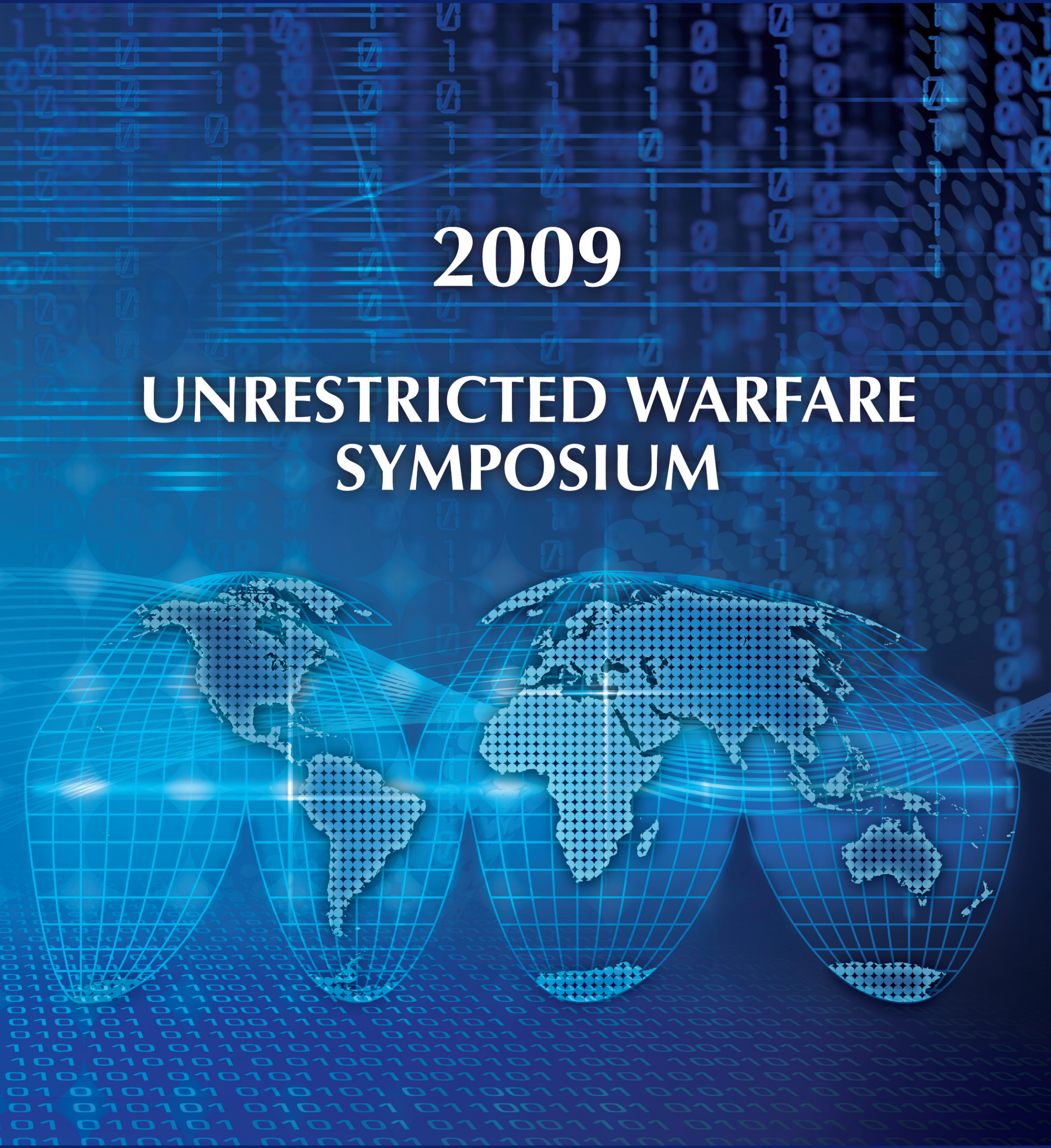
Proceedings on Interagency Action for Attacks Involving:
Terrorism • Resources • Economics • Cyberspace



2009

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 2009

Proceedings on Combating the Unrestricted Warfare Threat:

Terrorism, Resources, Economics, and Cyberspace

24-25 March 2009

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 Heather Pontius Daniel Portwood Ellen Wilkinson
Art Directors:	Brenda Waltermeyer George Travez
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/

Copyright © 2009

By The Johns Hopkins University Applied Physics Laboratory

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

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

Dr. Ronald R. Luman,
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

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

Chapter 1
Featured Papers

1.1 Keynote Address
James Locher 11
1.2 Cybersecurity: Attacks on the Critical Infrastructure
Dan Wolf 37
1.3 Resource Attacks
Michael Klare 61
1.4 Economics and Financial Attacks
James Rickards 77
1.5 Resiliency in the Face of Unrestricted Warfare Attacks
Stephen Flynn 119
1.6 Al Qaeda's Interagency
Bruce Hoffman 147
1.7 Analysis Support for the Interagency
Eric Coulter 167
1.8 Intelligence Support for the Interagency
Karen Monaghan 193

Chapter 2
Responding to Cyber Attacks

2.1 Moderator's Summary
Thomas McNamara, Jr. 205
2.2 Strategic and Operational Responses
Robert Gourley 215
2.3 Cyber Resilience for Mission Assurance
Anthony Bargar 221
2.4 Questions and Answers Highlights
Transcripts 225

Chapter 3
Responding to Resource Attacks

3.1 Moderator's Summary
Lesa McComas 247

3.2 Responding to Resource Attacks: Protecting Critical Infrastructure
Celina Realuyo 253

3.3 Questions and Answers Highlights
Transcripts 263

CHAPTER 4
RESPONDING TO ECONOMICS AND FINANCIAL ATTACKS

4.1 Moderator's Summary
Ted Smyth..... 275

4.2 Overarching Economic Threat
Pieter Bottelier 279

4.3 Responding to Economic and Financial Attacks
Richard Cooper 287

4.4 Putting Economics Back at the Center of National Strategy Attacks
William Overholt..... 299

4.5 Questions and Answers Highlights
Transcripts 311

CHAPTER 5
RESPONDING TO NUCLEAR TERRORISM

5.1 Moderator's Summary
Todd Masse 317

5.2 The Impact of Cataclysmic Events
Brian Jenkins..... 329

5.3 Sharing Science and Technology Within the Interagency
Jonathan Medalia..... 343

5.4 Creating An Interagency "Critical Mass" for U.S. WMD Terrorism Analysis
J. Scott Cameron 353

5.5 The Elements of Response
Harvey Johnson, Jr. 361

5.6 Questions and Answers Highlights
Transcripts 375

Chapter 6

Analysis Support

6.1 Moderator’s Summary
John Benedict 379
6.2 Threat Finance and Counterradicalization
Matthew Levitt 387
6.3 Analysis of Interagency Activities and Complex Operations
Andrew Caldwell 403
6.4 Analysis Support for Unrestricted Warfare
George Akst 417
6.5 Questions and Answers Highlights
Transcripts 425

Chapter 7

Senior Perspectives

7.1 G. Peter Nanos 435
7.2 Bernd McConnell 441
7.3 Vahid Majidi 447
7.4 Questions and Answers Highlights
Transcripts 455

Afterthoughts

Thomas Keaney 471

Appendix A

Symposium Agenda 475

Appendix B

Acronyms and Abbreviations 481

Foreword

Welcome and Perspective on Unrestricted Warfare

FOREWORD – WELCOME AND PERSPECTIVE ON UNRESTRICTED WARFARE

Ronald R. Luman

INTRODUCTION

In these proceedings of the Unrestricted Warfare Symposium, our collective objective is to share ideas, insights, and lessons learned and to identify strategic strengths, weaknesses, opportunities, and threats to interagency collaboration. In addition, we will look for gaps in agency responsibility and identify solutions to mitigate weaknesses and seize opportunities for positive change and collaboration in strategy, technology, and analysis. Our nation and our allies are facing unique challenges from both state and nonstate actors in what we have come to know as the long war, where irregular methods of warfare are expected and conventional approaches are obsolete.

In 2006, I initiated this symposium to develop an integrated community and document a body of knowledge on unrestricted warfare because I am committed to the sharing of information with an effective, integrated community of strategists, analysts,

Dr. Ronald R. Luman is Head of the National Security Analysis Department at The Johns Hopkins University Applied Physics Laboratory. Dr. Luman has expertise in applying systems engineering principles to guidance system accuracy, unmanned undersea vehicles, countermine warfare, ballistic missile defense, and intelligence systems. He was Chief Analyst for the Joint Countermine Advanced Concept Technology Demonstration. He leads a cross-enterprise activity at The Johns Hopkins University Applied Physics Laboratory to understand future conflict and build appropriate technical capabilities to counter unconventional warfare. Dr. Luman earned his doctorate in Operations Research from the George Washington University, received his master's degrees from Michigan State and Johns Hopkins University, and is a 1976 graduate of Middlebury College.

and technologists dedicated to meeting critical challenges with critical contributions.

This year, as in previous years, we are fortunate to be able to learn from and interact with innovative and proactive leaders in government, defense, and industry. A distinguished group of speakers and expert panelists will present their unique insights and extensive experiences in forging interagency partnerships and collaboration to meet the unconventional demands of unrestricted warfare.

I would like to take a few minutes to reflect on the theme of this fourth annual symposium, beginning with a brief overview of the nature of unrestricted warfare and a clarification of what it does, and does not, encompass. Unrestricted warfare spans three of the four quadrants of the DoD warfare environment (Figure 1). The chief characteristic of unrestricted warfare is unrestricted use of measures, not unrestricted strategies or objectives. Surprise and deception are often involved, as are integrated attacks, to exploit more than one vulnerability of a conventionally stronger opponent.

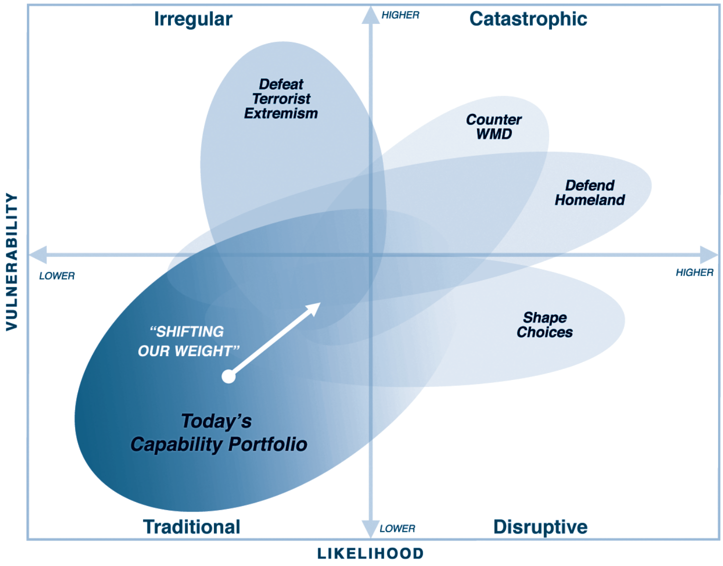


Figure 1 DoD Warfare Environment

The unrestricted warefare battlefield includes new, unexpected domains such as infrastructure, natural resources, financial and economic markets, and chemical, biological, and nuclear threats, all of which represent unprecedented challenges to government, DoD, and industry. These proceedings will discuss the critical challenges we face and the interagency imperatives that they impose.

Small units of organized adversaries, rather than large military forces, characterize unrestricted warfare. These units are cell structured and integrated within their society. Technology and instant access to global broadcast media have provided a means to disseminate propaganda and project an image to a connected global audience. The dynamic alliances between state and nonstate actors, their means of finance, and the intricate relationships between them are difficult to trace—enabling the few to impact the many. These groups engage in tactical engagements that have immediate strategic impact on the U.S. and our allies.

We call this kind of conflict unrestricted warfare because the enemy takes actions that cause shock and fear, offend us, and generate disbelief in the American mind even now. New areas are under attack, forcing government, industry, and military organizations to arm themselves in new and challenging areas. Consider, for example, the conflict that began on 8 August 2008 when Russian troops crossed into South Ossetia, vowing to defend their "Russian compatriots." As this was taking place, a multi-faceted cyber attack was launched against the Georgian infrastructure and key government web sites. The attack modalities included: web site defacement, web-based psychological operations, a fierce propaganda campaign, and a distributed denial of service attack in a community where virtually every financial or business transaction takes place on-line.

Attacks in Asia in 2009 violated our cultural sensibilities and norms when adolescent boys detonated suicide bombs stowed in back-packs, in a resort hotel lobby, killing innocent civilians on holiday. There is a ready supply of young, fervent, technologically savvy jihadists to further insurgent objectives, promote fear, and perpetrate terrorist acts in the pursuit of their objectives, including al Qaeda's public vows to obtain and use nuclear weapons and to bleed America to the point of bankruptcy.

Americans and our allies are still surprised that the enemy uses techniques that we do not understand or expect, and though acts of terrorism will, I believe, always offend our sense of justice, we need to predict where and how this enemy will strike next. We must be prepared both at home and abroad to meet the unknown challenges of unrestricted warfare. Consequently, the objective of this symposium is to pull together a community to develop new approaches to unrestricted warfare and maximize the collaboration of interagency teams to improve the effectiveness of our strategic planning and response to threats.

In our first symposium, in 2006, we focused on defining aspects of the unrestricted warfare challenge. The second year, we aimed at developing solution approaches. In 2008, we focused on the Global War on Terror campaign concept (Figure 2). So what ideas have we germinated to date? I am impressed, but not surprised, at the volume of data and the value added of sharing knowledge and expertise across disciplines and organizations. In four years, we have discovered that we need to employ nonkinetic approaches for combating new threats and that deterrence, dissuasion, and conflict have to be tailored to the threat. The human element demands that we broaden our perspective and are sensitive to our projected international image and brand. We understand that different parties value different issues and that the analysis community faces significant challenges in terms of defining metrics, developing models, and collecting data of use in modern warfare. We have seen a re-emergence of competitive games and war gaming, but we must approach these with structure so that results are repeatable and we can validate new models on which games and simulations are built. We have learned that technology development must be agile enough to protect our warfighters, as well as our networks and information.

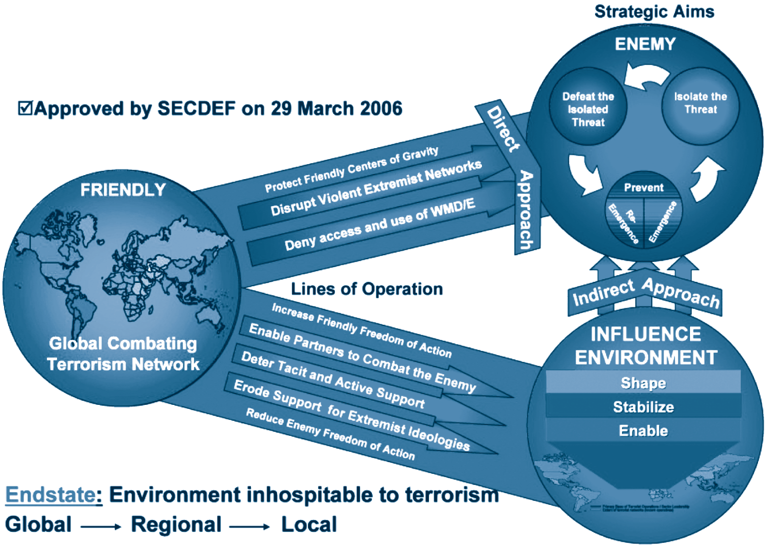

Strategic Aims
ENEMY
Defeat the Isolated Threat
Isolate the Threat
Prevent
Re-Emergence
Emergence
☑Approved by SECDEF on 29 March 2006
Direct Approach
FRIENDLY
Global Combating Terrorism Network
Protect Friendly Centers of Gravity
Disrupt Violent Extremist Networks
Deny access and use of WMD/E
Lines of Operation
Increase Friendly Freedom of Action
Enable Partners to Combat the Enemy
Deter Tacit and Active Support
Erode Support for Extremist Ideologies
Reduce Enemy Freedom of Action
Indirect Approach
INFLUENCE ENVIRONMENT
Shape
Stabilize
Enable
Endstate: Environment inhospitable to terrorism
Global ⟶ Regional ⟶ Local

Figure 2 Global War on Terror Campaign Concept

Each year, as I finalize my summary of insights from all of the dynamic discussions, a new, more complex series of challenging questions arise or are revealed in the thoughtful questions posed by participants in session or by blog. I am inspired that the symposium participants have so enthusiastically responded to my call to action: to interact, share perspectives, and collaborate to illuminate future areas of study.

