decision somewhere along the way because I agree absolutely that co-location is critical. If you have a co-located PRT and BCT who have one clear job, a common conception of the effort, and an understanding of what each brings to the table, then it almost does not matter who is in charge because the civilian is not going to understand the business of his military colleagues and vice versa. This question of who decides if we go out in support of the PRT or go out on a combat patrol would be solved if the civilian head of the PRT were in charge. The more fundamental problem is that the PRT is perhaps being given too much to do. Somebody has not made a decision as to the real center of gravity of our effort in a given province.

Q: *Rod, do you have any comments on that?*

BRIG Rod West – Turf battles like that often come down to who is providing the resources, where they come from, and if there are enough. As soon as resources become tight, people try to protect their own patches. I do not know the funding arrangements for the PRT, but I did observe them pretty closely in Iraq, and I feel that PRTs have the potential to be very powerful. They are being constricted in the ways that Henry described, although my own impression was that it was not quite as bad as Henry was describing. Can it be fixed by unity of command? I do not know about the American context. In the Australian context, our civilians will not adhere to the term command at all. They do not understand it, do not believe it, and do not believe anyone outside of a uniform can be commanded.

So, we would relate to unity of effort in Australia. If you have unity of effort and unity of resources, so that there is a single dog that can wag its tail and have the resources sent in the right direction, you are halfway there.

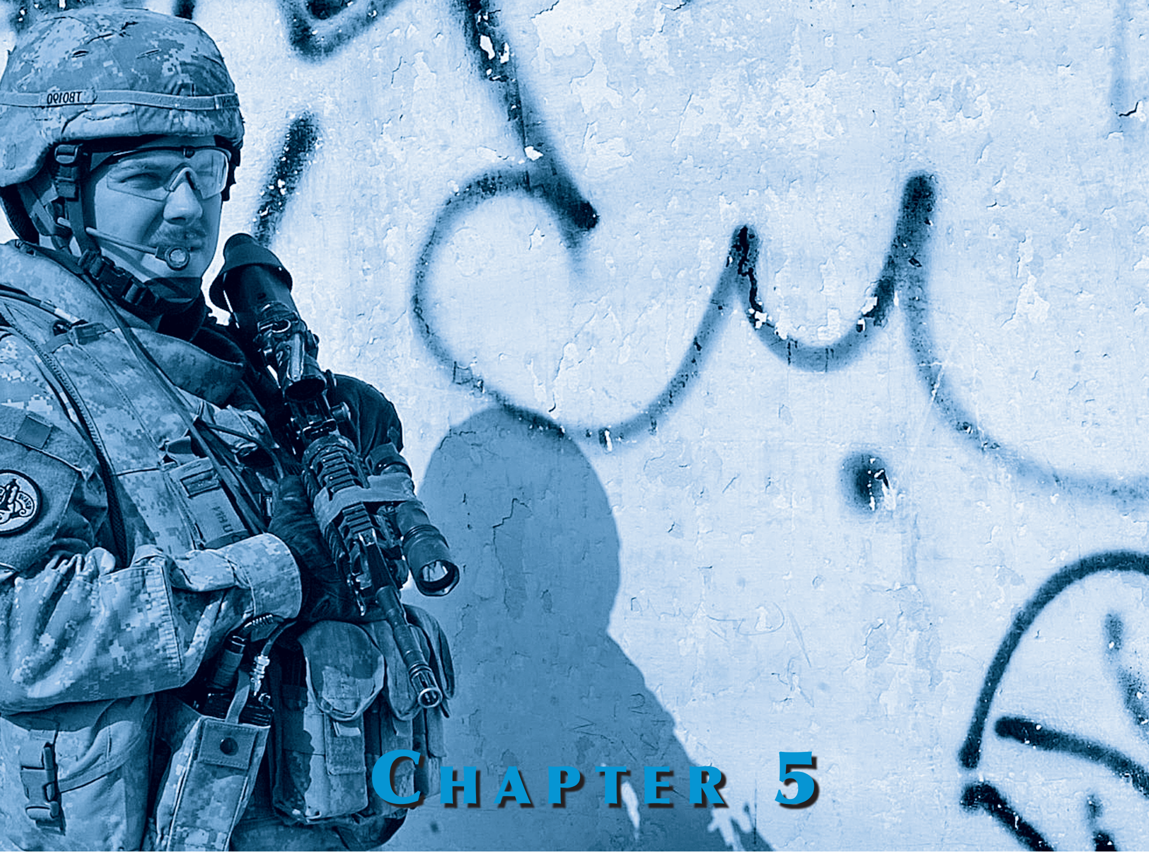
Q: *Our final question has to do with barriers in information sharing, particularly information sharing at the secret level. The question is: Are these barriers mainly political as opposed to ways of protecting sources? If so, how can we get beyond the political barriers?*

Mr. Robert Grenier – I am not sure exactly what you mean by a political barrier as opposed to a substantive barrier or sources and methods.

Prof. Thomas Keaney – I think political here refers to sharing with a country that we are not sure of or the interaction between the countries, as opposed to the information.

Mr. Robert Grenier – Let me just cite two factors, and there may be others as well. One has to do with trust. For me to feel free to share information at whatever level, I have to trust that it is going to be used responsibly. But there is another factor here that is much more pernicious. Again, speaking for people who come from my background, we tend to keep secrets because that is what we do. Keeping secrets becomes reflexive—for what may be very good reasons. By and large, most times, most places, most situations, it is best to protect information. But in drilling that into people's heads, many of us lose the underlying understanding of why we are keeping the secrets.

You need to have that understanding in the frontal cortex of your brain to make proper tactical decisions as to what to share and what not to share. If we are talking about making a whole level of information, which we have arbitrarily called secret, available to all our colleagues within government and to all of our allies by giving them common access to a broad communication information system, that is going to make people in the intelligence world very, very uncomfortable. They do not know how the information is being used; they do not know how it is being protected. Therefore, rather than dealing with those issues, they will tend to keep information out of it.



Chapter 5

ROUNDTABLE 4

Deterring Tacit and Active Support

5.1 MODERATOR'S SUMMARY

Thomas McNamara

How can we deter or dissuade terrorists and terrorist organizations from committing hostile actions against our country, particularly from the use of WMD?

I will start with a review of the deterrence policy that the Office of the Secretary of Defense (OSD) and DoD were forming at that time for the Global War on Terrorism (GWOT). Figure 1 provides an overview of the GWOT campaign concept. The fourth line of operation in the influence environment concentrates on deterring tacit and active support for terrorism.

The United States has traditionally confronted the challenge of deterrence at the national policy or strategic level, focusing on the former Soviet Union during the Cold War era. The United States and the Soviet Union achieved deterrence chiefly by balancing nuclear threats between the two nations. Deterrence became synonymous with the words nuclear and strategic. Today,

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 challenges and strategic balance and integration of joint defense capabilities. Previously, he advised the United States Strategic Command and the David Taylor Naval Ship R&D Center. He has published and presented his expertise in undersea warfare, autonomous unmanned vehicles and systems, advanced R&D, DoD acquisition, systems engineering, and command and control. Mr. McNamara earned a M.S. in Technical Management from The Johns Hopkins University and a B.S. in Ocean Engineering from Florida Atlantic University. He has received several Navy acquisition awards.

some communities within DoD still speak primarily of strategic deterrence as being nuclear.

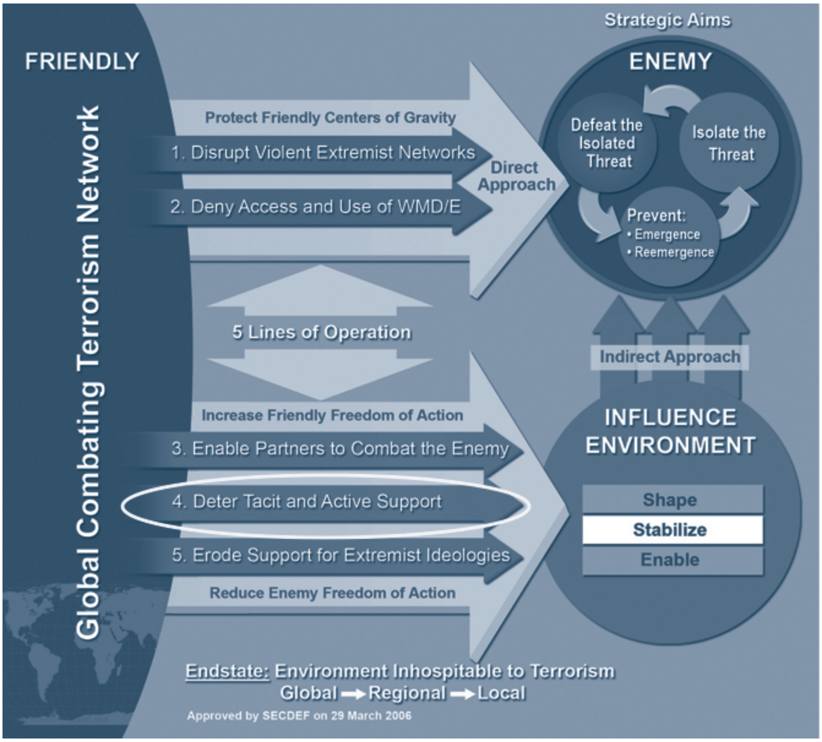

FRIENDLY
Global Combating Terrorism Network
Protect Friendly Centers of Gravity
1. Disrupt Violent Extremist Networks
2. Deny Access and Use of WMD/E
Direct Approach
5 Lines of Operation
Increase Friendly Freedom of Action
3. Enable Partners to Combat the Enemy
4. Deter Tacit and Active Support
5. Erode Support for Extremist Ideologies
Reduce Enemy Freedom of Action
Strategic Aims
ENEMY
Defeat the Isolated Threat
Isolate the Threat
Prevent:
• Emergence
• Reemergence
Indirect Approach
INFLUENCE ENVIRONMENT
Shape
Stabilize
Enable
Endstate: Environment Inhospitable to Terrorism
Global → Regional → Local
Approved by SECDEF on 29 March 2006

Figure 1 DoD GWOT Campaign Concept

However, at the outset of the 21st century, the recognition became widespread in DoD at the policy level that deterrence had to encompass far more than just the threat of nuclear retaliation. The adversaries we are facing are not going to be deterred by our nuclear arsenal or nuclear capabilities. Subsequently, the Nuclear Posture Review, submitted to Congress on 31 December 2001, introduced the idea of a new triad—not the old nuclear triad of sea-based, land-based, and air-based nuclear weapons but one composed of offensive strike systems (both nuclear and nonnuclear), active and passive defenses, and a revitalized defense infrastructure that will rapidly provide new capabilities to meet emerging threats. All three elements of the new triad are tied together by enhanced Command and Control (C2) and Intelligence, Surveillance, and Reconnaissance (ISR) systems.