The compelling question that arose throughout last year's symposium was how do we inform leaders in strategy, analysis, and technology of the interagency imperatives that will provide a road map and planning alternatives to succeed in current threats and the future of the long war (Figure 3). Hence, our objectives for the 2009 Unrestricted Warfare Symposium are to:

- Understand challenges of working across agencies and explore suggestions for constructive change
- Focus on unrestricted warfare lines of attack that mandate interagency collaboration to address:
  - Cyber warfare

  - Resource warfare
  - Economic/financial warfare
  - Nuclear terrorism
- Dive deep into critical concepts:
  - Interagency analytic advances
  - National resiliency
  - Intelligence estimates
- Provide senior panel experts to address current and future collaborative interagency efforts.

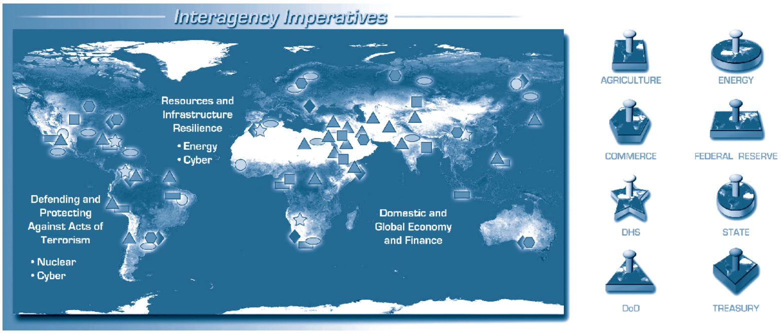

Interagency Imperatives
Resources and Infrastructure Resilience
• Energy
• Cyber
Defending and Protecting Against Acts of Terrorism
• Nuclear
• Cyber
Domestic and Global Economy and Finance
AGRICULTURE
ENERGY
COMMERCE
FEDERAL RESERVE
DHS
STATE
DoD
TREASURY

Figure 3 Strategic Collaboration for Interagency Imperatives

Why is working together so important? Each of the communities needs something from the others (Figure 4). Strategists need to understand the risks and benefits of alternative courses of action based on analysis conducted with rigorously developed and valid models. They also need to understand the potential effects of technology on the information and the physical domains. Analysts need to understand the measures of success. How do we know what, in a strategic sense, is valued in the geopolitical domain with regard to cyber, resource, and economic attacks? Analysts also need to know where they will collect appropriate data and how to apply that data to new, innovative analysis perspectives. Technologists need to understand what strategists want to do across a full range of warfare using all elements of national power. Technologists also need to understand, in context, the value of their particular technological approach. An integrated community will enable us to develop tailored interagency responses and courses of action, prioritize objectives, measure outcomes, and guide those of us working toward critical contributions to resolve unrestricted warfare challenges.

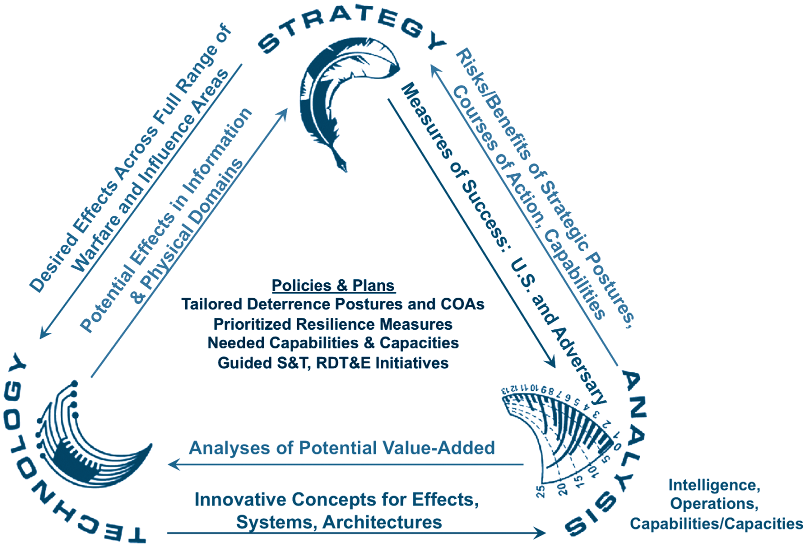

STRATEGY
TECHNOLOGY
ANALYSIS
Desired Effects Across Full Range of Warfare and Influence Areas
Potential Effects in Information & Physical Domains
Risks/Benefits of Strategic Postures, Courses of Action, Capabilities
Measures of Success: U.S. and Adversary
Policies & Plans
Tailored Deterrence Postures and COAs
Prioritized Resilience Measures
Needed Capabilities & Capacities
Guided S&T, RDT&E Initiatives
Analyses of Potential Value-Added
Innovative Concepts for Effects, Systems, Architectures
Intelligence, Operations, Capabilities/Capacities

Figure 4 What We Need From Each Other

I am honored to host this symposium with a stellar group of featured speakers and distinguished panel experts to interact with what has evolved as a collaborative community of analysts, strategists, and technology experts in the unrestricted warfare arena.

Our Keynote Speaker, the Honorable James R. Locher, III has more than 25 years of professional experience in both the executive and legislative branches of the federal government. He is currently the Lead Instructor for the Department of State's Combating Terrorism Program for senior foreign leaders, Staff Adjunct at the Institute for Defense Analyses, Executive Director of the Project on National Security Reform, and author of *Victory of the Potomac: The Goldwater-Nichols Act Unifies the Pentagon*. He will provide his unique perspective on imperatives for interagency actions and also a road map to future administrations on national security reform. He is joined by Mr. Eric Coulter, of the Office of the Secretary of Defense Program Analysis and Evaluation, who will offer insights as to how unrestricted warfare creates imperatives for analytic approaches that integrate diverse interagency analytical capabilities.

In addition, Dr. Stephen Flynn, from the Council on Foreign Relations, will apply the principle of resiliency across the federal and private industry sectors. I welcome Professor Bruce Hoffman of Georgetown University, who will provide a riveting update on terrorism trends and future directions.

Relevant and intriguing economic and financial insights come from Mr. James Rickards, of Omnis, Inc., who will address the potential of financial and economic attacks in the context of a global economy, and Professor Michael Klare, author of *Resource Wars,* who will provide insight on resource and infrastructure threats. Mr. Dan Wolf, former Director of the Information Assurance Directorate at the National Security Agency outlines actual and potential threats to information systems, networks, and the computers that have become integral to our lives and our intelligence collection. Ms. Karen Monaghan, of the National Intelligence Council, will provide a critical intelligence perspective. Again, we have invited a panel of senior leaders to provide their unique perspectives and a synergistic approach to summarizing key policy and strategy issues that arise from panel discussions and audience questions.

Chapter 1

Featured Papers

1.1 KEYNOTE ADDRESS

James Locher

THE HONORABLE JAMES LOCHER'S KEYNOTE ADDRESS

This Unrestricted Warfare Symposium provides the opportunity to exchange ideas on how to collaborate more effectively across the government. Ron Luman has identified four areas where we need to be able to work horizontally across our government departments and agencies. We can think of dozens of areas where we need the ability to work in effective, horizontal teams, but we do not have that capacity today.

The U.S. national security system employs many talented experts. Our national security professionals are working incredibly hard and with unsurpassed dedication. However, our organizational deficiencies are wasting much of that talent and hard work. This symposium gives us the chance to discuss progress, but we need to make some fundamental reforms.

The Honorable James R. Locher, III has more than 25 years of professional experience in the executive and legislative branches of the federal government. He is currently the Lead Instructor for the Department of State's Combating Terrorism Program, Staff Adjunct at the Institute for Defense Analyses, and Executive Director of the Project on National Security Reform. Upon leaving government service in June 1993, he was awarded the DoD Medal for Distinguished Public Service, the department's highest civilian award. Mr. Locher graduated from the U.S. Military Academy in 1968, received an MBA from the Harvard Graduate School of Business Administration in 1974, and was awarded an honorary Doctor of Laws degree from Hampden-Sydney College in 1992.

National security reform is the number one national security issue. You might be thinking, "How in the world can he say that? Hasn't he heard of Afghanistan, Iraq, North Korea, Iran, or combating terrorism and counterproliferation?" National security reform is the number one national security issue because our organizational dysfunction undermines our ability to perform in these other specific mission areas. We are crippled in many respects in terms of our performance:

- We do not have the ability to collaborate across the government, so we cannot produce a unified effort.
- We, in many respects, do not plan. We clearly do not practice integrated planning across the government, so we do not have unity of purpose.
- We have inadequate training for our people to perform these complex missions, and almost everything is done on an ad hoc basis, whether within organizations or processes.

"National security reform is the number one national security issue because our organizational dysfunction undermines our ability to perform."

This year, I think there is a great opportunity to make progress in the area of national security reform. My project, the Project on National Security Reform, has invested much time and talent working the intellectual side of what is wrong with our system and what needs to be done. George Bernard Shaw said, "Reformers have the idea that change can be achieved by brute sanity." We are going to bring a lot of brute sanity to this particular subject, but we also understand that there is a vastly important political dimension.

The attendees of this symposium are very committed to the idea of improving our interagency capabilities. I am here not only to inform you but also to recruit you. These changes have to take place. If you did not like the performance of our national security system in the last seven or eight years, then you are not going to like what is coming in the future if we do not change. The problems that we have recently experienced are evidence of our organizational dysfunction. Unless we solve it, we are going to continue to have many setbacks.

BACKGROUND

The Project on National Security Reform is an independent, non-profit, non-partisan organization working on solutions to interagency dysfunction. We are a private-public partnership consisting of a coalition of think tanks, universities, businesses, consulting and law firms, and government personnel, including 13 working groups and a large network of over 300 participants. Our 2008 report, *Forging a New Shield* [1], was mandated and funded in part by Congress, but an equal amount of funding was provided from private sources. Our funding for Fiscal Year (FY) 2009 is governed by a cooperative agreement with the DoD and the Office of the Director of National Intelligence (ODNI).

As background to the subject of national security reform and the interagency process, we need to start with the National Security Act of 1947, which focused on military unification. It gave almost no attention to the National Security Council (NSC) and surrounded a battle over creation of what eventually became the DoD in 1949. The Navy and the Marine Corps offered the idea of a NSC as a scheme to prevent the creation of a DoD. There was no consideration of this idea on Capitol Hill, and before President Truman had offered this up as a bone, he had stripped the NSC of all its planned authority. The entire burden of integrating across our government was placed upon the President's shoulders.

The NSC then had the World War II concept of national security, focused on diplomacy, military, and intelligence. Since the Kennedy Administration, it has focused on policy. This policy focus is a problem because there is an end-to-end process of policy, strategy, planning, execution, and assessment. We cannot do the policy part well while the rest of the process ends up clogging in departmental stovepipes.

We bifurcated national security in 2001 when we created the Homeland Security Council (HSC), which had some utility at the time but created a lot of organizational challenges. The magnitude of recent setbacks (e.g., 9/11, Iraq, Afghanistan, Hurricane Katrina) has produced an emerging consensus that we urgently need to reform the national security system.

What is the major impetus for reforming the national security system? The primary problem is that the interagency is misaligned with the challenges—and the opportunities—of the 21st Century. We cannot handle complex, rapidly-paced threats and challenges. We are still dominated by our departments and agencies, which are outmoded, bureaucratic, stovepiped, rigid, and highly competitive. We need the ability to work horizontally across our government, but we currently have a vertical government. We do not have the kind of horizontal teams that can integrate all of the expertise and capabilities of our government on a timely basis. Newt Gingrich, who is a member of the guiding coalition of the Project on National Security Reform, said, "We have met the enemy—and it's our bureaucracy" [2]. I absolutely agree.

". . . the gap between the demands that are being placed upon the system and the ability and speed of the system to respond is widening. The world is changing faster than our ability to address it."

We have had many catastrophic setbacks in our ability to formulate, plan, and execute policy. There has been a lot of compelling evidence in recent years that the system is not working: the terrorist attacks of 9/11, the troubled stability operations in Iraq and Afghanistan, and the poor response to Hurricane Katrina. These setbacks are not coincidental. They are evidence of a system failure, but the problems have been long-standing. They actually have origins in the National Security Act of 1947, which was not adequate for what the nation needed at the time, and that inadequacy has grown as the world has gotten more complex. The need for multi-agency work has increased, as has the speed at which we need to operate. There have been efforts to focus on the problems in the system, but we really have not come up with the fundamental solutions that are required.

As I mentioned earlier, two things have magnified the problems in the system. One is the complexity and the other is the speed of change. We are not able to deal with either. One of the frightening conclusions that emerged from the Project on National Security Reform is that the gap between the demands that are being placed upon the system and the ability and speed of the system to respond is widening. The world is changing faster than our ability to address it.

WHY IS THIS THE BEST TIME FOR NATIONAL SECURITY REFORM?

Why institute national security reform now, and why am I so optimistic about this particular period of time? In the Project on National Security Reform, we have been studying this issue for two years. In early December 2008, we released an 800-pg report, *Forging a New Shield* [1]. Many people from our project have gone into key positions in the Administration. Right at the top, the Vice President, Mr. Joseph Biden, is a big supporter of national security reform and has talked of the need for a new National Security Act. When he was Chairman of the Senate Foreign Relations Committee (SFRC), he held hearings on this subject. He had an advisory group on national security reform, of which I was a member. He is a big believer.

"The stars are aligned to make progress in this area, this particular year."

National Security Advisor General James L. Jones was a member of the Project on National Security Reform. Secretary of State Hillary Clinton was going to lead national security reform for the Project in the Senate. As a member of the Joint Forces Command Transformation Advisory Group, she became quite knowledgeable about the interagency problems and is a big supporter of reform ideas. We have always had the support of Secretary of Defense Robert M. Gates and Admiral Michael G. Mullen. Admiral Dennis C. Blair, the Director of National Intelligence, was my deputy in the Project on National Security Reform; he is also deeply grounded in the issues. James B. Steinberg, the Deputy Secretary of State, was part of our guiding coalition, as was Ms. Michèle Flournoy, the Undersecretary of Defense for Policy. We have been working with a wide range of members of Congress. The stars are aligned to make progress in this area, this particular year.

GOALS AND PHASES

The goal of the Project on National Security Reform is the approval of a new system early in the Obama Administration. We see national security reform as having two phases. The first phase, currently underway, focuses on how we are going to operate in the interagency space between the departments and the President. That space is going to be populated by many more organizations in the future, and it is where the most difficult multi-agency work will have to be done in the future.

The second phase focuses on discovering how the departments and agencies need to be reformed to align them with how the government as a whole is going to operate in the field of national security. Therefore, national security reform is probably a 10-year undertaking. Even if we were able to get the interagency reforms approved this year, it would take us 10 years to fully implement them and a lot of attention to make certain that we implement them wisely. Then there are the reforms that are required within each department and agency.

PROPOSED REFORMS

We have three sets of reforms in mind. First are the reforms that can be achieved under existing authority, new executive orders, and Presidential directives. One proposal that the Obama Administration is considering is merging the NSC and the HSC, which can be done under existing law. There is a provision in the HSC statutes that gives the President authority to operate with only one council.

The second set of reforms is on Capitol Hill. National security reform will be imperfect without fixing Congress. Congress never had its own National Security Act of 1947, so it is even more stovepiped than the Executive Branch. One idea that we have been promoting is to create an interagency team on Capitol Hill, which we call the Select Committee on National Security.

Third, we have a new National Security Act in mind. The Executive Branch does not have all the authority it needs to be effective in the 21st Century, so there are some changes that need to be made in statute.

OVERARCHING PROBLEMS

Although the national security system has dozens of organizational problems, I will present five that have been the focus of our work. The first is that our system is grossly imbalanced. We have very powerful departments and agencies that have all of the resources. They are tied in with their congressional patrons. The integrating mechanisms are the NSC and the HSC system which are incredibly weak because they only have advisory responsibilities and are much too small. Two hundred people in the NSC staff have a budget of $8.6 million. The NSC staff has a personnel system from the 1930s, an organization from the 1940s, a management doctrine from the 1950s, and processes from the 1960s and is supported by technology from the 1970s. The very top of all our government is stunningly broken and small. All of the burdens are on the President's shoulders at a time in which the challenges and threats require an extraordinarily greater degree of integration, but the integrating mechanisms are extremely weak. That is the number one problem.

The second problem is that the components of national security are not managed as a system. One of the proposed responsibilities of the Executive Office of the President is to manage this whole system. What is the strategic guidance? What are the macro-resource allocation tradeoffs that need to be made? What is our organizational strategy? How are we going to manage the human capital dimensions? How are we going to assess the performance from a system-wide perspective, not from a departmental perspective? All of these system-wide management tasks are currently not performed, which denies us an important set of contributions.

". . . there is no strategic guidance from the President. The strategy documents that are issued are not truly strategy documents; they are statements of goals."

For example, there is no strategic guidance from the President. The strategy documents that are issued are not truly strategy documents; they are statements of goals. Often, because we have so many strategy documents, we have not been able to resolve the conflicts amongst them. They do not drive anything in the departments and agencies. No one is picking up the national security strategy and understanding what they should be doing. This lack of strategic guidance from the President denies us unity of purpose. In the absence of that strategic guidance, each department and agency figures out, to the best of its ability, its own way forward.

Because the system does not work well, we are doing a lot of things down in the stovepipes. The White House often finds that if it wants the national perspective to be applied, it has to be handled in the Executive Office of the President. The Executive Office then becomes seriously overburdened and can become a bottleneck because it can only handle a few issues. Centralized issue management is not really a strength. However, because of the system's inabilities, we see that tendency for issues to be brought back to the NSC to address.

Our resources are not aligned with strategic objectives. We still put the President's budget together on an input basis, as well as what the departments and agencies would like to do, but it is not aligned with what the President thinks are the strategic objectives and the missions he would like to accomplish.

The fifth overarching problem originates in Congress, which is focused on the parts. It cannot provide a whole-of-government approach; consequently, it has a tendency to reinforce the divisions in the Executive Branch. If you collaborate in the Executive

Branch, you are certain to be punished when you get to Capitol Hill. Congress has to make some fundamental changes.

In addition to these overarching problems, we face a number of other problems, including the following:

- **No effective means for delegating the President's authority**: Today, under law, the entire responsibility for integrating across departments and agencies is on the President's shoulders. Two techniques have been used to delegate his authority.
    - One approach is to appoint a lead agency. As it turns out, no self-respecting department is going to follow another department on a particular issue, especially if there are departmental prerogatives involved. Therefore, the lead agency often ends up being the lone agency. One department tries to push the issues but does not have an interagency team supporting it.
    - The second approach is the czar method; those poor czars, they are even worse off than the lead agencies. At least if you are a lead agency, you have one agency that is following you. When you are a czar, you do not have any agency that is following you; you have all of the people on Capitol Hill, supporting their departments and agencies, who are against you. We have no means right now of effectively delegating the President's authority.
- **No means for effective multi-departmental execution**: Whenever we want to do something, we have to do it ad hoc. The coalition provision authority in Baghdad is a great example of an ad hoc approach for execution.
- **No government-wide strategic planning, and, beyond that, no strategic visioning**: The top of our system is completely consumed by today and tomorrow. In part, this tunnel vision comes from the organizational dysfunction. The people at the top must devote all their energy just to handling today's issues, and to do that, they must work

incredibly hard. People burn out on the NSC staff in less than two years. They are done. They have been worked so hard that we have to put them out to pasture and get somebody else.

- **No interagency culture**: We are dominated by the cultures of the various departments and agencies so unlike the DoD that we do not have a joint culture to help us carry out tasks in the interagency.
- **Lack of trust between the departments and agencies**: This is a huge tax on the system and creates enormous friction.
- **Limited detailed integrated planning**: Because many agencies do not plan, we cannot practice fully integrated planning.
- **Minimal regional interagency planning, coordination, execution, or oversight**: At the regional level, the only entities who are trying to create interagency mechanisms are the combatant commands. They are only a shadow of what is really required.
- **Specialists instead of leaders**: We are a government of specialists; we are not a government of leaders. We have spent much of our time developing technical expertise, advancing by becoming technical experts. During the Cold War, when things were slower moving, we could muddle through with non-leaders in leadership positions. In today's world, we are hugely dependent upon visionary leaders who can mobilize organizations to address the changes that are coming.
- **No interagency human capital plan and poor information sharing**: The government knows a tremendous amount. However, it cannot apply the knowledge. Much of this is a cultural problem and our lack of trust.

RECOMMENDATIONS

In the Project on National Security Reform, we have made 38 recommendations, and they are grouped into several themes.

New Approaches for National Missions

Our number one theme is that we need to adopt new approaches that are focused on national missions and outcomes. We are overly focused on what departments want to achieve. Let us get ourselves up one level from that. What is it that the nation requires? What are those national missions and outcomes? This is going to require a lot more emphasis on integrated effort, collaboration, and agility. We had a tendency in the past to consult Cabinet Secretaries, who are highly competitive. I have spent most of my career watching the Secretary of State and the Secretary of Defense continuously be at war with each other. That era is over.

No department can carry out a single national security mission by itself. In many instances, we need seven or eight major departments working as an effective team. We need people at the top with incredible skills of collaboration. As I mentioned, our current scope of national security is very narrow and needs to broaden out to pick up the economic and energy issues. The environmental issues need to be a part of our consideration of national security. We propose merging the NSC with the HSC and creating a new position in the Executive Office of the President, one we call the Director for National Security.

The titles are not important. We often use titles to indicate that we have created something that is now different from what we had in the past. What we are really trying to achieve is to shift the role from a National Security *Advisor* to a National Security *Manager*. The President needs somebody who can help him make this system decisive, integrated, agile, fast, and focused on the national mission. We believe that General Jones' position needs to shift into being more powerful, being the manager that the system really needs.

Unity of Purpose

Our second major recommendation is to create unity of purpose. The Executive Office of the President, the NSC staff, and the HSC staff really need to focus on high policy, grand strategy, and strategic system management—all of the things they are not doing today. We are proposing a huge shift in the core competencies required at the top of the system to stop the key players from focusing on issue management—which consumes them today—and more on actions directed from the White House and the Executive Office of the President.

". . . there is a strong tradition that the people around the table feel an obligation to defend their departmental perspective."

We have proposed instituting a National Security Review, like the Quadrennial Defense Review (QDR), to be performed every four years at the *national* level. The President would sign an annual National Security Planning Guidance that would go out to all of the departments and agencies that play in the national security system with a clear statement of the President's strategic objectives, missions he would like to see accomplished, and whatever other guidance he would like to provide.

To further unify system management, there should be an official at the NSC: the Executive Secretary. We are proposing that the Executive Secretary be given the responsibility for supporting system management.

If we are going to take the people who are now managing the issues and have them focus at a much higher level, who is going to take over issue management? We propose that we decentralize management of issues and achieve unity of effort through two processes:

- **Shift to interagency teams**: We propose that the President select five to seven priority issues—on which we have not been able to make adequate progress in the current arrangements—and create an interagency team to tackle them.
- **Create interagency crisis task forces**: During crises, we have proposed creating interagency task forces with a unified chain of command, as opposed to the current

multiple chains of command that sometimes work at cross-purposes. It will be a bit of a challenge for us to adjust our thinking about how to implement this. However, as we go forward in our government, we need to have that unity of effort.

INTERAGENCY TEAMS

I will tell you how our proposed redefinition of the role of "interagency team" differs from an interagency team today. Currently, committees dominate our government interagency process. I do not know if any of you have attended meetings at the NSC Principal committee level, or Deputy's committee level, or what we currently call policy coordinating committees, but the people who come from the departments and agencies are there primarily to defend departmental interests. They often are given explicit instructions, when they come from their department and agency, that they are not to yield on the department interests. I have attended hundreds of these meetings at the policy-coordinating level, but I also attended 200 Deputy's committee level meetings, and there is a strong tradition that the people around the table feel an obligation to defend their departmental perspective.

Clearly, they have expertise that is important to bring forward, but what we really need is people who are figuring out how that departmental expertise and their capabilities fit into solving the national problem. We end up brokering among the various departments and agencies with an outcome that has been watered down, may not quite solve the problem, and can be—even when it is agreed to—undermined in its execution through departmental means.

The idea of teams is a concept used extensively in business because business faces the same challenges as the government—it has to deal with complexity and often has to take action rapidly. Businesses recognize that their functional stovepipes do not give them the mechanism that is required to bring all of the expertise of the corporation together, focus on a single problem, and rapidly provide the leadership of the corporation with an integrated perspective. We are proposing interagency teams that take the same approach. They have authority as well as a clear statement of purpose. They are staffed by people who are going to be rewarded for contributing to the team. Right now, the personnel incentives in our system reward those people who defend departmental prerogatives.

"Right now, the personnel incentives in our system reward those people who defend departmental prerogatives."

When I used to attend those meetings, representing DoD, I was given explicit instructions from the DoD. There were three standing rules back in the first Bush Administration: (1) do not tell them anything, (2) do not let them interfere with our operations, and (3) do not let them get their hands on our money. If I did not abide by those rules (which I did not), and somebody found out about it, I would be punished. Therefore, we are looking for mechanisms where we train people to be part of a team. They need to be trained in team dynamics and conflict resolution. They should focus on what it is that the nation requires. Then we need to have formal leaders who have authority to bring efficiency to decision making.

Elements of Interagency Teams

In the leadership role, we are proposing that the President designate a senior National Security Executive, perhaps a former undersecretary. The presidential envoys are the National Security Executives that we had in mind (e.g., those who had been selected such as Special Envoy Senator George Mitchell and Air Force Major General J. Scott Gration, who was just named as a Special Envoy for the Sudan).

The leader would be able to create a small, select team with only the skills needed to contribute to the team's mission. The team would perform its mission under a charter developed by the National Security Advisor and team leader and approved by the President. We would like teams to be suspended once they have completed their mission.

The teams will have to go through intensive training. Even in the business world, much training is needed to prepare people to transition from being elements of functional stovepipes to team members focused on a corporate mission.

The essential element is a charter, signed by the President, that would include a precise statement of the team's mission, clear objectives, and authority of the team to direct action, control resources, and other key aspects of its mandate. The new Administration has shown interest in this concept.

Linking Resources to Goals

The next major recommendation theme focuses on how to link resources to goals. We are proposing that all national security departments and agencies have six-year budget projections based on National Security Planning Guidance and that there be a joint President's Security Council. We have renamed the merged NSC and HSC as the President's Security Council, signifying that it is something different from what we have had in the past. In the end, it will probably still be called the NSC, but we think the NSC will drive those joint reviews with the Office of Management and Budget (OMB) so that we focus on what it is we are trying to achieve and make certain that the resources are moving in that direction.

"We have a huge problem with the flow of information and knowledge."

We have also proposed production of an integrated national security budget, which would be shown to Congress. This gives us the opportunity to make those tradeoffs across budget categories.

The next thing we need is to align our personnel incentives with strategic objectives. We think there should be a human capital strategic plan to create a National Security Professional Corps, like the Joint specialty officers in the DoD, full of people who have decided they want to specialize in interagency tasks. They will go back for multiple assignments. We will make certain that their education prepares them for that work.

Then, we will establish an interagency personnel system. We will use promotion incentives. You may not be promoted to a senior level in any department or agency until you have successfully completed an interagency assignment or an assignment in a different department or agency. We will also require that, before you go to particular jobs, you will have to undergo certain education and training. For example, people who are going off to embassy staffs are referred to as country teams. They are not country teams; they are feuding fiefdoms. All of the problems of Washington go out to the embassies. We propose that no one relocate to an embassy staff who has not been through some sort of team training. We will have education requirements much like the Joint officer management system that was imposed in the Goldwater-Nichols DoD Reorganization Act of 1986.

"They are not country teams; they are feuding fiefdoms."

We have a huge problem with the flow of information and knowledge. We are proposing that, at the NSC, we have a Chief Knowledge Officer. We will have a single security classification and access regime to consolidate security clearance and approval procedures. Each one of these organizations has their own classification system and clearance procedures. However, if we are going to manage this as a national security system, we will have to break down a lot of these barriers. Establishing a consolidated security clearance system will require substantial work but is essential.

With respect to Congress and creating select committees on national security, our idea is to have those committee members be the chairmen and ranking members of the committees with national security jurisdiction or their designees. They would be people who would bring that committee perspective. Again, they would have to be trained on looking at whole-of-government and how this all fits together. We think this would be hugely beneficial on Capitol Hill, and it would give the national security community in the Executive Branch somebody to talk to in Congress.

We need much more flexibility from Congress on funding matters concerning contingency funds, transfers of money between departments and agencies, and reprogramming. The two foreign policy committees on Capitol Hill—the SRFC and the House Foreign Affairs Committee (HFAC)—are broken, and we need to make certain that we really have a good voice from them on Capitol Hill; they need to be empowered to formulate and enact annual authorization bills. It goes back to the inadequacy of the soft power part of our work.

OBAMA ADMINISTRATION'S REFORM INTENTIONS

What has the Obama Administration had to say about its agenda on national security reform? In early February 2009, General James L. Jones gave an interview to *The Washington Post* [3], as well as a speech at the 45th Munich Security Conference [4], in which he mentioned some of the items on the Administration's reform agenda. One is that the National Security Advisor's role will be expanded; they are going to merge the NSC and the HSC. President Obama has signed a Presidential Study Directive to determine exactly how this needs to be done. They are going to expand the membership of the single NSC, recognizing that national security is much broader and we need a lot more expertise around the table to help the President, but they have decided that they would invite participation on an issue-by-issue basis.

They will look at what expertise we need around the table. When the meeting gets too large, it does not serve the President's needs, and then he is not likely to ask the NSC for help. The council needs to hold a smaller meeting but with the right expertise to assist the President. Especially in the nontraditional national security departments and agencies, they are discussing having an assistant there who will work on national security matters, maybe in agriculture, education, or other areas. They have talked about a common alignment of world regions. Because of our departmentalism, we have allowed each department to decide how it wants to carve up the world, so there are a lot of inefficiencies when we have to work on an interagency basis. They are planning to spend more time monitoring implementation at the NSC, so they have discussed appointing a director. General Jones has talked about creating action groups, which are like the interagency teams that we have proposed.

THE WAY AHEAD

What is the way ahead for the Project on National Security Reform? What are we doing now? We completed our study, but we are still charging ahead, trying to assist people considering the reforms we have proposed, both in the Executive Branch and Congress. We are now very much engaged in assisting the Executive Branch in thinking about how they could implement some of these reforms under existing authority. We are drafting legal instruments, amendments to the rules of the House and the Senate in the new National Security Act.

We have initiated a major collaboration effort. We have our recommendations, but we need to drill down in those recommendations in much more detail. We need to reach out to stakeholders. We need to be thinking about implementation, so we have formed 30 to 40 issue teams that have about 15 members from across the government and from outside government, people who have expertise. They are in the process of drilling down into those recommendations, getting stakeholders involved, and doing some thinking about implementation. Then, we will publish the results of those teams' work. We are continuing to publish our supporting documents, which we think will inform those that have to make these decisions.

That is the story for the Project on National Security Reform, where we are and what we are hoping to achieve to complement the efforts of this symposium and those who are motivated to make our government more effective in the challenges that are confronting us.

Q&A SESSION WITH HONORABLE JAMES LOCHER, III

Q: *Looking at the need for combining interagency teams with presidential advisory teams, do you see the teams funded separately?*

James Locher – Currently, there is no way of funding these teams separately. All funding has to go down through the departments. If, in the future, we are going to do things primarily through interagency teams, maybe they need a separate funding line. It is like the combatant commands in the DoD. They still have executive agents that fund them, but there is the question of whether the President will want the ability to fund something through an interagency team or will ask Congress.

The relations between the Executive and the Legislative Branch are not good. There is not a lot of trust there. The contingency funding arrangement has slowly been eroded, in part because there have been some abuses in the past. I think the President has a contingency fund of about $25 million. Therefore, we are thinking carefully about what the grand bargain might be between the Executive Branch and Congress in which we can really create that partnership and explain to Congress in the 21st Century why the Executive Branch needs more flexibility.