In 2003, U.S. Strategic Command (USSTRATCOM) gained some previously unassigned duties associated with the new triad, taking on new missions including global strike, integrated missile defense, and information operations. In 2006, the Quadrennial Defense Review (QDR) introduced the concept of tailored deterrence. However, this new term in DoD policy needed further definition. Certainly, the term "tailored" implied that the United States would not rely on a one-size-fits-all solution anymore; the problem was much more complex than that. The three main elements of the tailored deterrence policy are to deny adversaries benefits from their actions, to impose sufficient costs on those actions to make continuing the action a non-viable option and to motivate them to accept the status quo—to realize that their current situation is better than the consequences of the aggressive action they were intending to take.

In the 2007 URW Symposium, Colonel Charles Lutes from the National Defense University introduced two terms:

- Deterrence: Convincing an adversary to not undertake acts of aggression
- Dissuasion: Convincing a potential adversary not to compete with the United States or take an undesirable path such as acquiring, enhancing, or increasing threatening capabilities

Preventing terrorist acts must combine deterrence and dissuasion. Tailored deterrence comprises three primary components that we can adapt to give the desired results:

- Tailoring to specific actors
    - Must adapt to type of actor
    - Must have knowledge of leaders, culture, and decision-making calculus

- Tailoring capabilities
  - Nuclear and conventional, kinetic and nonkinetic
  - Deterrence, dissuasion, and assurance
- Tailoring messages
  - Actions with multiple interpretations among different actors
  - Balancing general policies with specific responses

In discussing deterrence at the 2007 URW Symposium, Dr. Jason Castillo, who was then at OSD, made the following statement about nonstate actors, which was the general opinion at the time:

> *"Finally, for the nonstate 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."*
>
> *— Tailored Dissuasion and Deterrence, Dr. Jason Castillo, 2007 URW Symposium Proceedings*

Until now, it has been difficult to deter someone who has an ideological motive that you cannot hold at risk, giving them immunity to some of the consequences that we might impose on them.

The panelists discuss how we can deter tacit and direct support, how we can conduct Cognitive Systems Analysis (CCSA) to identify values as a basis for deterring terrorists, and how to use Information Operations (IO) to defeat al Qaeda and associated movements as well as perspectives on recent recommendations from the Iraqi Advisory Task Force (IQATF) on Information Operations.

5.2 DETERRING TACIT AND DIRECT SUPPORT

Paul Davis

THE DEFINITION OF DETERRENCE

The deterrence paradigm has changed, and the Cold War no longer provides a good model. Also, we phrase the problem in terms of "counterterrorism," but we are really discussing counter-insurgency and counterrevolution. To help frame this discussion, colleagues at RAND and I have distilled the following summary highlights of the latest principles in characterizing the terrorism challenge:

- Terrorists are opposed to the status quo, grandiosely ambitious, and uncompromising.
- Terrorist networks are shadowy, distributed, and hidden, making them difficult to target.
- Leaders have a discounted attachment to readily attacked targets.

Dr. Paul K. Davis is a senior scientist and Research Leader at RAND and a Professor of Policy Analysis in the Pardee RAND Graduate School. He has expertise in strategic and defense planning, counterterrorism, military transformation, high-level decision support, advanced qualitative and quantitative methods for modeling and simulation, ballistic missile defense, and defense acquisition. Previously, Dr. Davis served on the Naval Studies Board under the National Academy of Sciences and was given the Vance R. Wanner award by the Military Operations Research Society for lifetime achievement. He was a senior executive in the Office of the Secretary of Defense and holds a B.S. in Chemistry from the University of Michigan and a Ph.D. in Chemical Physics from the Massachusetts Institute of Technology.

- Some terrorists might even welcome martyrdom or apocalyptic events.
- Attributing the sources of attacks may be difficult.
- There are moral problems with collective punishment, especially indiscriminate retribution.

Many terrorists see themselves as revolutionaries in a sense. This is significant. We can all imagine ourselves in parts of the world and in societies where we would be revolutionaries. Saying that terrorists are against the status quo is not as inane as it may sound. Even al Qaeda, which is on the two-sigma end of the curve in many respects, thinks of itself as under attack.

Its members think of themselves as reactive. Their "organization" is diffuse, which makes them difficult to target, and their personal associations are likewise nebulous. It is hard to deter somebody who has discounted the connections to family and society that can be targeted or threatened.

Religious ideology is also problematic through its connections with martyrdom and apocalypse. Much debate revolves around how fundamental the ideological aspect is: which comes first, the ideology or the terrorism? Examining particular cases in that respect can become quite complex and confusing. However you sort that out, it is clear that some terrorists are at least willing to talk about—and some apparently do believe in—things like martyrdom and promoting an apocalyptic worldview.

Therefore, it is difficult to frame deterrence around these issues. In addition, if we were to be attacked again, it might be difficult to know where the attack came from. Sometimes that is hard to imagine because after 9/11, we did know where the attack came from; that may not be true in the future. The last point in the list at principles—the moral issue—really goes to the heart of some of the most difficult problems with deterrence. Certainly, underlying the Cold War were serious moral questions, but they could be rationalized—although it took quite a bit of work over the years. The moral dilemma is even worse today, however, because if you consider a massive retaliatory response to a terrorist attack, who is targeted? The relationship probably would be quite indirect. Many innocent people would be attacked, and that is difficult to justify.

Thus, the moral issue of retaliatory response to terrorism concerns collective punishment, which is a term that people seldom talk about; yet, historically, it has been one of the tools used to deal with terrorism. It is also indiscriminant on a broad basis.

THE SCORE CARD

Granted that these issues make deterring terrorism a difficult problem, how do we approach it? Where do we place our focus? In the context of some of the broader issues, the following checklist is based on the dominant conclusions Brian Jenkins and I have reached in studies since 2002—to provide a scorecard to see how we are doing [1–3]:

- Take a multifront approach
- Use a "systems approach;" terrorist system = entire network
- Think "influence," not just "deterrence"
- Sympathy of the population is crucial; terrorists may be their own worst enemy, but U.S. actions can hurt badly, generating impressions of arrogance, callousness, hypocrisy, and incompetence
- Unique problem: deterring use of WMD

One of the first conclusions Brian and I drew was that whatever it is we are going to do to respond to this threat, the approach will have to be on multiple fronts because the threat is not monolithic, as it was during the Cold War. No single, attackable "center of gravity" exists in the counterterrorism universe. A second conclusion we reached in 2002 was that we had to take a systems approach. We had to get over the notion that we had to attack al Qaeda leadership per se for success. Why? Because al Qaeda is a complex, multifaceted, Gordian network existing worldwide and consisting of leaders, followers, lieutenants, religious fanatics, logisticians, financiers, and so forth. Any of these parts could and should be targets.

Third, we need to think not in terms of deterrence but in terms of influence. This is a deep issue because words actually mean something, and they affect the way our minds work and the way we communicate. If we do not use the right words, we do dumb things; we become incoherent. The term "deterrence" has a lot of baggage, and it is very narrow. "Influence" is much broader. Thinking in terms of influence broadens the battle space in which we can seek to have important effects.

Fourth, for several years now, it has been clear that the sympathy of the population is essential on both sides. If the terrorists do not have the sympathy of the population, they can be in deep trouble. This may not apply to every kind of terrorist organization, but if we are looking for high-leverage areas to go after with influence—not just deterrence—then the sympathy of the population has to be a major factor. Historians can certainly confirm that. To elaborate, one point is that the terrorists are often their own worst enemies. Historically, that is correct: in the last seven years, we have seen al Qaeda run into trouble where they overextended. They attacked Muslims. When they did things that were not approved by society and by their own culture, they backed off a little, but then they would go back and forth. They have continuing struggles.

The other side of this issue probably has even higher leverage and is more troublesome. We can do a lot of damage to ourselves. If we look backward objectively, it is clear that between roughly 2001 and 2005, the United States did many things that were exactly the wrong thing to do—if the purpose was to gain the sympathy of the population for the al Qaeda cause. The good news is that phase is well behind us, and behaviors in recent times have been really quite different; we are moving forward with a different approach.

The last item in our list of conclusions from the 2002 study [1] is the unique problem of "deterring" the use of weapons of mass destruction. One of the troubling aspects of this problem, for example, concerns the relatively easy issue of biological warfare or dirty bombs. It is not clear what we can do in response to that threat other than the active measures of trying to intercept these weapons before they are deployed. It would be very nice if the people in the general region from which the terrorists come all believed in their gut that if the U.S. or the West were attacked with these weapons, they would be attacked too, even if not in a very straightforward way and not clear how. It would be good if they believed it was inevitable. Unfortunately, I do not think they do.

If we look at the preceding list of issues as a scorecard, I think the United States government is doing really quite well on several of these. Everyone seems to understand that we need to take a multifront approach and that we are facing a nebulous network. However, on the issue of influence versus deterrence, I give it half credit because people do not like to use the word influence; they like to use the word deterrence, even though it does violence to the history of the language. The Pentagon has also clouded the definition of dissuasion.

INFLUENCE VERSUS DETERRENCE

Figure 1 may help define what I mean by influence. Starting at the bottom, the figure lists actions that have been taken to deter or react to terrorism, and the scale shows the increasing level of violence each action implies.