We also have the Executive Branch honoring the role of Congress in national security. When I was in the DoD, we often would not want to think about an important issue because we were afraid Congress would find out we were thinking about it. We were afraid that the other branch of government would somehow be able to examine our thinking on these issues.

This is why we have talked about a partnership. In today's world, we need a much different arrangement. I think the congressional part of this will be most difficult. They have no mechanism—Congress can reform the Executive Branch, but we do not have anyone who can mandate reforms on Capitol Hill. We have spent a lot of time on the Hill talking to people about the need for these changes. If we were able to create a select committee on national security, it could become the catalyst for all sorts of reforms in the House and in the Senate, but we have a lot of work to do on this particular subject.

Q: *I am struck by the similarities between the Project on National Security Reform and the work done in 2003–2004 that led to the Intelligence Reform and Terrorist Prevention Act of 2004 and the creation of the National Counterterrorism Center (NCTC), where counterterrorism experts had a senior clearance. Have you taken a lessons-learned approach to looking at the similarities in terms of what NCTC has or has not accomplished—maybe because it is in the middle of an analogous 10-year process—compared with the direction you want to move the Project?*

James Locher – Yes. Recently, we have made a lot of changes in government. We created the ODNI. We created NCTC. We created the Department of Homeland Security (DHS). Most of those reforms, however, only focused on one element of organizational effectiveness. We focused on the structural aspects in creating these organizations, but, to a great extent, they are structural shells. They do not have all of the elements that make organizations effective. In the Project on National Security Reform, we have spent a lot of our time thinking about all of the elements of organizational effectiveness and what is the most fundamental element. It is something we call shared values.

It is an agreed vision. It is an agreed statement of our missions. It is an agreement of the principles under which we are going to operate. If you think about it, in the interagency, we do not have shared values. Even in various departments, you do not have shared values. If you think about the DHS, it does not have shared values. If you think about the intelligence community, it does not have shared values. We have looked at some of these things in the past. Does the Director of National Intelligence have the authority he needs? No. He has been given a lot of responsibility, but he does not really have the authority that is required.

At NCTC, there is a strategic operational planning directorate. Does it have the authority it needs? No, it does not because the departments and agencies were able to push back. NCTC was supposed to do an integrated plan, and, because they got a lot of pushback from the departments and agencies, they ended up doing a catalog, not a plan. The people who first served out at NCTC, as they went back to their home departments, were treated like they were absent without leave (AWOL). As a consequence, the next group that goes to NCTC to serve in the strategic operational planning directorate will not be quite as enthusiastic as the first group. The human capital part of that has not been fixed.

In part, there is the argument that we cannot reform a small part of the system when the overall system remains unreformed. When the departments and agencies are still focused on their own perspectives, when we are not thinking about what the nation needs, and when we have very weak integrating mechanisms, then it is not, in my view, possible for the strategic operational planning directorate at NCTC to be successful. In this larger environment, it cannot make progress because the system as a whole is not yet prepared for these kinds of changes. We have been trying to study these issues to the best of our ability.

The Director of National Intelligence, Admiral Dennis C. Blair, would like us to do a study on ODNI later this year to think about what is the concept for ODNI and what is the concept of operations for the intelligence community as we go forward. I do not know whether we will complete that, but we have tried to think about all of those elements of organizational effectiveness, shared values, processes, structure, organizational skills, the core competencies, required staff skills, our future organizational strategy, necessary resources, and personnel systems. We considered all of those elements in terms of levers that help us move this agenda forward.

Q: *As I have been listening to your presentation, there is one word that I have not heard you say, which is accountability. Shared values and leadership will take you some distance, but, in the end, are you going to see the Attorney General being eaten up by Congress because the DHS messed things up or the Secretary of Commerce being eaten up by Congress because the State Department messed things up on international trade? It is true that the government works very hard in pursuit of shared values, but it is also true that, at some point, the government works in ways that make it difficult to know who is to be held accountable.*

James Locher – Part of the problem you have today is that it is not clear who is responsible for anything. Responsibility is divided across a lot of places. Let us say, though, we had a National Security Executive who was responsible for an interagency team with a crosscutting vision. Then we know who to go to. The Departmental Secretaries are a little bit like the Secretaries of the military departments. They played huge roles in the past, but their role is somewhat less today because of the fact that we need the ability to work across departments and agencies and we need something like the combatant commanders.

That is what these National Security Executives are. They give us the ability to do joint things in the interagency arena. If you think about it, the situation is similar to what happened as a result of the attack on Pearl Harbor in 1941. Many of you may not have known it, but prior to Pearl Harbor, the Army and the Navy refused to operate with unity of command. We had known since the time of Napoleon the importance of unity of command. Because of service jealousies and in the interest of maintaining their independence, however, they operated under the principle of mutual cooperation. We were defending the Hawaiian Islands under that principle. You can imagine, when you operate by that principle, a lot of things can slip. There was a huge outcry over Pearl Harbor that forced President Franklin Roosevelt to create unified commands.

The European Theater completely unified under President Eisenhower. Because of service jealousies, we ended up with both General Douglas MacArthur, Allied Commander of the Southwest Pacific Theater, and Admiral Chester Nimitz, Commander in Chief of the Pacific Fleet and Pacific Ocean Areas. In the interagency, though, we are still operating under the principle of mutual cooperation. It denies us the ability of really figuring out who has the responsibility and who can be held accountable for these complex operations. This needs to be clarified because, until that is the case, Congress, who is confused, will continue to go after the Secretary of Commerce for something that the State Department did.

We can only hold people accountable when we can be much more precise as to who has the responsibility. Not only do they have the responsibility, they have the authority that commensurates with their responsibility.

Q: *Are you looking for the presidential appointment of an interagency team soon?*

James Locher – In part, we have proposed that idea. These presidential priority teams were the idea behind selecting an area where the President would like to make rapid progress, where he has an interest, and where we are likely to see him ensure that the team is going to be successful that we could try and see what works. We are working in one area to try to develop this. We think that if we are successful in interagency teams, it will spread like wildfire and that you will see a regional interagency combatant command. It could be this teaming concept.

We have been pushing this idea: let us try this, let us develop it, let us see what the problems and benefits are and figure out what kind of authority we need from Congress—there are limits to what authority the President can give the head of an interagency team today—and how we are going to get it. I was very pleased when then-President-Elect Obama announced his National Security team; in their press statement, they talked about whole-of-government and the ability to collaborate; they used the term "team." They continuously referred to themselves as a "national security team."

Given the background of all of these senior people, their understanding of these problems, there is a good chance that you could have the kind of collaboration and cooperation that you could go off in one area, be in an interagency team, and really learn from it. I think we have the right environment for that.

Q: *Is the concept broad enough to include the Treasury Department and the Fed? In my experience, the DoD has not been successful in reaching out to the Treasury.*

James Locher – In that regard, we proposed in the Project that any economic issues that have security implications would be addressed in the single council, and General Jones has endorsed that idea in his comments. In the Project, we debated the scope of national security for 18 months. In part, we knew it was too narrow today, but if you broaden it too far, it becomes meaningless. We tried to think about how it needs to be broadened, and we ended up with a fairly flexible approach that implied the Department of Education is not a national security department but does have a role to play on occasion, as does the Department of Agriculture (USDA).

We need to develop little cadres in those departments that, when we need to turn to them, are able to play a role. General Jones mentioned having assistants for national security in those departments who could remain linked into what the NSC was doing. We would expect the Secretary of the Treasury to be around the NSC table when there are economic or financial issues that require his expertise. I think the Obama Administration understands that that is how they have to proceed; they are not going to look at this rigid membership, and those are the people who are invited.

They are going to look at that full spectrum of expertise that they have in the government and figure out on a particular issue who needs to be involved. One of the case studies that we started to develop was of the Asian financial crisis that had some security implications, but the two communities really never discussed these issues. They remained very separate. We were making decisions on the economic crisis without worrying about what the security implications were. We see the need for all of that to be pulled together. Much of our work will be thinking about what statutory authority is required for different departments and agencies for them to be able to play their role.

I have often heard people from the Treasury Department say that people would like us involved in NSC matters, but we really do not have a statutory base for doing that. We are looking at the issue of what we need to have in the DoE's statutory provisions—or the USDA or the Treasury Department—that permits them to play the role that is required in particular circumstances.

Q: In this process of national security reform, have you considered the role that industry, the defense industry particularly, can play in this process?

James Locher – One thing that we have been trying to think about, especially on the homeland security side, and somewhat on the international security side as well, is that we need to be much more inclusive. Our federal government has a tendency to think about just our departments and agencies. On the homeland security side, we need to do a much better job with the state and local communities, but there is the business-industry-nongovernment world that needs to be brought more into this. In that regard, one of the proposals we have on homeland security is to create a homeland security collaboration committee that would work for the NSC and would have people from the states, local communities, outside of government, business, and nongovernmental institutions, and we would formulate policy and begin to do planning.

We are reaching out and having more of that involvement because, in today's world, even the whole-of-government is not the correct term. It really needs to be "whole-of-society" or "whole-of-nation." We are trying to move in that direction.

REFERENCES

1. http://www.pnsr.org/data/files/pnsr_forging_a_new_shield_report.pdf.
2. *San Francisco Chronicle*, 22 March 2007, available at http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2007/03/22/EDGRJN7BSL1.DTL.
3. K. DeYoung, "Obama's NSC Will Get New Power: Directive Expands Makeup and Role of Security Body," *The Washington Post*, 8 February 2009, p A01.
4. http://www.securityconference.de/konferenzen/rede.php?menu_2009=&sprache=en&id=259&.

1.2 CYBERSECURITY: ATTACKS ON THE CRITICAL INFRASTRUCTURE

Dan Wolf

INTRODUCTION

I spoke at the 2007 Unrestricted Warfare Symposium here two years ago on cyber warfare; one of my contentions is that cyber war is underway, but we just have not admitted it. Today, I will talk about the threats to our critical infrastructure, which is a topic I cover in my Homeland Security graduate course at the University of Maryland that addresses food, agriculture, and water security. Last semester, one of my students said, "Before I took this course, I could sleep at night; now I can't sleep." Having completed a number of topics related to bioterrorism and the food supply, another student actually ran Clorox through their Thanksgiving turkey, concerned about the safety of the food. Naturally, I do not want you to go home and cleanse your computers or turkeys because that is not our primary concern with regard to cyber warfare.

In March 2006, Mr. Daniel G. Wolf became the President of Cyber Pack Ventures, Inc. after 39 years of government service. He was previously the Director of the Information Assurance Directorate of the National Security Agency, providing direct support to the U.S. military worldwide and worked with numerous foreign partners to provide interoperable secure communications and networks. Mr. Wolf has received numerous awards over the years, earned a B.S. in Electrical Engineering from Case Institute of Technology and an M.S. in Electrical Engineering (Computer Systems) from the University of Maryland College Park, and is a graduate of the Senior Executive Fellow Program at Harvard University (Kennedy School of Government) and the Federal Executive Institute.

However, I will discuss the sources of threats to the critical infrastructure, what they are, how they are defined, and a little bit about the dimensions in cyberspace, and then provide some examples of potential cyber attacks.

Due to government classification issues, we do not tell the public and commercial industries the seriousness of this threat. I think the threat has just started to come to light over the last couple of years in terms of bad actors and some of the things that they are trying to do to distrupt our infrastructure. I will try to communicate this today from unclassified examples, and you can extrapolate what a really bad actor can do.

My emphasis here is on financials, and Supervisory Control and Data Acquisition (SCADA) systems, and I will provide examples of some attacks on U.S. international industry. One of the interesting examples—and this is probably a misuse of the word "interesting"—is Estonia, a country very connected electronically. You can hardly buy a loaf of bread in Estonia without having access to the Internet. The cyber attack in 2007 was significant because it was a battleground that exemplified what bad guys could do to you.

I will discuss the cyber initiative and some concerns I have in terms of what we need to do to make that successful. I will make the point that I am no longer a government employee, so these are my personal opinions. Let me start with a quote from Admiral Dennis C. Blair, the new Director of National Intelligence (DNI), in February of this year, in which he talks about cyber attacks on the major financial services, what the impact could be, and the infrastructure in terms of what could happen with the power grids, the oil refineries, etc. It is really a recognition that the critical infrastructure is vulnerable, and we need to start paying more attention to it.

> *"A successful cyber attack against a major financial service provider could severely impact the national economy, while cyber attacks against physical infrastructure computer systems such as those that control power grids or oil refineries have the potential to disrupt services for hours to weeks."*

— Admiral Dennis Blair, DNI [1]

IDENTIFYING THREAT SOURCES

So, who are the malicious actors who are interested in doing bad things to us? The following list of threat sources comes from the U.S. Computer Emergency Readiness Team (US-CERT): [2]

- National governments:
  - Propaganda, Web page defacements, espionage, disruption of services, disruption of the infrastructure
  - Cyber actions to weaken, disrupt, or destroy the U.S.
  - Espionage for attack purposes, technology advancement, or to weaken critical infrastructure
- Terrorists:
  - Disrupt, destroy, terrorize
- Industrial spies and organized crime groups:
  - Financial gain
- Hacktivists:
  - Anti-U.S. sentiment, spread propaganda
- Hackers:
  - Thrill of success
  - Publicity

If you look at the bad actors that network defenders encountered maybe four or five years ago in DoD, we had a different set of players; this has changed. Yes, the sources of the threat from national governments include their propaganda as well as Web page defacement and espionage, but disruption of the infrastructure is a priority. In the past, I do not think the US-CERT threat description included much about the infrastructure and its importance. The idea of weakening, disrupting, or destroying the U.S., whether it is military, financial, power grid, etc., directly concerns the infrastructure. Of course, espionage is a reason to consider technology advancement.

Terrorists, naturally, are interested in disrupting, destroying, or terrorizing. They are not as interested in mass casualties so much as bringing down the U.S. infrastructure. You can look at 9/11 and ask whether or not that was partially an attack on the financial infrastructure in New York. Could terrorists bring down the financial institution of the U.S.? Was that one of their goals, in addition to making a visible statement by going after one of our icons?

> *"… the sources of the threat from national governments include their propaganda as well as Web page defacement and espionage, but disruption of the infrastructure is a priority."*

Industrial spies and organized crime stealing design information from industry constitutes a major issue today. Foreign entities are buying this information and quickly advancing their technology based on U.S. research. The motives of organized crime typically involve financial gain in some manner, either to steal money directly or to hold a victim hostage as part of a ransom scam.

Hacktivists are foreign, politically activist, anti-U.S. hackers whose goals are to support their political agenda through propaganda more than by damage to critical infrastructure. The damage they cause is aimed at achieving notoriety, including such tactics as Web defacement and online harassment. When I get to the Estonia example, you will see where this was very obvious.

The last category, more publicized a few years ago, concerns the hackers who just want to do it for the sake of saying, "I got into that system" or "I caused that problem." These six categories are the typical cyber threat players today.

NATIONAL INFRASTRUCTURE PROTECTION PLAN

The National Infrastructure Protection Plan (NIPP), revised in 2009, includes the following list of critical infrastructure components: [3]

- Banking and finance
- Energy
- Transportation systems
- Information technology and communications
- Healthcare and public health
- Defense industrial base
- Agriculture and food
- Water systems
- Chemical, commercial facilities, critical manufacturing, dams, emergency services, nuclear reactors, materials, and wastes
- Government facilities
- Postal and shipping
- National monuments and icons

The 2009 NIPP added U.S. manufacturing to the preceding sectors but broke it out as a separate entity. The NIPP, which is about 180 pages, also requires follow-on plans, the Sector-Specific Plan (SSP). Each of the sectors in the list is supposed to put together a plan following an outline detailing what the SSP needs to include in terms of what must be done to protect their sector. One of the themes that emerged from the 2009 plan, as opposed to the original plan written in 2002, is that cyber now is actually called out, and each of these sectors is supposed to put some special consideration into looking at cyber and its impacts. Cyber touches every sector on the list because our networks are used to control SCADA, financial and bank transactions, or energy facilities, the power grid, etc. The fact that they finally are recognizing that cyber is important is significant. We have taken a step forward.

DIMENSIONS IN CYBERSPACE

Figure 1 illustrates the dimensions of authorities, ownership, privacy, and liability. At the National Security Agency (NSA), I was responsible for protecting the .mil net, so the chart starts in the .mil sector on the right, the inner oval. The commercial sector might start in the critical infrastructure protection (.cip) area. The point of this chart is that one needs to consider authority, ownership, privacy, and liability dimensions in securing and protecting cyberspace and assessing the threat and how to deal with it.

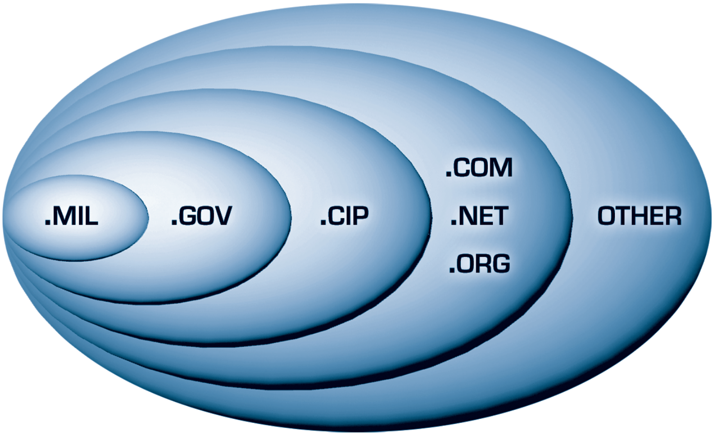


Figure 1 Dimensions in Cyberspace: Authorities, Ownership, Privacy, Liability

The .mil net is owned, managed, and controlled by DoD and its operations. DoD can assert, "Here is the process and here is the equipment you are going to use. Here is how it is set up." It also means that if I want to look for hackers or other activity, because the .mil net is owned and controlled by DoD, I can monitor the communications and activities. I have full authority. I also have the authority to react. Therefore, I can do the detection, but also, if something is going wrong and I detect it, I can do something about it whether it is simply changing my port settings or going out on the net to carry out some sort of Information Assurance (IA) operation.

In contrast, the .gov domain is managed by many organizations. In the President's *National Strategy to Secure Cyberspace*, which was written in 2002, that responsibility went to the Department of Homeland Security (DHS). DHS is responsible for the non-national security systems that are part of the government. The challenge with the .gov is that, in some cases, the government controls it. A particular agency may run the setup or have control, but many of the smaller agencies may not; perhaps a commercial agency is actually running it as the Internet Service Provider (ISP). As a result, the authorities, ownership, and privacy start getting a little fuzzy here.

The .cip is not really a domain name but more of a notional construct for this discussion. The critical infrastructure protection (CIP) notional domain includes the financial sector, the power grid, and surprisingly, the national laboratories. For example, in the Department of Energy (DoE), some of the labs that do nuclear development, like Los Alamos and Livermore, are not necessarily on a .gov domain. Again, the authorities, ownership, privacy, and liability in the CIP domain can vary.

If the financial sector has a problem in its network, what does it tell the government? A financial institution has some liability there because its shareholders may say, "What do you mean you were not protecting your networks?" Further to the left in Figure 1, in the .com, .net, and .org domains, the authorities, ownership, privacy, and liability become even fuzzier. At the far end, we are at what I call the "other" category, which is the home user. With the home user, what authority do I have to say, "You will do the following or you will report the following"? Again, I have very little authority in that respect. It is an interesting challenge in terms of how you deal with these domains.

POTENTIAL CYBER ATTACKS

A recent study by the University of New Hampshire (UNH) [4] provides an interesting set of quotes, which I will paraphrase: "Cyber threats against which the U.S. critical infrastructure are real and growing." I think we observe some of that from headlines in the newspapers. "The impact of a cyber attack could be substantial on the power grid and the financial sector." Again, "A cyber attack could impact a number of sectors, including agriculture, emergency response and preparedness systems, transportation, energy, health care, financial services, and telecommunications." When NSA conducts scenario exercises, it typically considers the impacts on multiple sectors at once (e.g., the emergency sector—911—as well as the financial sector—the bond market in New York City).

According to the study, "The top cyber threats to the U.S. are China and Russia because they have both the intent and the technical capabilities." Probably four or five other countries certainly have the technical capabilities, but, as was mentioned earlier, any 20 people who have some good cyber background could probably create havoc very easily.

Another challenge the UNH study discusses, which many people do not realize, is that over 85 percent of the critical infrastructure is owned by the private sector. The ability to make changes, to mandate things to happen in the private cyber domain, is very difficult and complex.

"We need to respond to activities on the Internet in under a second."

The NIPP also considers the dimension of the U.S. economy, which has become dependent upon the cyber infrastructure because it enables a highly interconnected and interdependent global network of functions and services. Malicious actors routinely conduct attacks against this critical infrastructure. If successful, these attacks could spread quickly and have debilitating effects because of that interconnectedness of the cyber infrastructure, both internally in the U.S. and globally. The word "attacks" can be used in several ways. We can talk about just reconnaissance—malicious actors going out on the network and seeing what the settings are of critical infrastructure cyber systems with the idea that, at some point, they might do something. They are out there, and they are actively planning or attempting attacks even if they are not actually doing them or succeeding. If they did succeed with an attack, the effects could rapidly spread through the global system and result in debilitating damage to commerce.

Rapid Effects Require Almost Instantaneous Response

We need to respond to activities on the Internet in under a second. Does the way we treat cyber attacks today really respond in that timeframe? Probably not in many cases, but we need to reach that level of responsiveness if we are going to have an adequate defense and protect our critical infrastructure. The use of innovative technology and interconnected networks in operations improves productivity and efficiency, but it also increases the Nation's vulnerability to cyber threats if cybersecurity is not addressed and integrated appropriately.

What is cybersecurity? It is preventing damage to and unauthorized use or exploitation of electronic information and communications systems to ensure confidentiality, integrity, and availability. The NIPP provides further guidance on what is needed to restore these in the event of a terrorist attack or natural disaster (i.e., resiliency). This symposium is covering the topic of resiliency in depth: When an attack happens, what does it take to recover?

My experience at NSA taught me to, on the .mil net, always assume that some malicious activity is about to happen—or is actually happening—inside the network. We need to ensure that the ability to maintain operations of critical functions exists, and therefore the idea of resiliency is extremely important. The network needs to be able to recover almost instantly. Innovative technology can help solve some of the problems, but we need more interconnections that must be integrated appropriately.

IT Attacks

In the information technology (IT) sector, "malware" poses a significant challenge. Malware is software designed to infiltrate or damage the computer without the owner's consent.

Malware includes viruses, worms, Trojan horses, rootkits[1], dishonest adware, and crimeware. The more significant attacks that have occurred involve the use of worms, which can significantly disrupt service (e.g., ILOVEYOU, Code Red, Nimda, Slammer). Some of the more advanced malware, theoretically, has the ability to deliver a package to a desktop to cause malicious damage. These programs are much more threatening than some of the earlier ones, which were simply a nuisance—although these "nuisances" can create significant havoc and can cost a lot of money to eradicate. Recent malware can actually deliver a payload that can carry out operations on a desktop or network, allowing an attacker to access and damage critical infrastructure computers and network resources.

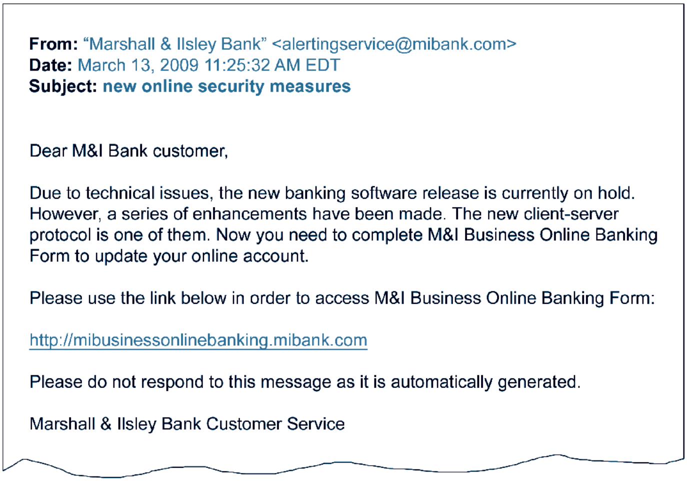
Financial Attacks

Consideration of financial attacks against the critical infrastructure can start with phishing, which is the criminally fraudulent process of attempting to get sensitive personal information such as user names, passwords, and social security numbers by masquerading as a trustworthy entity in an electronic communication. The techniques used include accessing Web pages and installing key loggers, rootkits, and other malware. Figure 2 is an email that I actually received on 13 March. Many others have gotten an email like this as well. I probably get two or three of these a day, which is an astounding number reflecting the amount of activity from these spammers and from phishing in general.

The trick here, of course, is considering whether to click on the link that takes me to the Web site, which may be set to automatically install something on my computer as I go to the Web site, or does the Web site ask me for personal information (e.g., social security number, bank account information)? It seems that by now, everyone should know about phishing and everyone would say this e-mail message should be trashed and would know not to do anything with it, but it is amazing how successful

[1] A rootkit is a program or combination of programs designed to hide attacker activity on a compromised system. An attacker may use a rootkit to replace vital system executables, which may then be used to hide processes and files the attacker has installed. http://en.wikipedia.org/wiki/Rootkit.

Red Team operations and nicely engineered messages can be. If someone were to send 10,000 of these messages, a few people would undoubtedly respond.



From: "Marshall & Ilsley Bank" <alertingservice@mibank.com>
Date: March 13, 2009 11:25:32 AM EDT
Subject: **new online security measures**

Dear M&I Bank customer,

Due to technical issues, the new banking software release is currently on hold. However, a series of enhancements have been made. The new client-server protocol is one of them. Now you need to complete M&I Business Online Banking Form to update your online account.

Please use the link below in order to access M&I Business Online Banking Form:

http://mibusinessonlinebanking.mibank.com

Please do not respond to this message as it is automatically generated.

Marshall & Ilsley Bank Customer Service

Figure 2 Example of a Phishing E-mail

There are some interesting examples of attacks on DoD computers in which very carefully crafted messages were sent to key individuals who opened them up and reacted to them. As a result, their systems were compromised. A good example of a threat—a simple, unclassified one, which suggests what a little more expertise could do to classified systems—is a financial attack in the form of credit card breaches. How many people in the audience have had their Visa or MasterCard reissued in the last 45 days? I see that the majority of the audience has responded positively to the question. Yes, I am one, too. When I called my bank to inquire why, they said, "There was a breach," but they would not identify it. It apparently was some consumer item that I bought—they were very vague about it. A recent *Computer World* article discussed a hacker who had obtained access to the processing center and successfully extracted credit card information. Because a good portion of the audience raised their hands, probably millions of credit cards were compromised. MasterCard gave a warning in mid-February, and it is interesting that both Visa and MasterCard were impacted. New cards are being issued.

In the famous T.J. Maxx incident, hackers stole information on 45 million credit and debit cards from the database. The financial motivation is certainly there. Think of it in two ways: (1) a financial gain for an individual or (2) an attack on the financial infrastructure of the U.S. Imagine the scenarios in terms of what might happen with the banking industry in terms of critical infrastructure to disrupt the financial economy of the U.S.

SCADA Attacks

SCADA systems present one of the scarier scenarios. SCADA systems arose in the 1960s, the idea being to reduce the number of people who physically had to go out to a dam, for example, and change one of the settings on the slew gates or turn a valve somewhere. Some of these are RS-232 modem connections. There are no passwords, no encryption, and no real security, but they control valves, motors, and other forms of equipment. Typically, these connections are network-enabled. It is basically the same technology that you have on any network or on a desktop, but it is actually controlling devices. Typical uses involve hydroelectric dams, water treatment, electric power distribution, transmission, dissemination, petrol storage and refineries, and transportation systems. How many people know that all the trains in the U.S. are controlled from a control center in Orlando, Florida? The fiber-optic cable comes up the tracks across the country to provide that control.

The following list provides a peek into some of the things an attacker could do to manipulate a SCADA system to create havoc; these are the ones that made the public news:

- In 2000, electric power servers were hacked into, and a couple of kids basically played games on the system.
- In 2001, California's Power Control Supervisory Operations Center (CAL-ISO) computer power grid operations were compromised for 17 days. At that time, there was a series of rolling blackouts in California, but California Power denied

that there was any connection between the computer incident and the blackouts. However, many news articles written by knowledgeable reporters implied that there was a connection.

- In 2003, the Slammer Worm infected the network-based operations control system at a FirstEnergy nuclear power plant.

The Slammer Worm attack highlights an issue concerning control of nuclear power plants. In this case, the operational capabilities of the power plant were actually coupled with the external Internet, resulting in some disruption of service there. At a minimum, there was at least some impairment of service. What this minor loss of control highlights is the lack of thought given to the idea that a hacker might try to get into the nuclear power plant through the external Internet. This is an example of a vulnerability we need to address. The source of this information, by the way, is Sandia Labs, which has a center for SCADA security. A lot of work has been done over the last couple of years to improve the SCADA systems, but a great deal more needs to be done.

Cyber Attacks on the U.S. Defense Industry

The U.S. defense industry has also suffered cyber attacks, which have been reported in the news. The source for the following examples is *BusinessWeek* [5]. In April 2008, there was an excellent article about Solar Sunrise in 1998. A couple of kids attacked Air Force and Navy computers, taking advantage of a vulnerability in their operating systems. Moonlight Maze refers to a series of cyber attacks from 1998 to 1999—roughly two years—during which a foreign entity got into quite a few DoD computers, through NASA and the DoE Weapons Labs, extracted data, and exfiltrated it out of the U.S. It demonstrates the vulnerabilities and how active some of these players are. Titan Rain, in 2004, was a similar kind of activity in which classified data were exfiltrated out of defense contractors, a national laboratory, and NASA. Data and sensitive information were exfiltrated because the connections with the Internet were vulnerable to hacking.

In 2007, Byzantine Foothold was the name used in the open press for an operation by the U.S. to investigate and defend against a series of "sophisticated, persistent cyber attacks on a large range of government and contractor targets across the infrastructure." That is a quote from the *BusinessWeek* article. DoD has declined comments on these reported incidents, but that is the open press perspective. This serious incident, I believe, was the "canary in the coalmine" that brought the attention of the government to this serious problem. Some of the hacking attacks we described earlier were merely nuisances. Yes, they cost a lot of money to investigate and recover from, and information was exfiltrated, but Byzantine Foothold, which I believe is the cover name used for investigation and cybersecurity activities, was very significant and finally seized the attention of the government. That was the push for a better strategy on how to deal with this problem.

> *"There are some interesting examples of attacks on DoD computers in which very carefully crafted messages were sent to key individuals and they opened them up and reacted to them. As a result, their systems were compromised."*

CASE STUDY: ESTONIA

Let us take an actual incident, one that has been extensively publicized. It is the cyber attack in Estonia that began in April 2007 and disrupted the network operations of the Estonian parliament, ministries, banks, newspapers, and broadcasters. It happened in the midst of a disagreement between Estonia and Russia about the relocation of a Soviet-era memorial to fallen soldiers, the Bronze Soldier of Tallin, as well as relocation of war graves. It exemplifies an integral connection with other countries, and it demonstrates how hacking cybersecurity is not just limited to activity across defined borders; it is worldwide, omnidirectional. As I will discuss, during the Estonian cyber attack, disruption was coming into the Estonian system via the Internet from 75 countries that use .net domains, showing how cyber attacks can spread across the world because there are no boundaries on the Internet.

As the Estonian cyber attack unfolded and escalated, it became, in a way, a real-world exercise, a cyber security exercise. Estonia is probably one of the most electronically connected countries in the world. You can hardly buy a loaf of bread or a gallon of gasoline without the Internet being required. Most of the banking transactions are done online; I believe the estimate are 97 percent. Electronic funds transfer, debit cards, and other forms of electronic financial instruments are the typical mechanisms for purchases. Actual currency transactions are the exception. The Internet is critical there.

It all started with the Bronze Soldier of Tallin being taken down in late April, an action condemned by the Russians shortly after that. Then, within a matter of days, a cyberspace attack started.