The base of this list begins with the way the world has dealt with people who have engaged in terrorism over the centuries—actually millennia—that is, often they are co-opted. This is hard to imagine with somebody like Osama bin Laden, but if we are talking about the Global War on Terrorism, we are talking about activities in countries all over the world. Most of these places have local problems, and many of the people have what they think of as legitimate grievances. Many of them quite possibly will be brought into some kind of political system. If we rule co-optation out of our vocabulary—if we imagine that all terrorists have to be killed—we are going to lose because many of the local problems are real. The activists there are more like revolutionaries than they are just religious nuts trying to attack the West. Therefore, co-optation and inducement should be part of the kit in persuading and dissuading.

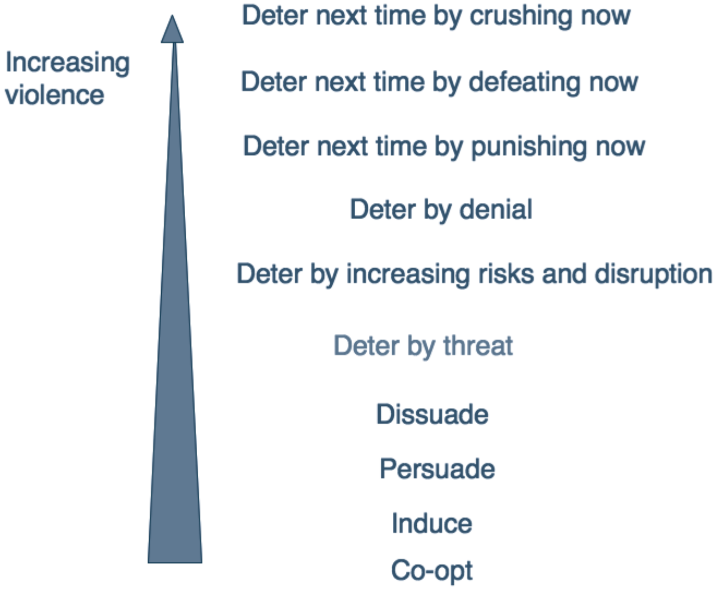

Increasing violence
Deter next time by crushing now
Deter next time by defeating now
Deter next time by punishing now
Deter by denial
Deter by increasing risks and disruption
Deter by threat
Dissuade
Persuade
Induce
Co-opt

Figure 1 An Escalation Ladder of the Coerciveness of Influence

At the top of Figure 1 are several kinds of deterrents from the Cold War—crushing, defeating, and punishing—that are now not as straightforward as the old tit-for-tat. They may still have value if we move our language into the broader construct of influence. I think we would find that it would affect the strategy and the tactics if we used that kind of terminology.

SYMPATHY MAPPING

I will briefly discuss our efforts in conceptualizing the contributors to sympathy with terrorism because it is not talked about as much or as systematically as one would think it ought to be. We will not find any magic bullets for countering terrorism, but if one exists, certainly understanding the sympathy of the population is a major tool. One of the things we are doing currently is assembling conceptual maps of all of the factors that affect the sympathy of the population for the terrorist cause. Figure 2 is an example of this kind of mapping. It is being adjusted in ongoing work, so think of it as an example, not a product.

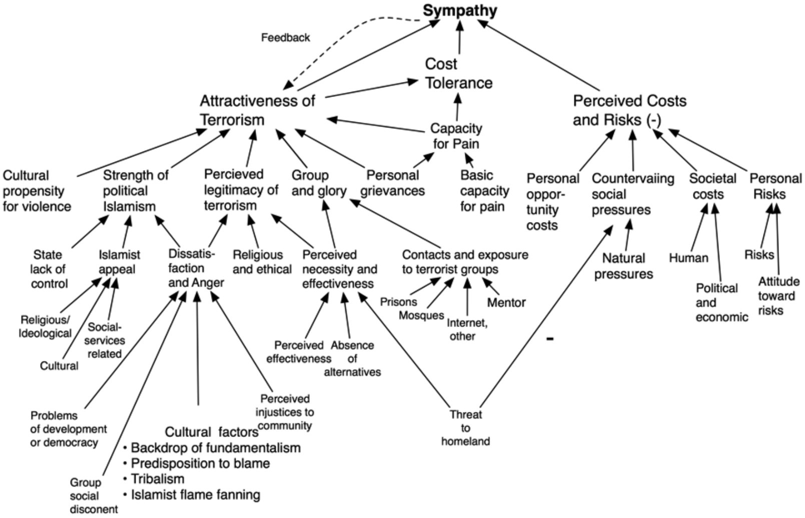


Figure 2 Contributors to Sympathy

There are degrees of sympathy. A person could be an extremist and ready to help and give shelter, arms, and money. He could be a sympathizer in the sense that he is all for the cause but does not want to get in trouble. Alternatively, he could be passive and try to avoid everything that is going on and put blinders on. Finally, he could be oppositional—i.e., not sympathetic but positively working to oppose terrorism and willing to turn people in. The objective is to move people along that spectrum toward oppositional; we would like people who tend to be passive to become actively oppositional, and we would like that to stick.

If you think about this in the framework of disease—where terrorism is a disease—part of the challenge is to reduce the contagion, but part of it is also to deal with those who recover and to try to make sure they do not get the disease again. What are the factors underlying sympathy? Although it is a work in progress, the map in Figure 2 has some interesting features. One is that—if you look at it objectively—the population is not sympathetic to terrorism just because they do not like the United States or they do not like the West in general. They might see positive values in the causes that use terrorism, and the positive values may arise from their personal grievances—for example, their brother, their cousin, or their spouse was killed—or that they are drawn into it because of the excitement that attracts people (especially young alpha males) to join organizations that are new, exciting, and seem to expand their horizons. They could be sympathetic because they think that terrorism is legitimate and because there are societal grievances of a gross nature; the only way they can deal with them is by using terrorist tactics.

Another factor that could be driving their sympathy is political Islamism—a term that is the source of much controversy. In other words, their motivation could be religious. On the other hand, it could be that, in part, they live in a society in which violence comes very easily. Some of the analysts I work with make this point, particularly about tribal cultures in which the history of violence is longstanding, and it is just a natural thing for them to fall into.

In short, the purpose of this exercise is to map the causes of sympathy to terrorism so that we can identify what we might be able to do about each of these factors. In many cases, the best thing we can do is to not do anything bad. In other cases, we might be able to take some actions, primarily in the realm of strategic communication, although I think that most people working on the terrorism problem would ultimately agree that strategic communication—if only we knew how to do it—would be a very high-leverage element. If anything, we are better at being bad at it than we are at being good.

On the right side of Figure 2 is a cluster that represents the economists' view that an important tool for affecting sympathy of the population may just be cost-benefit calculations. Data from the Vietnam War supports this view. You try to get the population to think pragmatically about what is in their best interest. In the middle of Figure 2 is a cluster of factors that are more visceral; they have to do with a population's capacity for pain: "This cause is all very fine, but I just cannot take the pain anymore." That would be a good thing for us to get some populations to believe. If you look at various places where terrorism is used, you certainly do see a fatigue reaction in the populace, where the cost-benefit calculation is not really the right language to use; "war weary" is a better term.

Figure 2 represents a beginning map of all the contributing factors. Better depictions will be forthcoming [4]. However, we are attempting to be systematic about drawing connections between everything we have learned from the social sciences, considering all of the different theories to try to make sure that we are representing the many factors that arise from the various research strands in a picture that is somehow integrated and coherent. That is where our work is leading us in better defining deterrence and influence.

REFERENCES

1. P. K. Davis and B. M. Jenkins, *Deterrence and Influence in Counterterrorism*, RAND, 2002.
2. P. K. Davis and B. M. Jenkins, *Deterrence and Influence in Counterterrorism: a Component in the War on al Qaeda*, RAND (2002).
3. P. K. Davis and B. M. Jenkins, "A System Approach to Deterring and Influencing Terrorists," *Journal of Conflict Management and Peace Science*, **2**(1), Spring, 2004.
4. P. K. Davis and R. Kim Cragin (eds.), *Social Science of Couterterrorism*, RAND, in preparation.

5.3 VALUES AS A BASIS FOR DETERRING TERRORISTS: CULTURAL-COGNITIVE SYSTEMS ANALYSIS (CCSA)

Christine MacNulty

CCSA FUNDAMENTALS

I believe that we need to be thinking more about influence, Information Operations (IO), and strategic communications as a basis for deterring terrorists and their supporter. Five years ago, I began to examine what was being done in these areas and concluded that there were many good pieces of work underway, both analytical and operational, but many of them were fragmented.

Although we talk about seeing and thinking about things from a systems perspective, we often tend not to do that. If we are going to conduct effective, influential information operations or strategic communications, we must consider three elements of the system: cultures—what people in a particular culture believe, what their values are, what motivates them; cognition—the way people actually make decisions; and networks—be they social, complex, or communication networks. Therefore, together with

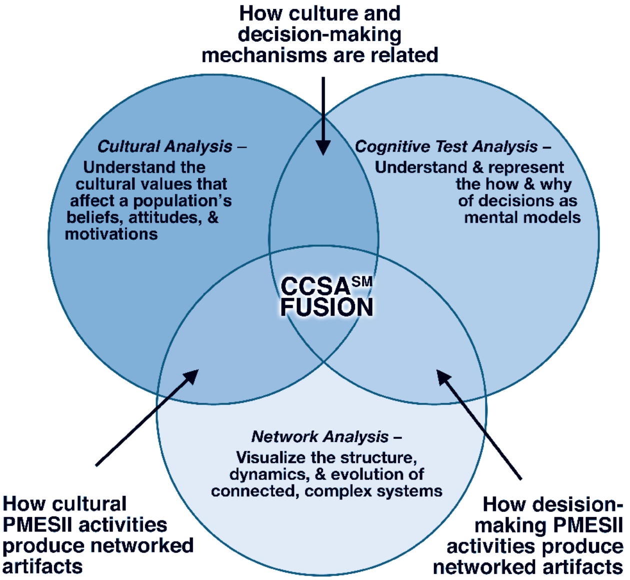
Christine A. R. MacNulty, founding President and CEO of Applied Futures, Inc., has more than 35 years experience as a consultant in long-term strategic planning, technology forecasting, technology assessment, and socio-cultural change. Her clients include The Joint Staff, OSD, USMC, USCG, USA, and NATO. She has applied her knowledge of strategy, culture, and cognition to understanding our adversaries and assessing effective nontraditional operations, information operations, and strategic communications. A prolific writer, she is the author of the Army War College monograph, "Transformation: from the Outside In or the Inside Out?" to be published Fall 2008. She was elected a Fellow of the Royal Society of Arts, Manufactures and Commerce for her contributions to British industry. Her monograph, "Truth, Perception and Consequences" was also published by the Army War College.

two colleagues from different organizations, we have developed the idea of Cultural-Cognitive Systems Analysis (CCSA^{SM}):

- **Cultural Analysis** determines cultural characteristics of a group—its values, beliefs, and motivations.
- **Cognitive Analysis** determines decision-making processes of a group—its mental models, cues, and factors.
- **Complex Network Analysis** determines the dynamics of group—its interactions, structural strengths, and vulnerabilities

CCSA^{SM} fuses cultural, cognitive, and network findings into an IO planning and assessment tool.