Estonia requested help from NATO and the U.S. That was interesting because the NATO charter establishes that if one of the NATO members is attacked by another entity, all of NATO is supposed to respond and support the country that has been attacked. When the Estonians said to NATO, "We are being attacked," it was one of the first times that the yellow flag had gone up to confirm that an attack on cyberspace is like a physical attack. It set a precedent.

The initial prediction was that a widespread attack would disrupt Estonia's commerce, government functions, and their e-Services, which is equivalent to what we call e-Government in the U.S., and is an integral part of Estonian society, an essential tool. In a presentation one of the IT directors from Estonia gave at the GovSec Conference [6] in Washington, D.C. this year, he reviewed how the Estonian government had developed the infrastructure for providing e-Services; they had just released it to the commercial sector.

"You can hardly buy a loaf of bread in Estonia without having access to the Internet."

The e-Services platform is used all over Estonia, which obviously requires the Internet. It provides Estonian citizens access to government; all information comes out across the portals, and people actually go to the portals to get information. People were so accustomed to obtaining their information this way that, the attack was quite significant to them individually because they lost their source of information. Thousands of systems attacked the Estonian system from over 75 countries worldwide, individual attacks, botnet attacks, Web page defacements—over 100 successful infrastructure disruptions that were tailored by device type and location. Attack techniques included both sophisticated and unsophisticated methods including attempts to control network components and "ping of death" attacks that overloaded systems and caused them to crash.

The targets were the government, the Internet Service Providers (ISPs), the telecommunication facilities, the banks, and the news sources; the attacks focused on these targets as if in response to the Bronze Soldier of Tallin memorial coming down. The Internet was used as a battleground. Phase 1—the attack came in two phases—was what might be called a primitive attack: hacktivists, who were anti-Estonians, got into chat rooms and organized what targets and how they were going to attack. They distributed tools and rough instructions to the participants and focused on the Estonian version of the U.S. .gov Websites. Phase 1 was more or less a denial of service, a little bit of Web defacement, etc.

Then, after a couple of days, the Estonians were able to recover and take charge, so the attack died off. However, soon the attack evolved into a much more sophisticated Phase 2. Secretary Lauri Almann, the Permanent Undersecretary of Defense for the Republic of Estonia, gave a presentation at the GovSec and U.S. Law Conference (24 April 2008) and said that the participants in Phase 2 were now terrorist-cyber-attack specialists rather than merely hacktivists. Their primary tools were software robots (botnets) running from "zombies"—compromised computers—worldwide; they estimated the attacks came from over a million computers in probably about 75 countries.

Next, the attacks went after the online media, the source of the people's information from the government. They went after the banks and commerce systems because, as mentioned earlier, Estonians can hardly buy a loaf of bread without using the Internet.

The attackers went after the two main banks in Estonia, and their primary tool was a denial-of-service attack. Figure 3 is a chart that Dr. Don Goff provided to me from some sessions that he had attended on the Estonia situation. The graph indicates where the attack peaked, where it died off, and then gradually came back up again. The chart is not important in terms of values of the numbers as much as the strategy: try something simple and then move into something a little more sophisticated.

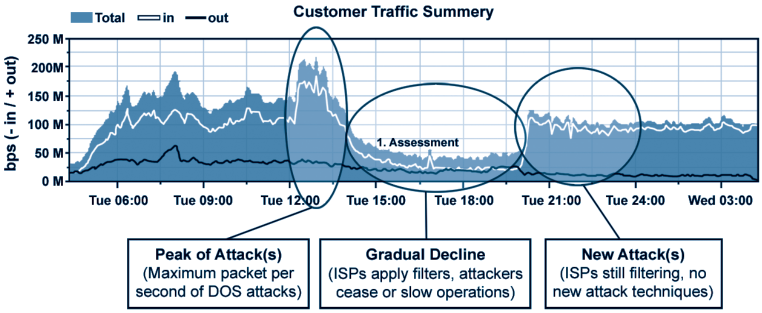


Figure 3 Attack Trend During the Estonian Cyber Attack of 2007

The Estonia attacks provide several lessons:

1. The attackers found out what they could do to cripple a small country.
2. They gauged and determined what the reaction would be of NATO or the other countries of the world and what the kinds of legal actions might take place in response.
3. More importantly, they got to test, in a real-world live exercise, how to bring down the critical

infrastructure of a small country that was very dependent upon it.

SIGNIFICANT GOVERNMENT RESPONSES

What has the government done to protect our critical infrastructure in these areas? The following is a brief historical retrospective—although only a sampling—of government responses to critical infrastructure protection:

- 1987: Computer Security Act
  - Improved security and privacy of sensitive information in federal computer systems
- 1998: Presidential Decision Directive 63 (PDD-63)
  - Established the national program for "Critical Infrastructure Protection"
- 2002: Federal Information Security Management Act (FISMA)
  - Highlighted information security in government IT
- 2003: Homeland Security Presidential Directive (HSPD) 7, the NIPP
  - Unified Critical Infrastructure and Key Resource (CIKR) protection efforts
- 2003: HSPD 8, National Preparedness
  - Established policies to strengthen preparedness for terrorist attacks, major disasters, and other emergencies
- 2008: National Security Presidential Directive (NSPD) 54/HSPD 23
  - Created the Comprehensive National Cybersecurity Initiative (CNCI)
- 2009: National Infrastructure Protection Plan
  - Updated NIPP with emphasis on cybersecurity

The list should also include the President's National Strategy to Secure Cyberspace from 2003. Concerted government efforts to increase cybersecurity date back to 1987 when the Computer Security Act initiated discussion of the protection of sensitive information. PDD-63, which was created during the Clinton Administration, was the first identification of the critical infrastructures that should be protected. FISMA talks about protecting information in government IT. HSPD 7 resulted in the National Infrastructure Protection Plan being written by DHS, and it attempted to unify critical infrastructure and key resources, at least the protection efforts in there.

DHS took that on, hence the origin of the NIPP. Then, the 2009 revised NIPP accounted for a previous oversight—which I consider one of the most significant pieces here—in defining cybersecurity. HSPD 23 and NSPD 54 created the Comprehensive National Cybersecurity Initiative, among other initiatives, but they are the basis for the CNCI.

Because the details of the CNCI are classified, the government is extremely careful about what it says and does not say, so the following list quotes the *BusinessWeek* article because I thought it did a nice job of categorizing the 12 areas of the CNCI:

- Cut connections to the Internet
- Passive intrusion prevention
- Active intrusion prevention
- Counterintelligence strategy
- Counterintelligence tools
- Education
- Fusing operations
- Cyber R&D
- Leap-ahead technologies
- Critical infrastructure protection

- Work with the private sector that owns/operates 85 percent
- Revisit Project Solarium
- Improve federal acquisitions

The *BusinessWeek* article brings up the idea of cutting the connections to the Internet to better control the traffic. Passive intrusion protection asks, “How do you build better firewalls to protect our networks?” while active intrusion protection is more “How do you respond when something is going on?” This is an important distinction. Returning to the Estonia case, the fact that they were able to react to what they saw and able to do something about it was very important. The counterintelligence strategy is to investigate who is doing what in the world in terms of hacking, who are the hackers, what countries are active, and who has an active program in this area.

The counterintelligence tools are somewhat self-explanatory: education—how do we train people? Looking at computer science in the U.S., the number of U.S. graduates is down by almost 30 percent compared to the number of students from foreign populations graduating from U.S. universities with Ph.D.s in computer science or engineering. Do these well-educated graduates stay and work in the U.S., complete their education, and go home? Is the U.S. losing its edge?

In terms of fusing operations, the national cybersecurity initiative is also focusing on how to bring information together. Concerning cyber research and development (R&D), how can we look beyond the low hanging fruit? Considering leap-ahead technologies, how can we do things differently? Finally, we must think of critical infrastructure protection. I believe that is one of the biggest challenges because the private sector owns and operates about 85 percent of the critical infrastructure in this country.

When President Eisenhower created Project Solarium in the early 1950s, he was searching for a strategy on how the U.S. could contain another nuclear power in the world. It was really the strategy of how to survive in a nuclear world. The question today is: how do you cope with the malicious actors in a cyber world? How should the U.S. react if there is an attack, especially if we can identify who the attacker is?

The last item in the list is the need to improve federal acquisitions. Anyone who has dealt in the federal process for procuring IT understands this priority.

As I review the list—and now I am speaking once again as a private citizen—what are some of the challenges that I see to make the cyber initiative successful? First, I think we need to make sure that we have a strategic view. Everyone is a stakeholder. We have to think about cybersecurity by looking at all aspects of how government manages it strategically. The critical infrastructures and the diversity of organizations and people that run those present a significant challenge. We really need to think strategically, not just tactically, from Harry the Homeowner to sensitive government operations, from personal computers to classified networks.

Second, how do we connect solutions of excellence? There are some areas where visualization of network activity is just phenomenal and others where analytic tools are phenomenal. We need to study how to connect all of those into a system so that our cyber defense can react. How do we deal with threats and not just vulnerabilities? We put a lot of emphasis on fixing vulnerabilities, but we really need to think about how we deal with some of the threats I have mentioned. We are never going to be able to totally secure our systems, so what do we do when somebody comes into our systems? How do we respond to that? What is the commercial response to the hacking attack? During James Locher's presentation, some of the questions from the audience concerned representatives from various companies. What do we do when our own company is under attack?

Much of the challenge goes back to the chart in Figure 1. As we move farther out in that domain space—out to the .com and "other" domains—we have less authority over what we can do. So how does the government interact with those domains? Who is in charge: NSC, NSA, DHS, Strategic Command (STRATCOM), or industry? How do we interact with the private sector? Concerning penalties for nefarious behavior, Microsoft offered a $250,000 bounty for information leading to the arrest and prosecution of whoever started the Conflictor Worm, which has caused millions of dollars of damage to Microsoft worldwide. Politics and cultural differences are significant challenges in coordinating efforts to counter cyber attacks.

One of the most significant challenges is developing the means to react at computer speed, meaning under a second. Somehow we have to get the human out of the loop. We cannot simply write reports a day later and say, "Somebody hacked into the computer" because our information may be gone by that point. We need to devise predefined reactions. The Cold War model of nuclear reaction and deterrence—going back to Project Solarium—provides a good model of how we might shape our policies and strategies.

How do we improve the capabilities of cyber analysts given that the U.S. no longer dominates the standards organizations; we have experienced a decline in Computer Science, Engineering, and Math majors; and we are outsourcing IT offshore? We need to invest in research on better visualization tools. The legislation that we fashion has to take into account the various network domains and the authorities and responsibilities illustrated in Figure 1. Can the .mil, .gov, .cip, and private domains share the same procedures within our legal system? How do we react to cyber attacks, actively or passively?

"Somehow we have to get the human out of the loop. We cannot simply write reports a day later …"

In a way, we have defined a new frontier; it is now ground, air, water, space, and cyber. Cyber war is here, and we need to deal with it now, especially in terms of protecting our critical infrastructure, because we are quite vulnerable. The open-source examples reveal that people are out there acting today against our critical infrastructure. The Estonian example, in particular, is cautionary because it shows what can happen in the real world and how a major entity, if determined to do so, could cause a significant problem. I hope my presentation was informative in terms of what some of the threats and vulnerabilities are and where we might proceed from here.

REFERENCES

1. Admiral Dennis Blair, "Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence," 12 February 2009.
2. http://www.us-cert.gov/control_systems/csthreats.html.
3. http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.
4. University of New Hampshire, "Who Are the Greatest Cyber Attack Threats To The United States, 25 January 2007: http://www.unh.edu/news/cj_nr/2007/jan/lw25cyber.cfm.
5. *BusinessWeek*, "The New E-spionage Threat," 21 April 2008: http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm?chan=magazine+channel_top+stories.
6. Almann, L., Permanent Undersecretary of Defense for the Republic of Estonia, "Cyberspace: A Perfect Battlefield? Lessons Learned from the Cyber Attacks Against Estonia," GovSec and U.S. Law Conference, Walter Washington Convention Center, 24 April 2008.

1.3 RESOURCE ATTACKS

Michael Klare

The central thesis of my presentation is that struggle over natural resources, land, water, food, energy, minerals, timber, and other basic commodities will increasingly dominate the terrain of international conflict in the 21st Century. Competition over these materials has, of course, been a central theme in human conflict since the earliest human recorded history. I think it is destined to be even more pivotal in the years ahead for several reasons.

First, because the international demand for all kinds of resources is growing as a result of population growth; globalization, the spread of industrialization to more and more parts of the world; urbanization; and increased worldwide income levels. Second, global supplies of many renewable resources, especially energy, are shrinking. While certain renewable resources, including fresh water, are not sufficiently abundant to satisfy ever-growing levels of demand. This means that the competition for available supplies is bound to become increasingly fierce. Third, as resource deposits in readily-accessible locations in safe, friendly countries are

Professor Michael T. Klare is the Five College Professor of Peace and World Security Studies and has been Director of the Five College Program in Peace and World Security Studies since 1985. Before assuming his present post, he served as Director of the Program on Militarism and Disarmament at the Institute for Policy Studies in Washington, D.C. (1977-84). Professor Klare has written widely on U.S. defense policy, the arms trade, and world security affairs. He has authored, edited, and co-edited published works on conflict, world security challenges, arms and weaponry, and human rights. Professor Klare received his bachelor's and master's degrees from Columbia University in 1963 and 1968, respectively, and his Ph.D. from the Graduate School of the Union Institute in 1976.

depleted, consuming nations must rely increasingly on supplies acquired from less-easily exploited deposits in remote, unsafe, unfriendly countries. This extends supply lines and exposes those engaged in extractive operations to increased risk of attack from terrorist insurgents and criminal bands.

Fourth, many governments have chosen to securitize key materials, viewing them as essential to national security and thus worthy of protection with military force if necessary. For some countries, such as the U.S. and China, oil is viewed in this manner. For others, including Egypt and Israel, water is seen in this light. Fifth, as the supply of vital materials contracts with respect to demand, their monetary value increases. This makes their ownership that much more attractive to rulers, or would-be rulers, of the countries in which large deposits of them are found. This is the origin of what is called the resource curse: the tendency of the rulers of these countries to retain power at all costs, including military dictatorship or other forms of authoritarian rule, and of their aspiring successors to employ military or violent means to unseat them, thereby acquiring control over the resource wealth for themselves. Many of the internal conflicts now underway in oil and mineral producing areas of the developing world are of this character.

Sixth, because the major resource importing nations, especially the U.S., China, and the European Union countries, are becoming ever more dependent on energy and mineral supplies from once colonial areas of the world in Asia, Africa, and the Middle East, there is a growing presence of giant multinational corporations in these areas. This, in turn, is provoking a certain amount of anti-foreigner and anti-imperialist sentiment that is exploited by various extremist groups, including al Qaeda and its spinoffs.

Seventh and finally, every aspect of the resource equation is bound to be affected by global warming. Although much remains uncertain, it appears that large parts of the developing world will experience a significant reduction in rainfall, jeopardizing the production of food for hundreds of millions of people and forcing many of them to migrate to more favorite(?) locations where they are likely to encounter fierce resistance from those already occupying those areas.

For all these reasons, I believe that conflict over resources will dominate the terrain of both interstate and intrastate conflict in the decades ahead. Other factors will, of course, play an important role, but disputes over access to and ownership of vital resources will prove increasingly vital. To appreciate this and to better gauge the impact of this trend on American national security policy, it is useful to examine each of these points in greater detail. Some are examined in greater detail than others.

The first is growing international demand. I am not going to say a lot about this because I think it is pretty obvious. You always have to be aware of it because it is the engine for everything else. It is because of sharply rising international demand for all sorts of critical materials, coupled with dwindling supplies, that so many of the other problems arise. This is especially true of demand for energy and water.

According to the U.S. Department of Energy (DoE), world energy consumption is expected to grow by 50 percent over the 25-year period between 2005–30, rising from about 460 to 700 quadrillion British thermal units (BTUs). The projected increase, 240 quadrillion BTUs, is equivalent to current energy consumption by the U.S., Canada, Japan, and Western Europe combined. In other words, it is a colossal amount of additional energy that will have to be acquired from every conceivable source in just a quarter of a century. Procuring this additional energy while simultaneously addressing the challenge of climate change will prove one of the most difficult challenges facing world leaders in the years ahead, as we are already finding in our own country.