Figure 1 shows how these three elements intersect. Looking at it as a Venn diagram, we could consider any of these areas individually, in pairs, or all three at a time. That is the essence of the notion of CCSA^{SM} fusion.


How culture and decision-making mechanisms are related
Cultural Analysis – Understand the cultural values that affect a population's beliefs, attitudes, & motivations
Cognitive Test Analysis – Understand & represent the how & why of decisions as mental models
CCSA SM FUSION
Network Analysis – Visualize the structure, dynamics, & evolution of connected, complex systems
How cultural PMESII activities produce networked artifacts
How desision-making PMESII activities produce networked artifacts

PMESII – Political, Military, Economic, Social, Infrastructure, and Information

Figure 1 The Fundamentals of Cultural-Cognitive Systems Analysis (CCSA)

The basis of cultural analysis is looking at the totality of a culture. We examine the culture from an anthropological point of view, but we also look at people's values, beliefs, and motivations. If we are talking about communications, it is through values, beliefs, and motivations that I believe we get the biggest payoff.

When we conduct cognitive analysis, we are thinking about how people make sense of things and what kinds of decisions they make under what kinds of circumstances. What are the cues and the factors that trigger them to do as they do?

Finally, network analysis determines the nature of group interaction in complex systems. We include all forms of network analysis, such as media usage, media habits, and any cultural or cognitive artifact that reveals the topology of group interactions; dynamics such as amplification and feedback; and how influence campaigns evolve through cultural drift and segmentation. CCSA^{SM} is a genuine fusion of these three areas.

CULTURAL ANALYSIS

We all have values and beliefs. Generally speaking, values and beliefs are long-term. They can last on the order of 20 years or even a lifetime. My mother and mother-in-law both died at ripe old ages with the same values that they had when they were teenagers. People's values tend to change slowly.

Values and beliefs manifest in the medium-term (2 to 5 years) as attitudes and lifestyles; those in turn manifest in the short-term (less than 2 years) as behavior. We are most concerned about people's behavior. That is the thing we can influence most easily. We are never going to influence values and beliefs in the short-term. If we want to influence them, we need to have a long-term strategy that is on the order of 20 years or so. We should be good at long-term strategy. However, generally speaking, we are too caught up in the moment. We want quick results, so we do not focus on our long-term strategy. However, in the short-term, we can begin to influence behavior. As people's behavior changes, it feeds back into their attitudes. Gradually, as those attitudes change, that feeds back into values and beliefs.

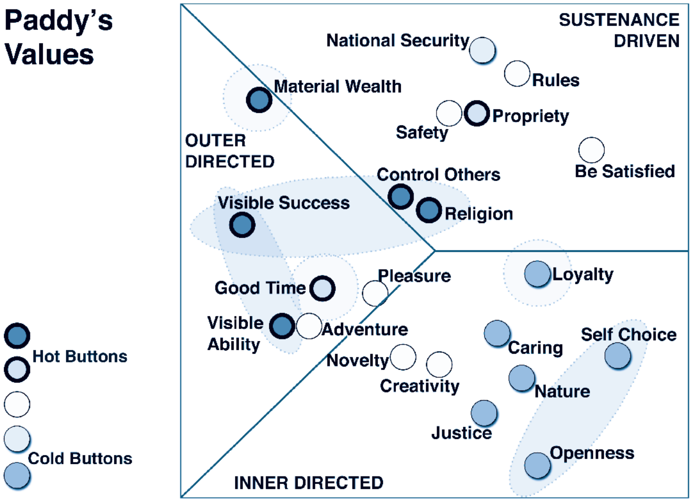
Values are key for effective communication. So, what are they? Values serve as standards and criteria for choices of all kinds, and they are ordered by relative importance. Values are beliefs that tend to have a very strong emotional component to them. These beliefs are tied inextricably to emotion—they do not come from objective, rational, or cold ideas; they operate subconsciously.

Certainly, we need some logic, but one of the things that we forget in IO is that we also need emotion. Values provide the background—the fundamental underpinning—for motivation. They are a motivational construct—referring to desirable goals people strive to attain. Of course, strong motivation is what a terrorist must have to become a terrorist and do all kinds of nasty things. We need to understand the terrorists' motivations. Where do they come from? If we understand motivations, then we can anticipate what he is likely to do next. If all we can do is extrapolate behavior, we are never going to be ahead of the game. Thus, understanding motivations is also a key to developing effective communications.

MAPPING VALUE SYSTEMS TO MOTIVATIONS

Applied Futures recently completed a successful pilot project using the CCSA^{SM} approach. Unfortunately, I cannot tell you the nature of the pilot project so I have translated it to show you how we can use CCSA^{SM} to build a motivational map. I will use the example of the Real IRA, which is a dissident splinter group of the Irish Republican Army (IRA) that is beginning to stir things up again.

This CCSA^{SM} examined the values, beliefs, and motivations of a group of Real IRA people—loosely termed Paddy—to develop a typology, i.e., a set of types of people within a population. Although the pilot project developed a typology of six different groups that could be expanded to 12, this example focuses on one particular group—Paddy—that has the set of values illustrated in Figure 2. These values are derived from Shalom Schwartz's Values Portraits [1, 2].



Cold Button Issues

- I think people make too much of the equality thing. Nothing says the world has to be fair – and, anyway, I'm not going to worry about justice for people I don't know.
- Taking care of the environment is another of those overplayed issues. Nature can take care of itself.
- I don't feel a particular need to help others around me.
- It's not important to me to be loyal to my friends.
- National security is not a big issue for me.

Hot Button Issues

- It's important for me to have lots of money and material things.
- It's important for me to be seen to be successful. I like to impress other people.
- I need to show my abilities. I really want people to admire me for what I do.
- Religious belief is important to me. I try to do what my religion requires.
- It's important to have a good time and I like to "spoil" myself.

Figure 2 Motivational Analysis of the "Paddy" Group

We performed a two-factor Principal Component Analysis (PCA) on the responses to the Schwartz portrait questions to give us the map shown in Figure 2. We also referenced them to Abraham Maslow's hierarchy of human needs [3, 4] as a basis from which to think about the broad areas of values (i.e., Outer-Directed, Inner-Directed, and Sustenance-Driven values). In Figure 2, the spots marked Rules, Safety, Be Satisfied, Adventure, Pleasure, Novelty, and Creativity represent the values that are neutral for the Paddy Group, indicating they are not very strong on them one way or another. The "hot button" spots are Propriety, Material Wealth, Control Others, Religion, Visible Success, and Visible Ability, while Good Times and Propriety are "warm buttons." These are the values that the Paddy Group holds that statistically are significantly above the norm.

Loyalty, Caring, Self-Choice, Nature, Justice, and Openness are values that Paddy holds that are statistically significantly below the norm—Paddy's "cold button" issues. National Security is a "cool button." Figure 2 gives a few examples of Paddy's hot and cold button values in his own words. (Refer to the URW Web Site for the complete version of this example.) Examples of hot buttons are "It's important for me to have lots of money and material things. It is important for me to be seen as successful. I like to impress other people." Cold button values include "I'm not hung up on making my own decisions. I do not feel a particular need to help others around me. I'm not driven to care for other people."

Using each of these values, we can analyze how Paddy sees the world—how he feels—and which of the values that are likely to inhibit him from becoming a Real IRA terrorist. In this case, the material wealth, desire for a good time, and lack of loyalty values demonstrate that Paddy is very self-interested and he has a strong desire for wealth. I would suspect that terrorists do not generally get very wealthy, and they probably do not have much of a good time. Therefore, we could use these specific buttons to formulate a strategy about how to influence him away from terrorism.

However, Paddy has a pretty strong motivation to become a terrorist, particularly in "hot button" values to do with Visible Success, Control Others, Religion, Visible Ability, Self-Choice, and lack of Openness. One of the key "cold buttons," in this respect, is that Paddy is definitely not open to change; he does not want to know about other people and other people's values.

Thus, Figure 2 represents how we can develop this kind of values portrait for each of the groups in a typology, using both hot and cold buttons, and expert assessment of the combinations of values that enhance or inhibit a move to terrorism. As I mentioned, the pilot project identified six different groups.

How do we use this typology map? It becomes a piece of a profile—a synthesis about Paddy or Paddy's group—a persona that indicates his demographics, his main characteristics, and his tendencies to act in particular ways. From our cognitive work, we can then look at the factors that cause him to make the kinds of decisions that he makes, which we combine with the values that I have just described to flesh out the meaning of the top hot and cold buttons that drive this type of person. Figure 2 provides some examples.

We can then place Paddy on a continuum from being a moderate loyalist who supports the government to being an extreme radical. Generally speaking, I would say that it is very difficult to even think about influencing somebody at the extreme radical end of this spectrum. Whether they are from the Real IRA, terrorists from the Middle East, or any kind of ultimate extremist, these people are pretty intractable.

We do not really need to influence those at the other end, either; they are already pretty loyal to the government, although we might want to support and reinforce their loyalty. The key area is somewhere in the middle of the spectrum. Based upon the values and our understanding of what they mean to the individual—his motivations—we can place Paddy on this spectrum and can even estimate the size of the potential group from which Paddy comes. Once we have done that, we can then decide how to approach them.

Crafting the Right Message

We use a range of methods in our communications—everything from relationship marketing, which comes from the values and the cognitive factors, to mass marketing and viral mass marketing, which is becoming popular at the moment. For this particular group, a mass message generation is below the baseline in the total audience it can reach; i.e., mass marketing does not really work for the Paddy Group. Instead, a focused, viral message (the solid line in Figure 3) can reach twice the audience of a mass message, as shown in Figure 3.

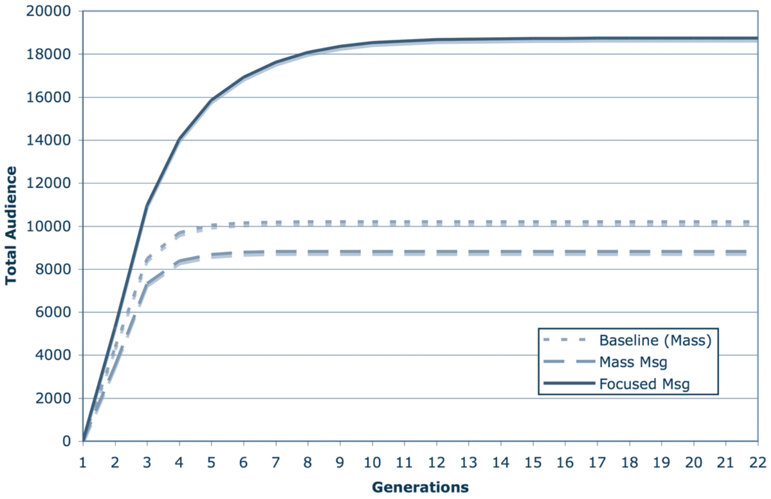


Figure 3 Total Audience Reached by Number of Generations of Mass and Focused Messages

Thus, CCSA^{SM} provides a profile of the values of the target audience from which we can decide which hot buttons to push or which cold buttons we must absolutely not push. Two basic principles come into play here:

- It is far easier to persuade than to dissuade. If we can shape messages that might convince Paddy to take actions that would be in his best interest, we are likely to have better results. The task of persuading Paddy to do things in his best interest is easier than dissuading him from doing things that benefit us—or do not harm us. We know never to include in our message ideas that reinforce Paddy's cold buttons because those will really turn him off.
- Messages that appeal to value need to be emotional. They must contain some logic, some factual data, but, generally speaking, the message needs to be emotional.

CONCLUSION

I want to conclude by reiterating this connection between values and the emotional dimension. To work effectively, messages must contain emotional content as well as facts. The emotional dimension can be brought out through words, images, and even music. The more we know about motivation, the better we can frame both the message and the medium through which we convey the message to alter behaviors and attitudes. As the value spaces in Figure 2 illustrate, there are complex relationships among outer-directed, inner-directed, and sustenance-driven values that cause somebody to say "yes" or "no" to terrorism. Although we need to be careful how we push those hot or cold buttons, we should be able to do it effectively if we can understand and internalize the values.

The key is to get inside Paddy's heart and mind and see the world through his eyes; understanding his values enables us to do that. Knowing these values, we can tap a variety of techniques that have been developed from various disciplines—techniques for persuasion, for influence, and even those developed through the personal growth movement—that we can apply to get inside Paddy's heart and mind. If we can do that, then we can communicate, and influence effectively.

REFERENCES

1. S. H. Schwartz, "Universals in the Content and Structure of Values: Theoretical Advances and Empirical Tests in 20 Countries," In M. P. Zanna (Ed.), *Advances in Experimental Social Psychology,* (**24**) 1–65, New York: Academic Press, 1992.

2. S. H. Schwartz, G. Melech, A. Lehmann, , S. Burgess, M. Harris, and V. Owens. "Extending the Cross-Cultural Validity of the Theory of Basic Human Values with a Different Method of Measurement," *Journal of Cross-Cultural Psychology*, **32**:519–542, 2001.

3. A. H. Maslow, "A Theory of Human Motivation," *Psychological Review,* **50**:370–96, 1943.

4. A. H. Maslow, *Motivation and Personality*, New York: Harper, 1954.

5.4 RECOMMENDATIONS FROM INFORMATION OPERATIONS ADVISORY TASK FORCE (IOATF)

Bruce Gibson

My goal is to speak as an information operations “operator” about some of the programs that are under way, point out some of the conflicts, and present some of the lessons that the Information Operations Advisory Task Force (IOATF) is actively learning—not at a 30,000-ft level but at a tactical level because the capabilities on the ground are the most important. The men and women that are serving need the tools and the methodologies now that will make them successful.

One of the programs in theater is one that we originally deployed to support Brigadier General Mark McDonald. It is not the only program underway, so I want to put out the general disclaimer that the operations I describe are not the be-all and end-all of the programs being conducted. They are means to bring information into the planning cycle that is incredibly relevant to the discussion today.

How do we inject the support, the life cycle, and the network into the environment in which our operators are living, breathing, and surviving? It is a complex equation because of factors such as economics, religion, culture, and tribal agendas, some of which we understand only superficially.

Mr. Bruce Gibson is the director of International Operations with SOS International. He is a retired U.S. Air Force officer, graduate of the U.S. Air Force Academy. He has served with Air Force Special Operations, Joint Special Operations Command, and U.S. Special Operations Command (SOCOM).

The IOATF is a program—an Iraq task force—developed to bring that cultural dynamic into the discussion and into the planning cycle. Programs like IOATF and some of the polling programs are very important tools that we need to implement and integrate into our methodology. For us to interdict and become part of the Iraqis' planning cycle, it is key that we understand how their society functions and how they think. It is easy to say, but it is very hard to do.

The IOATF employs nearly 200 U.S. operatives, who run a network of approximately 500 local nationals that is designed to map the human terrain to identify who the people in Iraq are and what they feel and think. The purpose is to improve situational awareness to help the local military commander and his staff identify who lives in the region and area of operations, the key influencers, the dynamic demographic of the local population, and what motivates them to support the counterinsurgency, or the insurgent or terrorist groups that may exist now or in the future. The following are some of the methods IOATF employs:

- Gather information, conduct analysis, and provide timely solutions and advice to command staff at the Force, Corps, Division, Brigade Combat Team (BCT), Regimental Combat Team (RCT), and Battalion (BN) levels.
- Facilitate access to key officials in the government and "influence targets" within selected communities.
- Improve understanding of cultural, religious, economic, political, and tribal biases and dispositions.
- Provide regional and tribal perspectives on specific issues and events.
- Fuse all source information and provide support across all staff functions at tactical, operational, and strategic levels.
- Assist with lethal and nonlethal targeting, gauging effectiveness of media campaigns—IO and psychological operations (PSYOP) products, programs, and initiatives.

Because IOATF was originally designed as a tactical program, the way it is structured increases its effectiveness. It was designed and employed largely at the BCT level in support of the division commanders. From my observations of the program in 2003 as an active duty member, I concluded that it was effective because it was designed to afford the commander eyes and ears outside the fence line. It became a means of not only seeing and hearing outside the fence line but also interpreting what was going on in the various communities and regions within Iraq.

It provided the commander with a pipeline to the citizens, allowing dialogue with people in the street—the ability literally to ask questions about what the people were seeing from the corner of X Avenue and Y Street—not only to get their perceptions of what was happening but also to know what they were thinking. For example, what services were they lacking? It gave the commander information with which to tailor a campaign plan that would deliver basic social services to initiate IO-type campaigns that could hit the key issues that would resonate with the local population.

An essential part of the equation is knowing which Iraqi citizens in that pipeline are key influencers because a U.S.- or Coalition-crafted message is very quickly outted as not credible. Colonel Lloyd brought up the point that the Iraqis have to see it to believe it. Simply hanging a commercial out there or dropping a leaflet is one means of communicating that we are here to support the citizens of Iraq. However, what they truly understand—what is really meaningful to them—is when you deliver them a service that they recognize as being needed or valued; that is the message that is believable.

The key for us as planners is to know what the real needs are and who is going to be seen as a credible, long-term provider of the message, the service, the food, the medical assistance, the trash removal—and the list goes on. Ultimately, the most important roles our teams play as we look ahead are bringing the information in, integrating it into our military planning processes, and refining the decision-making processes, both at the tactical level and now, more and more, at the strategic level.

Many of the IOATF people are involved in this IO campaign, and they are integrating it with the civil affairs and the medical elements on the ground. The products that our crews produce are very reflective of what the local commander needs and wants. The following list is a summary of some of these products generated from over 3,000 reports per month:

- Periodic reports (weekly "Word of the Street"):
  - Mosque monitor reports (firsthand information)
  - Word on the Street (local perspectives and commentary on a national scale)
  - Price surveys (surveys conducted of food items, fuel, perishables, etc.)
- Multiple source information papers and studies: Request for Intelligence (RFI)-focused, key "interest areas," local Web sites, local media reporting, etc.
- Quick response replies: RFI-focused, targeted responses required in less than 24 hours
- Executive Summary (EXSUM) reports: personal accounts of conversations and contact reports
- Special Advisor (SA) support: personal introductions and action items
- Strategic communications initiatives: media assessment reports, IO effects assessments, and local media outreach
- Spot reports: event-driven, quick-reaction eyewitness reporting (not necessarily driven by customer requirements)

The top three items in the list are our best sellers. Out of the 3,000-plus reports we produce each month, the report about what is said in the mosque is the most-read. In many of the local communities, the key influencers are often the mosque leaders. We may not necessarily be driving the rhythm, but that is definitely how the rhythm is being communicated. It is essential for us to understand issues on both a national and local level. Strategically speaking, we need to know how the demographics break down countrywide and by neighborhood so we can understand how the word on the street changes in response to our IO campaigns.