A similar challenge arises in the case of food and fresh water. The two of which are closely related; approximately 70 percent of human water usage is devoted to irrigation for food production. The world population is expected to grow by 28 percent between 2008–30 from approximately 6.5 to 8.5 billion people. The need for drinking water and other basic human materials will naturally grow by a like amount, which is going to put enormous pressure on all supplies of basic resources. This is the demand side.

"I believe that conflict over resources will dominate the terrain of both interstate and intrastate conflict in the decades ahead."

What about the supply side? If we could be certain that the global supply of all basic commodities, food, water, land, energy, minerals, and so on was growing in tandem with the increase in world demand, we would not have to worry so much about the prospects for future conflict over resources. However, that is not the case. There is growing evidence that the global supply of many critical materials will not be able to grow enough to meet rising world demand. In some cases, it will actually diminish.

Now let us take a look at oil, the world's most important source of energy. According to the most recent DoE projections, world liquids output in 2030, including petroleum, biofuels, and non-conventional petroleum sources, will be about 112.5 million barrels a day, just enough to satisfy anticipated world demand at that time. Most professional energy experts question this optimistic picture, claiming that the world's liquid output will fall far short of 112 million barrels per day. They do so on several grounds.

First, daily output in many of the most prolific fields, now in production around the world, is declining at a much faster pace than previously thought. Second, the rate of discovery of new oil fields is also declining, meaning that there is less new oil available each year to replace that being extracted from existing fields. Third, most of the untapped fields now in development are located far offshore or in corrupt or unstable countries, raising the startup costs and discouraging investment.

Suffice it to say that many energy professionals now agree that 100 million barrels per day is probably the upper limit for a conventional oil production. This figure will be supplemented by the addition of biofuels and nonconventional oil. However, this will not be enough to avert an eventual contraction in the supply of petroleum liquids. Moreover, the peak of 100 million barrels will last for only a few years.

After that, conventional oil production will decline. Even with the addition of nonconventional fuels, we will see a contraction in total supply. When this will occur is not exactly known. Most analysts believe it will occur probably between 2015–20, suggesting that the projections offered by the DoE are far too rosy and that we could expect a significant gap between world supply and demand well before 2030.

The picture for natural gas is not as discouraging, if only because natural gas was developed later in the industrial age than oil. Gas, like oil, is a finite substance. It too will reach a peak of production and then commence an irreversible decline probably a decade or so after oil. I do not have time to run through all the other materials. Coal is more abundant, but it too will reach a peak of production and contract probably around the middle of the century. Uranium is now considered sufficient for current needs for quite some time, but if we turn to nuclear power for environmental reasons and ramp up nuclear production, then uranium will become a scarce commodity.

We look at minerals. Some are plentiful like iron. Others including copper, cobalt, and nickel are found in less-abundant deposits. Many of the most prolific of these are already now being exploited. We face shortages of those in the years ahead. When supplies of these and other materials dwindle, whether in absolute terms or in relation to demand, competition for what remains of the available supply is bound to grow. This competition will most often be expressed in financial terms in the form of rising prices as we have seen, but it will also have political and military consequences.

"Even with the addition of nonconventional fuels, we will see a contraction in total supply."

It is not just the imbalance between supply and demand that is likely to provoke competition and friction, but also the fact that the major consuming nations must rely increasingly on sources of supply located in distant and troubled areas. This is probably even more important. This is the product of a natural feature of the resource extraction process. Almost invariably, entrepreneurs begin by developing deposits of whichever resources we are talking about that are close at hand, close to the surface, easy to exploit, or are located in countries that are friendly, stable, and respect the law.

It is only when these easily exploited resources are depleted that producers will turn to remote, hard to exploit deposits in countries that are unfriendly, unstable, and corrupt. In the case of many vital resources, especially energy and certain team minerals, this is the point we are at today. Because many consuming nations cannot avoid reliance on these materials, they face an increased threat to their overseas supply lines from terrorism, criminal violence, piracy, and war.

Consider, for example, America's reliance on petroleum. Up until the 1970s, we obtained two-thirds to three-quarters of our petroleum from domestic supplies. We now rely on imports for 60 percent of our petroleum supply. This percentage may drop a bit in the coming years if all of the efforts to increase our reliance on domestic alternatives succeed, but we will continue to rely on imports for at least 50 percent of our petroleum supply for a good decade or two to come.

Now, we used to be able to rely on countries in the Western hemisphere—Canada, Mexico, Venezuela, Columbia, and Brazil—for a good share of our total import supply, but this is no longer the case because most of the supplies in those countries are in decline or their demand is increasing. More and more of their own output will be consumed domestically. As a result, the U.S. will become increasingly dependent on imports from extra hemispheric sources, primarily in the Middle East and Africa.

This means, of course, greater reliance on energy supplies carried by tanker over long distances, in some cases traversing pirate infested or potentially war-affected waterways, such as the Persian Gulf, the Gulf of Guinea, the Red Sea, and the Straits of Malaka. The same is true of minerals. We have used up a lot of our domestic minerals. We can rely less and less on Western hemisphere minerals, and more and more will have to come from Eurasia and Africa. What is true for the U.S. is increasingly true for China, which used to be self-sufficient for most minerals and energy but is now drawing more from Latin America and Africa. Europe has always relied on seaborne commerce and resources but is becoming more dependent on pipelines. The pipelines of the world are becoming longer and more vulnerable to attack.

"The pipelines of the world are becoming longer and more vulnerable to attack."

My next point is the securitization of natural resource dependency. As the major consumers become more dependent on resources that are at-risk, they are coming to view them more through the lens of national security as something that can legitimately be protected through the use of military force. Of course, nations have always used military force to acquire and protect natural resources. This was a big part of the history of the world from the beginning of the Colonial era right through World War I and World War II.

After World War II, however, the use of force to acquire or protect foreign resource supplies was not viewed as a legitimate cause for initiating combat, at least among the western powers except when such supplies were said to be threatened by the Soviet Union or its clients and surrogates. That threat was, however, the backdrop for some of the most celebrated presidential doctrines of the Cold War era, including the Truman, Eisenhower, and Carter doctrines, all of which were enunciated in response to perceived Soviet-backed threats to Middle Eastern oil.

Of these, the Carter doctrine is the most relevant today. As articulated by then President Jimmy Carter on 23 January 1980, an attempt by an outside force to gain control of the Persian Gulf and thus choke off the flow to Western markets will be regarded as an assault on the vital interests of the U.S. Such an assault will be repelled by any means necessary, including military force. This was the basis upon which Carter established the nucleus of the U.S. Central Command (CENTCOM).

Although intended at the time to deter Soviet adventurism in the Persian Gulf area, the Carter doctrine's underlying principle has been extended over time to other threats to Persian Gulf oil, including those from Iran and Iraq. During the Iran/Iraq war of 1980-88, for example, President Reagan authorized the use of force to protect Kuwaiti oil tankers against attacks by Iranian gunboats, which became Operation Ernest Will. Then when Iraqi forces invaded Kuwait on 2 August 1990, posing an apparent threat to Saudi Arabian oilfields, the first President Bush concluded that such an assault would threaten vital U.S. interests and thereby justified an American military response, which was the basis for Operation Desert Storm.

A similar policy has since come to govern U.S. links with major oil producers in Africa and the Caspian Sea Basin. The protection of global oil transportation systems has also come to be securitized in this manner. As the U.S. has become more dependent on supplies acquired from distant transoceanic locations and as the threat to oil shipments from pirates and terrorists has grown, the military has been accorded greater responsibility for the flow of global oil flow.

". . . an attempt by an outside force to gain control of the Persian Gulf and thus choke off the flow to Western markets will be regarded as an assault on the vital interests of the U.S. Such an assault will be repelled by any means necessary, including military force."

Under National Security Presidential Directive 41, approved by the most recent President Bush on 21 December 2004, the military services, especially the Navy, are given increased responsibility for protecting the global supply chain, a key component of which is the global oil flow. The Navy and its sister (? brother) services have responded to this with the new guiding doctrine, a cooperative strategy for 21st Century sea power adopted in October 2007.

In this sense, the flow of oil has been highly securitized by the U.S. Its protection has been designated a matter of national security. The armed forces have been tasked with responsibility for ensuring its safe delivery to the U.S. Other countries have also securitized oil in this fashion. For example, China has behaved in this way with respect to the South and East China Seas.

For some countries, it is water rather than oil that has been securitized. For example, Israel has declared that access to the waters of the Jordan River is vital to its national survival. Water to Israel is not a luxury, former Prime Minister Moshe Sharett once declared. It is not just a desirable and helpful addition to our natural resources. Water is life itself. A similar outlook has long governed Egypt's stance with respect to the Nile River. The next war in our region will be over the waters of the Nile, not politics, then Minister of State for Foreign Affairs Boutros Boutros-Ghali declared in 1988.

"The next war in our region will be over the waters of the Nile, not politics, then Minister of State for Foreign Affairs Boutros Boutros-Ghali declared in 1988."

The facts that these states and others not mentioned have securitized vital resources in this manner increases the risk that competition over their procurement will result in crisis in conflict as demand increases and supplies dwindle. This is not to say that conflict over resources is inevitable. I am only suggesting that a predisposition to view resource disputes through the lens of national security will lead to a greater inclination to imply force in a crisis.

As I mentioned earlier, there are two other aspects of this problem. The first is the resource curse because this is the kind of conflict that we are increasingly being drawn into. An increase in the monetary value of vital resources stemming from the growing disparity between supply and demand is also likely to exacerbate the phenomenon known as the resource curse or the tendency of authoritarian rule in developing nations to receive a large portion of their natural income from the export of a particular raw material.

Because this income is the only major source of wealth in such a society, those in power, whether a royal family, a tribal group, a military clique, or a political faction, tend to retain power for as long as possible rather than lose control over the allocation of resource royalties or rents. Typically, they use a share of their income to buy off the military and police to ensure their royalty in any clash with opposition forces. As one would expect, the obverse of this phenomenon is a greater likelihood that those who would seek to replace the existing regime and thus alter the allocation of resource rents or keep the money for themselves will employ force in effecting political change.

". . . a predisposition to view resource disputes through the lens of national security will lead to a greater inclination to imply force in a crisis."

Resource rich states in the developing world are therefore especially prone to internal attack from dissident tribes, military cabals, political factions, and ethnic groups. Because the prevailing regime obtains most of its wealth and funds needed to retain the loyalty of security services from foreign energy and mineral firms, these too often become targets of the rebels' wrath.

An important example of this phenomenon is the struggle waged in Nigeria by the Movement for the Emancipation of the Niger Delta, or MEND, against the federal government in Abuja. For the past few years, MEND and a number of other rebel groups have been attacking oil installations in the Delta region, where most of the oil is produced, and kidnapping or killing aid patriot oil workers in an effort to channel some of the vast oil wealth collected by federal officials and bring it back to the Delta, which rarely sees any benefit of the production.

Although probably numbering no more than a few hundred competent and equipped with light weapons alone, MEND and its sister organizations have had a devastating impact on oil production in the Delta area. According to the DoE, as much as one-fourth of Nigeria's daily oil output of approximately three million barrels per day has been shut in due to rebel activity. The resource curse has also spurred the separatist ambitions of various ethnic groups, especially when valuable oil or mineral reserves are located in their imagined ethnic homeland.

In such cases, oil abundance often tends to provoke civil wars by giving people who live in resource rich areas an economic incentive to form a separate state. Indeed, the inhabitants of such areas express a widespread belief that the central government was unfairly expropriating the wealth that belonged to them and that they would be richer if they were to form a separate state. It is precisely these views that are often cited by groups like the Ogadon National Liberation Front and the Front for the Liberation of the Kabinda Enclave to justify their ongoing struggles against the central governments of Ethiopia and Angola, respectively. This is also a factor in Kurdish aspirations to establish an ethnic homeland in Northern Iraq.

Finally, I will discuss terrorism, insurgency, and criminal violence. As production of vital resources has declined in more favorable locations around the world, consuming nations have been forced to rely increasingly on supplies acquired from distant and unfavorable locations, as previously noted. In the case of oil and natural gas, this has been greater reliance on supplies acquired in the Islamic world, notably the Persian Gulf in North Africa. This, in turn, has resulted in the extensive presence of energy and mining companies associated with the major western powers and now China in these areas, often accompanied by an equally conspicuous diplomatic and military presence.

No matter how hard these firms and their home governments try to paint these activities in a benign development friendly light, they are going to be seen by many in these countries through the lens of the colonial experience, which will generate resentment against the intrusion of foreign firms and personnel. The fact that the outsiders often seem to cozy up to the authoritarian governments that tend to rule these countries in consonance with the resource curse only makes the situation worse.

In some cases, extremist groups, who seek to overthrow the prevailing government, oust the foreigners from the region, and install a revolutionary regime of some sort, have exploited this resentment. By far, the most dangerous product of this phenomenon is al Qaeda and its offshoots. From Osama bin Laden's perspective, the House of Saud has become a willing partner in America's effort to occupy the Middle East in the pursuit of oil and the subjugation of Islam and so must be swept away, along with its American backers.

"If current trends persist, it seems to me inevitable that the U.S. military will increasingly evolve into a global resource protection service."

Other factors have undoubtedly figured in Osama bin Laden's thinking. However, the link between oil, western economic interests, and the corruption of the royal family is the persistent theme in his repeated calls for violent attacks on the U.S. and the House of Saud. Although bin Laden himself no longer appears capable of playing a direct role in attacks on U.S. and Saudi interests, shadowy groups that share his extremist views have continued to attack key elements of the Saudi oil infrastructure.

The first in a series of such assaults occurred on 1 May 2004, when gunmen killed five Western oil industry workers in Yanbu, the site of a major petrochemical complex. A second attack took place four weeks later when a group of armed militants, said to be allied with al Qaeda, stormed a residential compound occupied by Western oil workers in Kobar and killed 22 people. A far more ominous assault occurred on 23 February 2006, when suicide attackers broke through the outer defense parameter of the Uptake oil processing facility and detonated explosive-laden vehicles inside the kingdom's most important energy installation, jeopardizing potentially 6.8 million barrels of daily oil output.

In response to these assaults, the Saudis, no doubt in cooperation with U.S. counterterrorism officials, have stepped up their defenses at major oil installations and have worked energetically to crush remnants of al Qaeda in the kingdom. Terrorist violence of this sort, specifically targeted at oil installations and personnel, has erupted in other countries where al Qaeda-like organizations have sprung up. In Algeria, for example, another group linked to al Qaeda known as the Solafus Group for Preaching and Combat (GSPC), attacked a convoy of vehicles transporting employees of Halliburton and the Algerian state-owned oil company Sanatruck on 10 December 2006, killing an Algerian driver and wounding four Britains and one American. In a communiqué claiming responsibility for the attack, GSPC said that it was determined to drive American companies out of Algeria. GSPC is now known as al Qaeda and the Islamic Magram.

Aside from terrorist attacks of this sort, which are driven by an explicit ideological impulse, the safe delivery of resource supplies from distant locations are imperiled by criminal activities, including piracy on the high seas and pipeline attacks by organized criminal bands. Although always a factor in international commerce, such attacks appear to be growing in number and degree of organization as economic conditions deteriorate in many parts of the world.

I was going to talk about global warming, but I don't think it is necessary for me to do that. As we go further into the future, though, global warming is going to primarily affect water supplies in many parts of the world, creating huge numbers of environmental refugees and provoking conflict over what remains of available water supplies.

What then do I see are the implications of all this for U.S. national security? If current trends persist, it seems to me inevitable that the U.S. military will increasingly evolve into a global resource protection service. The armed services will be asked to devote an ever-increasing portion of their time, manpower, and capabilities to the protection of overseas resource deposits and facilities, along with the governments that grant us access to those deposits, and the sea lanes that connect us to those foreign sources of supply.

This is readily apparent, I believe, in such key strategic documents as NSPD 41 and the Navy's 2007 policy statement, "A Cooperative Strategy for 21st Century Sea Power." Perhaps there are some in the military community who feel comfortable with these developments or simply believe that it is not their place to question them. However, I feel compelled to point out that this trend poses enormous costs and risks for this nation. The deployment of American combat forces in overseas resource zones inevitably stokes the hostility of those who recall the transgressions of the Colonial era or otherwise recent foreign intrusion into their homeland and so adds to the intensity of anti-Americanism in these areas.