When we do conduct a kinetic campaign, is it perceived as being productive, helpful, or destructive? When we produce a softer science or a medical improvement, is that seen as being more helpful? Economically, we need to conduct price surveys to track the prices of food, fuel, medicine, and other commodities as they change.

MULTIFUNCTIONAL TEAMS

Our methods still rely to a large extent on an old-school type of a technology: We use Multifunctional Teams (MFTs) consisting of Military Analysts (MAs), who are former Special Operations personnel, and we pair them up with local Iraqi Advisors (IAs), who are Iraqi citizens or Iraqi-born Americans. The IAs can provide us with the cultural background and understanding of the ways of the locals and the lay of the land, and they give us the language capability as well. The MFTs typically recruit and drive a network of 8 to 14 local and national advisors. They develop the informant network to solicit and gather raw information in response to standing requirements and RFIs from the local commander. Each MFT provides professional quality information, technical assistance, analysis, and written products as well as advice and assistance to commanders and their staff in planning kinetic operations and focused IO campaigns. As shown in Figure 1, the MFTs are deployed theater-wide, focused on eight functional areas that are geographically spread. A typical MFT is coupled to an operations center that is co-located with the division commander and the functional teams.

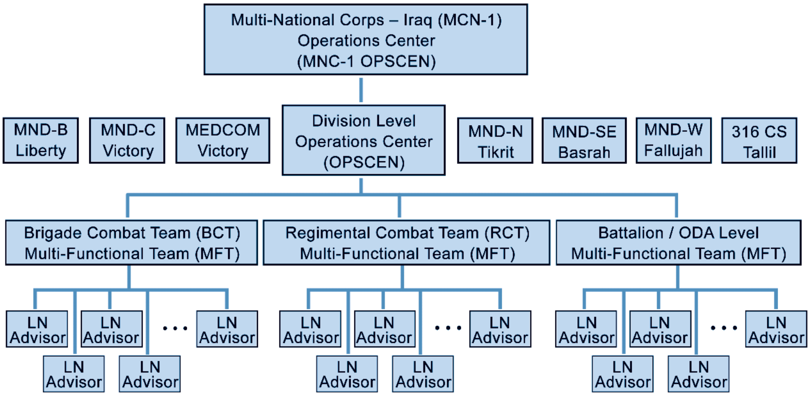

Multi-National Corps – Iraq (MCN-1) Operations Center (MNC-1 OPSCEN)
MND-B Liberty
MND-C Victory
MEDCOM Victory
Division Level Operations Center (OPSCEN)
MND-N Tikrit
MND-SE Basrah
MND-W Fallujah
316 CS Tallil
Brigade Combat Team (BCT) Multi-Functional Team (MFT)
Regimental Combat Team (RCT) Multi-Functional Team (MFT)
Battalion / ODA Level Multi-Functional Team (MFT)
LN Advisor
LN Advisor
LN Advisor
LN Advisor
LN Advisor
LN Advisor
LN Advisor
LN Advisor
LN Advisor
LN Advisor
LN Advisor
LN Advisor
LN Advisor
LN Advisor
LN Advisor

Figure 1 Multifunction Task Force Organization

As we go forward, one of the major challenges we face is that, because we generate a lot of product, we also generate a lot of white noise—information that may not be useful. We need to find new ways to filter, analyze, fuse, and focus that information for consumption by the local commander.

5.5 EXPERIENCES FROM THE FIELD: USING INFORMATION OPERATIONS TO DEFEAT AQAM

Karen Lloyd

The following quote shows the individual frame of reference and the human side of the topic presented here, i.e., perspectives from those in the field actively engaged in using information operations to defeat al Qaeda and associated movements (AQAM):

> *Somewhere a True Believer is training to kill you. He is training with minimum food or water, in austere conditions, day and night. The only thing clean on him is his weapon. He doesn't worry about what workout to do, his rucksack weighs what it weighs, and he runs until the enemy stops chasing him. The True Believer doesn't care "how hard it is." He knows he either wins or he dies. He doesn't go home at 1700; he is home. He knows only the Cause. Now, who wants to quit?*
>
> *— Unknown source, Fort Bragg, North Carolina*

Colonel Karen Lloyd entered army ROTC through Wheaton College. After earning a master's degree in political science from Duke University, she taught political science courses at West Point as well as elective courses in media, public opinion, and political participation. She transitioned her career into information operations, served in Bosnia, and then as the Information Operations planner and observer/trainer, she provided IO training and coaching to multiple National Guard divisions and brigades preparing for rotations to Bosnia, Kosovo, Iraq, and Afghanistan. In August 2005, she deployed to Iraq where she served as the Multinational Force, Iraq, Information Operations chief. In 2006, she was reassigned to the Joint Special Operations Task Force, where she served as Information Operations chief through 2007.

I share this quote to emphasize that our soldiers, who have been fighting and serving down range, understand the passion and the total commitment of the enemy with whom they are fighting. I submit that we need to approach our fight against the enemies with the same passion and total commitment with which they approach us.

I will begin by defining the problem—two problem sets, actually: (1) terrorists who are actively participating in attacks and (2) those who are supporting those attacks through silence, inaction, or some other form of implied consent. However gratifying it may be for those of us that wear the uniform to engage in the kill-capture operations, we realize that is not the decisive fight. We will not kill our way to victory; we have to focus more on the disruption and denial of sanctuary. We can do much of that through Information Operations (IO).

THE AUDIENCE FOR INFORMATION OPERATIONS

Figure 1 compares the two types of supporters of terrorism: active and tacit. This is a simplistic overview, but it helps in identifying the basic underlying beliefs, motivations, and values of the adversaries and potential adversaries we are attempting to influence. If we cannot understand them, we cannot hope to change them. In considering targeting strategies for information operations, we look at how to appeal to both logic and emotion, realizing that both are important.

I want to illustrate two approaches. Although these strategies will appear to focus mainly on the populace that is providing tacit support, many regional governments are also providing tacit support. We know that most of the foreign fighters that come into Iraq come in through Syria. We have relatively good reason to believe that the Syrian government is providing tacit support by looking the other way as those fighters cross the border. Why would they do that? We have indications that they do so because of a somewhat quid pro quo arrangement in which al Qaeda refrains from attacks within the country and the government, in exchange, provides that indirect support by looking the other way. Thus, our challenge is to do a good job—and this is somewhat outside the scope of the military—of convincing those other governments that al Qaeda poses a real and credible threat to them in the long term.

Active Supporters	Tacit Supporters
Who are they?	Who are they?
Fighters	Populace in areas of hostilities
Leaders	Regional governments
Financiers	
Recruiters/media	
Why do they support?	Why do they support?
Ideological commitment	Fear
Desire for power/glory	Financial considerations
	“Quid pro quo” arrangements
	Mutual anti-Western bias
Targeting strategies:	Targeting strategies:
Create friction/suspicion	Demonstrate success (not an invincible enemy)
Highlight moral/religious inconsistencies	Highlight alternatives
Provide examples of “My Recruiter Lied”	Provide moderate “heroes”
Demonstrate “lost cause”	Demonstrate long-term risks
Embarrass, shame, dishonor	

Figure 1 Analysis of the Audience for Information Operations

We also have to do something to get past the anti-Western bias in which the people in a region feel that attacking the U.S. is justified just because they do not agree with U.S. policies or take issue with what they perceive U.S. behavior to be based on our actions in theater.

EXPLODING THE MYTHS

Two myths must be dispelled to fairly assess the sorts of hot button issues among the populace and allow us to shape effective IO. When I first arrived at MNFI, we were told over and over, "You need to drive a wedge between al Qaeda and the Iraqi people." Hence, working with the public affairs community, we put together press conferences, press releases, and an information campaign that highlighted the atrocities of al Qaeda attacks—they attacked this, they killed this many people, etc. Our influence products and IO push focused on showing the devastating nature of al Qaeda attacks, the violence, and the people whose lives were forever changed as a result of their attacks.

However, if we had looked at our own polling, we would have seen that generally less than 5% of the Iraqi public identified with al Qaeda ideologically in any way, whether they agreed with them on religious grounds or saw them as providing hope for the future of Iraq. Most did not agree with al Qaeda's principles. Most of those who supported al Qaeda did so out of fear; they were worried about the security of their country. Thus, the following results of polling the Iraqi people exploded the myth that "The Iraqi people support al Qaeda."

- Less than 5% of Iraqis identify ideologically with al Qaeda.
- Most Iraqis who provide tacit support do so out of fear for themselves and their families.
- When Iraqis were asked about their assessment of the security situation, most were relatively positive about their own neighborhoods, less positive (in general) about their regions, and very negative about the country overall.

In the last polling question—which may initially seem somewhat unrelated—we asked Iraqis what they thought about the security situation in their neighborhood, in the region, and in the country at large. Our analysis led us to conclude that what they perceive in their neighborhoods—what they see firsthand with their own eyes, what their families and friends see—is not too bad.

What they perceive about the nation comes from TV, our press conferences, and our media reports and influence products.

The bottom line was that our emphasis on publicizing devastating al Qaeda attacks actually served to reinforce security concerns and paralyzed good citizens with fear. We concluded that our campaigns were actually counterproductive to the extent that some of the messages that we were sending—which showed how devastating and horrible al Qaeda was—were actually fueling Iraqis' fear and contributing to the paralysis and tacit support. I am pleased to say that we have moved away from the "Driving a Wedge" strategy towards showing that al Qaeda is a force that can be beaten. Nevertheless, we struggled with this for quite a while.

Another example of the kinds of myths that tend to circulate—this one derived from informal, anecdotal surveys—is that suicide bombers are committed martyrs. Although that may be so in a few cases, the majority of them are not, based on our experience with forensic analysis. What real evidence we have about suicide bombers that we could trace forensically indicates that most suicide bombers are foreign fighters originating from outside of Iraq. Many of them are recruited not by the lure of becoming a martyr and dying for Islam but the notion of joining the holy war. They had come to fight the Christians—fight the Infidels.

The foreign-fighter network is not one in which someone just leaves Saudi Arabia, drives to Iraq, and becomes a foreign fighter. There is an extensive network of facilitators that gets these people into the country and into position to conduct these acts. These facilitators confiscate their passports and keep them relatively isolated in very closed environments: no contact with the outside world, no contact with family, and very little opportunity to see anything else. After six months or so, many of these folks are so hopeless that they see suicide attacks as their only option. They do not have passports, and they cannot go home; going home would mean disgrace and dishonor to their families, so suicide becomes their only option. We have also seen many cases where the suicide bombers are unwitting, or unwilling, participants. We have seen al Qaeda use mentally and physically handicapped people to conduct their attacks. We have also seen instances where people thought that they had control over the detonation of their suicide device when it was actually controlled remotely by someone else in case that person had a change of heart at the last minute. Finally, we have seen cases where people were truly unwilling—hands duct-taped to the wheel of the vehicle that they were driving. How many of you have heard a lot about this?

I submit that we have not heard as much as we should. The bottom line is that we allow al Qaeda to gain ideological ground by not exposing these situations to the greatest extent. We should be advertising the fact that suicide bombers are not just martyrs. They are truly dedicated folks, and al Qaeda is exploiting this as much as they possibly can.

SUCCESSES

We realized fairly early on that the detention centers that the Coalition operated were breeding grounds for terrorists. Minor criminals would enter our prisons, and they would leave as hard-core jihadists because of the extremist religious education they were exposed to within the walls. To solve this problem, we reached out and conducted a global survey to examine some other models of success—Egypt, Saudi Arabia, Jordan, and Singapore—where they had successfully rehabilitated criminals within their prisons. We were able to capture some of that knowledge and incorporate some of the same practices through local imams in Iraq to moderate extremist propoganda. We have had some initial success with these methods, and I would submit that the long-term success will depend upon conveying that knowledge to the Iraqis, handing it over to them to educate their own people to continue the program.

Imam Mohamad Bashar Arafat, an American Muslim imam from Baltimore, who is Director of Civilizations Exchange and Cooperation Foundation, has traveled throughout Muslim countries with the close coordination of the State Department. He brings with him other Muslim Americans and Christian Americans, and they meet with small groups of people in these local areas. They meet with women's groups, kids, religious leaders, and rural groups in people-to-people exchanges to dispel the notion that America is at war with Islam. They present a view contrary to the one al Qaeda is trying to promote, and in the areas where they are able to go, they are very successful. They are very welcomed and well received.

Another area where we have had some success is our "Al Qaeda is Losing" campaign, which we started after we realized that the "Driving a Wedge" campaign was not the right approach. We really needed to demonstrate that al Qaeda could be beaten so that people would not be paralyzed with fear. Therefore, we are using IO to bring to light some of the successes that we have had against al Qaeda militarily. We have highlighted our ability to locate and eliminate al Qaeda by conducting "find, fix, and finish" operations. We have also spotlighted the success of local Iraqis by standing up to al Qaeda. The sheiks in the al Anbar Province are one of the most notable examples. Even President Bush made note of that during his trip out there. We have also tried to exploit friction between al Qaeda and some of the other movements. Al Qaeda is a coalition just as we are, but the various groups within al Qaeda and the associated movements do not all play from the same sheet of music.

One of the frequent complaints that we have heard from some of the associated movements is that al Qaeda is too indiscriminant in its use of violence—so we played that up. We revealed the way that al Qaeda attacks—indiscriminately killing women and children—and we emphasized that they kill other Muslims. Evidence of our success with that comes from some of the most recent video products from al Qaeda in which bin Laden said that he expected his followers to be more careful in not indiscriminately killing civilians and Muslims in their attacks.

We have also used humor as a weapon to some extent and somewhat effectively by highlighting situations that cause embarrassment and diminish the terrorist mystique. Because terrorists come from a very hierarchical, traditionally male society in which honor and machismo are powerful values and shame and humiliation have strong emotional impact, humor is an important weapon to the extent that we can erode their image of competence by showing them to be comically inept. We have had some limited success with that. Many of you may have seen the video in which we highlighted Musab al Zarqawa's limited ability to correct his own weapons malfunction, revealing that he was not quite the fighter that he would like everybody to think he was—he was wearing American tennis shoes at the time. We highlighted the dichotomy that although he advocated overthrowing the West, he was wearing our products. At the time it was released, the video backfired to some extent because it opened us to the criticism: "If this guy is so incompetent, why haven't you caught him yet?" Fortunately, not too long after that we were able to kill him.

We have also exploited the cowardice of the al Qaeda agents who were captured dressed as women, apparently in the hope that the disguise would protect them from some of our operations. The growing anti-extremist sentiment coming from within the Umma is encouraging. The more we can get Muslims themselves speaking out against violence and extremism, the more progress we will start to see.

CHALLENGES

The following are some areas where we need to do more. Major challenges include aggrandizement of al Qaeda, our aversion to risk, difficulty integrating and synchronizing operations, imperfect assessment methods, limited freedom of movement, and overemphasis on immediate, tactical operations rather than the long fight. I will expand on these challenges and suggest some ways to overcome them.

Over-aggrandizement of al Qaeda

Attributing too much power and influence to disparate groups by lumping them together under the banner of al Qaeda hinders the effectiveness of IO. We tend to group all associated terrorist movements under the large umbrella of al Qaeda, which makes them seem more powerful than they really are. When we do that, we miss opportunities to exploit some of the schisms and differences between them, which are ripe areas for targeting.

Risk Aversion

Most of our risk aversion has to do with IO actions that may have legal, political, or policy implications. Considering the total commitment of the adversaries, it is possible that not taking these risks may be the most risky behavior of all. For example, we are missing an opportunity to deny sanctuary: the place that the terrorists have the most sanctuary is the virtual haven of the Internet. Although we have the tools and techniques to do so, we have done little to attack their ability to operate on the Internet. Because of issues with authorities and intelligence agency interdiction, we have been limited strictly to posting attributed messages on the Internet, at least within DoD—although other agencies may not have those same restrictions. We know that any attributed web site—if it has any Western (especially U.S.) bylines on it at all—is going to be immediately seen as not credible and not believable and will have no relevance at all. We have to be able to operate on the Internet in an unattributed fashion.

Delays in changing policies and procedures also hinder us. We learned years ago that Iraqis do not believe anything unless they see it. Hearing in a press conference or press release that a certain al Qaeda terrorist leader had been captured or killed is not good enough. In their culture, suspicion of rumor is very high. We requested permission to show photos of these detainees to demonstrate that they were now no longer a threat to them. It took well over six months of policy and legal battles to finally be able to demonstrate that. That is a small victory. We were able to get that permission, and it has been effective. However, many other policies are very slow to change.

Another impediment in the risk-aversion category is the reluctance to use a religious or ideological slant. Our adversaries know that, and they use it against us. Therefore, we have to get over the fear of using religion in our messaging.

Finally, we have an overwhelming reluctance to influence an issue that pertains to the distinction between IO and public affairs. The DoD and the U.S. government are comfortable with public affairs kind of messages, but anything that smells of influence is perceived to be dishonest and should not be employed.

Integration and Synchronization Issues

Sharing information across agencies has to include more than just actionable intelligence. We also need to share information with them to coordinate operations, assess outcomes, and develop long-term strategies.

Assessment Challenges

Reliably assessing information operations is also somewhat of a challenge. We have outsourced or contracted a lot of the support to develop influence products for commercials, radio programs, and so forth. One of the challenges is that the companies we have contracted to develop these products for us are the same ones who are running the focus groups that are testing these products. Not surprisingly, they conclude that these are culturally effective. Outside sources should be vetting those products to provide checks and balances.

Because of a lack of standardized and objective metrics, it is difficult to assess efforts to change cognitive beliefs. How do you measure whether someone is less supportive of a terrorist or not? It is a complex problem, and we need some reliable metrics to do that.

Limited Range of Operations

From a DoD perspective—this does not apply to everyone—our freedom of maneuver is largely restricted to Iraq and Afghanistan. Although we have realized that the problem is transregional—the fighters, the money, the weapons, and the ideology are coming from across the region and, in fact, across the globe—our authority to do anything militarily is limited to those two countries. We tend to focus very much on the five-meter target, the current fight, without much consideration of the long fight. If we are going to change values, we have to start now because it is going to take 20 years or so to effect change. We must start thinking about that because, at some point, we all want to go home, and we want to leave that place stable and able to operate on its own.

INFORMATION OPERATIONS AND PUBLIC AFFAIRS

Figure 2 illustrates some further distinctions between IO and Public Affairs. Information operations and public affairs are very closely related, yet distinct. Public affairs operates entirely in the truth and credibility realm; information operations—while contrary to some public conceptions—actually operates most effectively when it is 100% truthful.

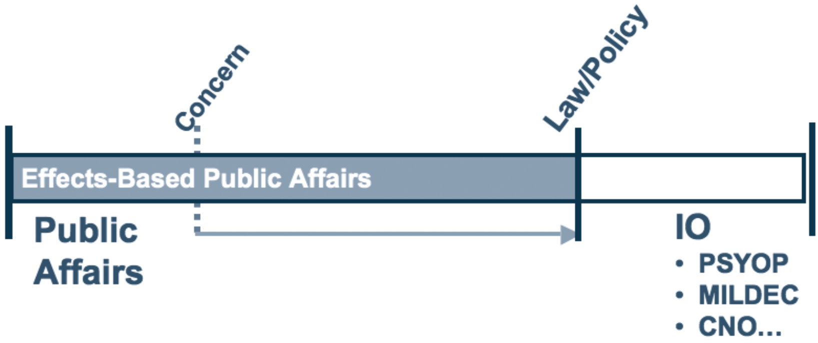


Figure 2 IO and Public Affairs

The deception plan that supported the Normandy operation was successful largely because it played upon pre-existing beliefs and a lot of truth. However, there are very clear limits. Those of us who operate in the information operations world realize that there is a line that we do not cross, and the public affairs folks realize there is a line they do not cross. Problems come in when we have issues that seem to cross those lines.

You may remember that in the fall of 2005, there were accusations that the military was paying for stories to be placed in the Iraqi newspapers—well, there was nothing wrong with this. It was not done by public affairs; it was done by our IO influence people, and it was perfectly legal and legitimate. It was vetted and investigated, and there was nothing wrong. However, because of political perceptions and other concerns, it caused a negative reaction.

Our public affairs people faced further restrictions on the kinds of activities they were allowed to do; the lines within which they were able to operate were pushed back. They were not able to work as closely with Iraqi media and be as aggressive in their operations. Because of that, we ceded a vast amount of the information domain to enemy propaganda for a year or so during which we were running scared because of some of the articles that had come out on this.

Fortunately, MNFI realized the limitations were hindering our effectiveness, so we are moving towards an effects-based public affairs approach in which Public Affairs is integrated with Information Operations while still remaining 100% truthful.

THE WAY AHEAD

Where do we go from here? How do we implement the strategies I have discussed? The following are some recommendations:

- The global insurgency nature of Al Qaeda and Affiliated Movements (AQAM) dictates a solution from within the Umma. This is much more than just putting an Iraqi face on the problem. We need to increase support and facilitation of Muslim-originated anti-jihadist ideals, and it must have a limited U.S. signature to be credible. The current rise in anti-jihadist support from the Islamic world needs to be exploited. The mantra we are hearing is that we cannot simply initiate the action and then let the Iraqis stand up, cut the ribbon, and say it is theirs. It has to come from within. It has to be their words, their ideas, and their style as it goes forward.

- We need to pursue a systems-based approach. It takes a network to defeat a network. This requires greater exchange of liaisons between agencies and organizations to allow us to develop a common operational picture throughout government. The special operations world has a good model for this in working with the intelligence agencies that needs to be exported and used much more widely across DoD and the intelligence agencies.

- Streamlining and decentralizing authorities will allow us to operate on the Internet without attribution and shorten the nonkinetic targeting process. My former commander used to voice concern that it was easier for him to drop bombs than it was to drop leaflets.

- To increase and maintain cultural expertise, we need to leverage academia and other experts, increase formal training, and facilitate the vetting of “cultural experts.” We in the military realize that when we go into a country for a year or so at a time, we are never going to have the depth of cultural knowledge that many of you in academia do. We need to develop closer partnerships and communities of interest to leverage the academic expertise to ensure that we are operating at the right level to attack the ideas of the enemy.

Abu Yahya al-Libi, a senior member of al Qaeda, offered the following suggestions several months ago as six steps that would help us to defeat al Qaeda. He did not do so out of sympathy towards the U.S. but more out of arrogance and a belief that there was no way that the U.S. could ever get its act together to implement these strategies. Yet, if you look at his recommendations, many of them are similar to the recommendations that those of us in the field have made. If we can get some of the legal, bureaucratic, and policy restrictions lifted or expedited, we can be successful with some of these suggestions:

1. Weaken ideological appeal by exploiting disillusioned jihadis.

2. Fabricate stories and exaggerate real jihadist mistakes.

3. Counter the “Jihadist University effect” of detention centers.

4. Amplify mainstream Islamic voices countering AQAM ideology.

5. Silence key ideologues guiding the jihadist movement.

6. Use information operations to fracture the AQAM.

The first two items in the list reiterate the observation that many suicide bombers are recruited, not by the lure of becoming a martyr and dying for Islam but becoming jihadists for a noble cause. When they realize that the al Qaeda recruiters who are trying to draft them are doing so under false pretenses, they may become disillusioned. We can further weaken the ideological appeal by publicizing al Qaeda's deceptions and mistakes. We have a variety of methods to do that, including humor and ridicule.

We have gained much knowledge by studying how detention centers can become training centers, but we must continue to emphasize developing methods to counter that. To augment the mainstream Islamic voices that are speaking out against the radical AQAM ideology, we need to use the resources of the Internet to their fullest extent. The Internet has become AQAM's primary means of communication. We need to be out there as well with credible, persuasive arguments by respected voices for Islam speaking out against AQAM's radical ideas.

For the fifth item in the list—silencing the most radical voices—we need to identify and track the ideologues that are most critical to the movement. Once we identify those high-payoff targets, we can either silence them through kill-capture operations or by making them irrelevant. Finally, IO can focus on exploiting the schisms and continuing to fracture the AQAM by implementing the strategies I have outlined here.

5.6 QUESTIONS AND ANSWERS HIGHLIGHTS

Transcripts

Q: *Is extremist Islamic terrorism a reaction against modernity or against injustice? In other words, if the undemocratic regimes in the Middle East were replaced with liberal democracies, would al Qaeda go away?*

Dr. Paul Davis – I think there is a general truth—which a report that RAND is publishing in a few months will emphasize—that almost any of these questions depend on multiple factors. So the answer is, "it depends." On the one hand, this may sound trivial, but on the other hand, it is profound because many people are looking for single measures or single causes. That leads to disappointment.

For instance, if you ask the question in terms of whether liberal democracies will replace al Qaeda, the relationship between democracy and other good behavior is not all that evident or probably empirical. It is not because democracy is not good; it is because there are other factors at work, such as the economy, the nature of the democracy that tries to take root, and many other considerations that come into play. So I think the disappointing answer is, you cannot really answer a question like that.

Christine MacNulty – One thing I might add—there does seem to be a huge amount of resentment towards the West, but this is not a new thing. In fact, Arab commentators wrote about it in the middle of the 19th Century. They wondered how on earth barbaric Christians could have invented something as awful and powerful as a cannon. They saw the Islamic world as having had a golden age that the West helped destroy. Whether that was true or not is open to some question, but that is the perception.

What we have to realize is that in this whole business of deterring and influencing, we are dealing with perception, not with fact. I do believe that the notion of resentment towards the West—resentment that we are as good militarily as we are economically, —is quite a powerful factor. Nevertheless, I would certainly agree with Paul that whenever we are looking at specific instances, we have to think about the context of those instances and the particular countries and cultures.

Q: It seems to me that Ms. MacNulty's diagrams could be taken equally as advice for how al Qaeda should recruit, which raises the question of what we do to inhibit the success of the adversary in being able to appeal to the population as distinct from our own positive appeal efforts.

Ms. Christine MacNulty – You are absolutely right. If al Qaeda were to look at these charts, they could use them in exactly the same way. So then the question is: what can we offer that al Qaeda can't? From the chart that I showed of Paddy's particular values, we can see that he wants excitement, wealth, and visible success, and he is not too concerned about his fellow man. He does not really like The Other, whatever The Other is. If we were trying to influence Paddy, we would say that we will give him the excitement, the wealth, and the visible success he needs but by using his own definitions of what those are.

Offering him a job in a manufacturing plant is probably not something he needs. He might very well want a job in a high-tech company because, after all, many people recruited by al Qaeda and other terrorist organizations are well educated but unemployed. If we can actually find ways of persuading people like Paddy through offering them things that appeal to those kinds of values, then we will stand a better chance than al Qaeda because, ultimately, al Qaeda can give them excitement but not wealth. It might give them a bit of visible success, but it is probably short-term visible success. Therefore, we have to think about how we can offer what Paddy wants in terms of his own values. What can we do diplomatically, informationally, and economically as well as militarily? We need to think more broadly about how we can influence or deter.

Q: *How do you use IO to fracture AQAM? How about an Arabic docudrama about the plight of a victimized suicide bomber?*

COL Karen Lloyd – I cannot go into many of the specific techniques that we would use to fracture AQAM. Understanding the potential differences between how these movements think is key. Al Qaeda is more global, but many of the associated movements are national. They are focused on regional and national gains. They want power for their country or their province. If we can show them—and we have tried to show them—that al Qaeda is just using them for their resources, access, and expertise about their part of the world to gain global power for al Qaeda, that group will no longer have any influence. Then that might realize it is not in their own self-interest to cooperate with al Qaeda.

If we can highlight some areas of religious disagreement—and we have done that fairly successfully—we can help fracture the movement. As I mentioned, probably the most successful discrepancy we have shown is al Qaeda's indiscriminant violence, especially against Muslims. Many of the other associated movements are much less willing to target indiscriminately, especially when it means killing other Muslims. Those are the kinds of messages that we have attempted to insert into the dialogue in various places and at various levels to further create those rifts.

Q: *Can Mr. Gibson please explain the nexus between what you described as Iraq task force advisors and the Army's Human Terrain Teams and systems? As Colonel Lloyd pointed out, synchronization and integration are important. The Army has been engaged in this for the past year. Is there a nexus between what your project is doing and what the Army is doing?*

Mr. Bruce Gibson – There is a nexus, but it is early in the life cycle. The Information Operations Advisory Task Force (IOATF) has been in existence since late FY 2003. The Army's first Human Terrain Teams (HTTs) are in place now and are growing in number. There is a synergy—with a bit of an overlap—between the two, with the distinction that the IOATF brings in a lot of the micro data, which are assessed, analyzed, and fused for use by the commanders. The Army's HTTs include cultural anthropologists embedded in deployed Brigade Combat Teams (BCTs) to provide insight into the local populations and tribal networks. They provide cultural advice based on a constantly updated, automated database on the BCT area of operations, and they can perform focused cultural studies for a particular commander's area while tapping academic resources.

The value of the HTT is that it contributes the upper-level analysis and evaluation of the data that IOATF provides. The HTT recognizes and interprets the value in the information from the word on the street. The way that the system is currently structured, two pieces of that machine bring the data in: sourcing-type organizations and programs that bring raw data in from the street.

How do you synthesize the data? How do you analyze them? How do you make them relevant to the daily operations of the local commander? The HTT contributes a lot of the brainpower to make that happen. In that sense, the HTT program is not standalone. As these programs evolve, they will become more integrated into the IO campaigns and the strategic communication campaigns so they operate synergistically as one unified system. As the information comes in, it orients the message; the message goes out, and there is a mechanism to measure results so that it can reorient the follow-on discussion. In that way, IO becomes more than just an information blast, it becomes an ongoing dialogue.