The close ties our government has fostered with petro regimes and other authoritarian governments afflicted by the resource curse further fans the flames of anti-Americanism and contributes to the recruiting success of extremist organizations. All too often American soldiers themselves become the target of militant attack, adding to the costs and risks of such operations. There are good reasons to ask moreover whether the use of military force is a cost-effective means of ensuring access to resource supplies in embattled areas abroad.

> *"If current trends persist, it seems to me inevitable that the U.S. military will increasingly evolve into a global resource protection service."*

If you believe, as I do, that the first Gulf War, the current war in Iraq, and the permanent deployment of substantial U.S. forces in the Persian Gulf area can be at least partially tied to this objective, then we have spent in the vicinity of two or three trillion dollars over the past few decades, not to mention the high cost in human life, without seeing a noticeable increase in the safety of Persian Gulf oil deliveries. Would the flow of oil have been less safe in the absence of such expenditures? Perhaps. I think at that level of expenditure, we could have long since devised better and safer ways to address our energy needs.

What this suggests, I believe, is that U.S. military policy and resource behavior are two sides of the same coin. The greater our dependence on imported materials that must be acquired from distant and dangerous locations in a world of every growing resource competition and conflict, the greater the likelihood that we will rely on military force to ensure our access to such supplies.

If we continue to securitize and make it a matter of policy that we use force, we could be entering an era of recurring resource wars at great cost to the nation's treasury, morale, and military preparedness. The only way to avoid this fate is to significantly reduce our reliance on imported materials through increased conservation and the development of alternatives derived from domestic materials. As our reliance on imports diminishes, we can place greater trust in market forces to provide us with the imported materials we still require.

After all, while some foreign producers may be closed to us through choice, others no doubt will be happy to take our money, especially in these times of economic hardship. Increased conservation and the accelerated development of homegrown alternatives to imported materials should therefore be viewed as national security priorities as a far better investment than some of the military solutions that have been proposed to safeguard foreign supplies.

I will conclude then by stating that the dangers posed by growing resource competition and inadequate supply, coupled with the growing impact of climate change, are destined to intrude into every aspect of international and national affairs. One aspect of this is an increase in interstate and intrastate conflict, but this is not the only major aspect. Ultimately, every aspect of human life will be affected by these developments. Becoming more aware of the significance of global resource trends is therefore essential to an understanding of the human predicament today.

1.4 ECONOMICS AND FINANCIAL ATTACKS

James Rickards

INTRODUCTION

National security has never been more captive to economic security than it is today. By economic security, we do not refer principally to the usual fluctuations in GDP, employment, productivity, and other metrics that have been the focus of macroeconomists for decades and that still predominate in academic studies. Analysis of trends in GDP such as the rise of China, decline or instability in Russia, and the outlook for the U.S., while important, do not by themselves pose immediate challenges to U.S. national security. We refer instead to global capital flows and the capital and commodities markets that accommodate those flows. It is through these channels that currencies can be destroyed, inflation can be transmitted, reserves can be depleted, and financial institutions can be destabilized. In the extreme, entire sections of global capital markets can be frozen and debilitated to the detriment of those who rely on them the most; in particular, the U.S.

Mr. James G. Rickards is Senior Managing Director at Omnis, Inc. and Co-Head of the firm's practice in Threat Finance & Market Intelligence. Mr. Rickards previously held senior executive positions at Citibank and RBS Greenwich Capital Markets as well as Long-Term Capital Management and Caxton Associates. Mr. Rickards has directly participated in significant financial events such as the 1981 release of U.S. hostages in Iran and the LTCM financial crisis of 1998 in which he was the principal negotiator of the government-sponsored rescue. Mr. Rickards holds an LL.M. (Taxation) from the New York University School of Law; a J.D. from the University of Pennsylvania Law School; an M.A. in International Economics from the JHU/SAIS, and a bachelor's degree with honors from The Johns Hopkins University.

Central Bankers and Finance Ministers and Treasury Secretaries speak glibly about systemic risk while rarely stopping to think about what they mean by the word "system," which is at the root of systemic. They have a concept of the system of money and banking (and the institutions that conduct those operations that create money and extend credit) that connects directly to macroeconomic theories expressed variously as Keynesian or Monetarist. This understanding translates into misnamed stimulus packages, which are, in fact, redistributionist inflation packages to be carried out by Treasury borrowing and Federal Reserve monetization of the resulting debt (Cogan et al., 2009 [2]). The circularity of this superficial understanding of system and the ineffectuality of macroeconomics in a systemic crisis is thus complete.

"National Security has never been more captive to economic security than it is today... [Through] global capital flows and the capital and commodities markets that accommodate those flows, . . . currencies can be destroyed, inflation can be transmitted, reserves can be depleted, and financial institutions can be destabilized."

Instead, we propose an analysis of the economic system through the binocular lenses of physics and engineering with an approach called econophysics. This approach studies the following questions: Are global capital markets a system? If yes, is it a static or dynamic system? If dynamic, is it a linear or nonlinear dynamic? If a nonlinear dynamic, what are the emergent properties of nonlinearity? Is the system scale-invariant? What are the appropriate metrics for normalizing and parameterizing scale? Does it represent an example of self-organized criticality? What are the boundaries of systemic phase transitions? The studies of these and other questions are the keys to understanding expected behavior and appropriate public policy in the face of the ongoing global financial collapse. A proper understanding of the behavior of global capital markets is furthermore the key to understanding the vulnerabilities of the U.S. and other national participants, which allows both for defensive and counterintelligence measures and offensive capability where necessary, all under the heading of weaponized money.

CAPITAL MARKETS AS COMPLEX DYNAMICAL SYSTEMS – ECONOPHYSICS

Financial economics has, over the past 50 years, specialized in quantitative analysis of problems of asset pricing, asset allocation, and risk management. Its contributions have been voluminous, leading to the creation of derivative products and the enormous expansion of the markets in which those products are traded. Key contributions have included the Black-Scholes options pricing formula and the Capital Asset Pricing Model. Underlying these developments are two hypotheses:

- The Efficient Market Hypothesis (EMH), which states that all available information is fully and rationally incorporated into market prices that move from one level to another based on new information without reference to the past, and therefore no individual analysis can outperform the market because all insights are effectively "priced in."
- A Gaussian or normal distribution of price movements (sometimes called the "random walk" model, i.e., each price move is independent of any prior price move, etc.) such that small fluctuations are common and extreme events are proportionately rare with the overall degree distribution of such events falling in the familiar bell curve shape associated with random phenomena.

These hypotheses were combined in a General Equilibrium Paradigm based upon mean reversion.

Beginning in the late 1980s, substantial doubt emerged with respect to this intellectual edifice. These doubts arose both deductively as the result of the new science of nonlinear physics, and inductively as the result of numerous empirical observations that failed to confirm either EMH or the Gaussian degree distribution. In effect, a paradigm shift was underway in which the influence of behavioral economics, fractal geometry, complexity theory, heuristics, network science, and related fields converged to demonstrate that not only did the General Equilibrium Paradigm fail to describe the reality of capital markets but a more robust paradigm with powerful explanatory ability was waiting to take its place.

The empirical failures of the General Equilibrium Paradigm are well known. Consider the 19 October 1987 stock market crash in which the market fell 22.6 percent in one day; the December 1994 Tequila Crisis in which the Mexican Peso fell 85 percent in one week; the September 1998 Russian Long-Term Capital Management (LTCM) crisis in which capital markets almost ceased to function; the March 2000 .com collapse during which the National Association of Securities Dealers Automated Quotation (NASDAQ) numbers fell 80 percent over 30 months; and the 9/11 attacks in which the New York Stock Exchange (NYSE) first closed and then fell 14.3 percent in the week following its reopening. Of course, to this list of extreme events must now be added the financial crisis that began in July 2007. Events of this extreme magnitude should, according to the General Equilibrium Paradigm, either not happen at all (because rational buyers will seek bargains once valuations deviate beyond a certain magnitude) or happen perhaps once every 100 years (because standard deviations of this degree lie extremely close to the x-axis on the bell curve, which corresponds to a value close to zero on the y-axis, i.e., an extremely low frequency event). The fact that all of these extreme events took place in just over 20 years is completely at odds with the predictions of stochastic methodology in a normally distributed paradigm.

Practitioners treated these observations not as fatal flaws in the General Equilibrium Paradigm but rather as anomalies to be explained away within the framework of the paradigm. Thus was born the "fat tail," which is applied as an embellishment on the bell curve such that after approaching the x-axis (i.e., the extreme low frequency region), the curve turns upward again to intersect data points representing a cluster of highly extreme but not so highly rare events. No explanation is given for what causes such events; it is simply a matter of fitting the curve to the data (or ignoring the data) and moving on without disturbing the paradigm. A better approach would have been to ask the question: if a normal distribution has a fat tail, is it really a normal distribution?[1]

Of course, many critics, notably Nassim Taleb (2007) [3] in his book, *The Black Swan*, have made the point that analytics based on normal distributions do not accurately describe market behavior in many instances. However, while these critics have been incisive—and in my view correct—on the deficiencies of the normal distribution, they have not provided a new and analytically rigorous paradigm to replace it. It is not enough to overthrow an intellectual paradigm without offering a useful replacement. Indeed, risk managers could almost be excused for continuing to use the current deeply flawed methodology in the absence of anything with which to replace it.

"One of the most common degree distributions in nature, which accurately describes many phenomena, is the power law, which shows that the severity of an event is inversely proportional to its frequency with the proportionality expressed as an exponent."

A Gaussian distribution is not the only possible degree distribution. One of the most common degree distributions in nature, which accurately describes many phenomena, is the power law, which shows that the severity of an event is inversely proportional to its frequency with the proportionality expressed as an exponent. When graphed on a double logarithmic scale, the power law describing financial markets risk is a straight line sloping downward from left to right; the negative exponent is the slope of the line.

This difference is not merely academic. Gaussian distributions and power law distributions describe two entirely different

[1] More recent embellishments on the simple bell curve model include T-models of implied volatility and Generalized Auto-Regressive Conditional Heteroskedasticity (GARCH); however, these methods are also flawed because they continue to rely on normal distributions as a base case and frame of reference instead of abandoning the flawed methodology completely.

phenomena. Power laws accurately describe a class of phenomena known as nonlinear dynamical systems, which exhibit scale invariance; i.e., orderly patterns are repeated at all scales. What is often taken for randomness at a given scale actually produces order (albeit chaotic, i.e., unpredictably deterministic) across scales. Examples of such systems in nature include earthquakes (consider the familiar Richter Scale's inverse proportionality of the severity and frequency of temblors with minor events being common and events of seven or higher being quite rare).

The field of nonlinear dynamical systems has recently been enriched by the concept of self-organized criticality as described in Bak (1996) [4]. The idea is that actions propagate throughout systems in a critical chain reaction. In the critical state, the probability that an action will propagate is roughly balanced by the probability that the original action will dissipate. In the subcritical state, the probability of extensive effects from the initial action is low. In the supercritical state, a single minor action can lead to a catastrophic collapse. Such states have long been observed in physical systems, e.g., nuclear chain reactions in uranium piles, where a small amount of uranium is relatively harmless (subcritical) and larger amounts can either be carefully controlled to produce desired energy (critical), or can be shaped to produce atomic explosions (supercritical). (Supercritical systems are just larger, more complex versions of critical systems; both are poised on the edge of an unpredictable but potentially catastrophic outcome.) Informed by this new paradigm of the self-organized, scale invariant, nonlinear dynamical system in the critical state (i.e., the Nonlinear Paradigm), we return to the field of finance to consider the implications from the perspective of systemic risk and threats to national security.

The theory of financial markets existing in a critical state cannot be tested in a laboratory or particle accelerator in the same fashion as theories of atomic physics (although experiments using recursive difference equations applied to simple economic models of inventory accumulation do tend to confirm the theory; Scheinkman, 1994 [5]). Instead, the conclusion that financial markets are a critical system rests on two nonexperimental bases, one deductive, one inductive. The deductive basis is the ubiquity of power laws as an explanation for the behavior of a wide variety of complex systems in natural and social sciences, e.g., earthquakes, forest fires, sunspots, polarity, drought, epidemiology, population dynamics, size of cities, wealth distribution, etc. (Lam, 1998 [6]). This is all part of a more general movement in many natural and social sciences from 19th and early 20th Century equilibrium models to nonequilibrium models; this trend has now caught up with financial economics.

For those who cling to perceptions of short-term equilibrium, the term "punctuated equilibrium" may be more congenial. The inductive basis is the large variety of capital markets behavior, which has been empirically observed to fit well with the Nonlinear Paradigm (Mandelbrot and Hudson, 2004 [7]). It is certainly more robust than the General Equilibrium Paradigm when it comes to an explanation of the extreme market movements described above (e.g., 1987 stock market crash, etc.). It is consistent with the fact that extreme events are not necessarily attributable to extreme causes but may arise spontaneously in the same initial conditions from routine causes. Experts who have pondered why the stock market fell almost 23 percent in a single day in 1987 have tried to retrofit various explanations with culprits ranging from a dispute with Germany on currency values to the rise of portfolio insurance. Similarly, experts have queried why in 1998 the hedge fund LTCM lost $4 billion in four weeks and nearly caused a systemic collapse, while in 2006 another hedge fund, Amaranth, lost $6 billion in one week and barely caused a ripple in financial markets. The answer in both cases is that there is no linear relationship between cause and effect and the search for differentiating proximate causes is futile. What does matter is that in all three cases, the system was in a critical state, but only in two (1987 and 1998) did initial conditions cause market losses to propagate into a full-scale panic whereas in the other case (2006) such propagation did not occur; it died out. This is exactly the kind of unpredictable but potentially catastrophic behavior that the Nonlinear Paradigm predicts.

In addition to these extreme events, research has shown that movements in stock prices adhere to the kind of discontinuous, scale-invariant behavior that the Nonlinear Paradigm describes. For example, if one were to compare two normalized stock price charts, one showing monthly fluctuations over a 50-year period (i.e., 600 observations) and one showing fluctuations every five minutes over a 50-hour period (also 600 observations), there would be no fundamental difference between the two in terms of amplitudes, periodicity of trends, discontinuities, and extreme events (Peters, 1991 [8]). In other words, the deep structure of financial markets is self-similar and chaotic at every scale.

What is important for our purposes is to understand those emergent properties of nonlinear systems that have most relevance for an analysis of the deep structure of financial markets. Emergent properties include the following:

- Such systems are subject to sudden sharp collapses.
- The severity of such collapses is inversely proportional to the frequency (e.g., one event of size 1000 for every 1000 events of size one); however, *the extreme events happen with greater frequency than expected in a Gaussian distribution*.
- A power law distribution allows events of all sizes with some frequency limited only by the scale of the system in which they occur.
- Events are scale-invariant, i.e., large events are just bigger versions of small events and are not otherwise qualitatively different; this is important because the implication is that either small or large events may be caused *by the same initial action*, rather like minor or major forest fires possibly being caused by the same carelessly thrown match.
- Complexity is correlative with unpredictability.

Recall that while extreme events occur with much greater than normal frequency in nonlinear critical state systems, these events are nevertheless limited by the scale of the system itself. If the financial system is a self-organized critical system, as both empirical evidence and deductive logic strongly suggest, then the single most important question from a national security perspective is: what is the scale of the system? Simply put, the larger the scale of the system, the greater the potential collapse with correlative macroeconomic and other real world effects.

The news on this front is daunting. There is no normalized scale similar to the Richter Scale for measuring the size of markets or the size of disruptive events that occur within them; a few examples will make the point. According to recent estimates prepared by the McKinsey Global Institute, the ratio of world financial assets to world GDP grew from 100 percent in 1980 to 200 percent in 1993 to 316 percent in 2005. Over the same period, the absolute level of global financial assets increased from $12 trillion to $140 trillion and is projected to increase to $240 trillion by 2010. The drivers of this exponential increase in scale are globalization, derivative products, and leverage.

Globalization in this context is the integration of capital markets across national boundaries. Until recently there were specific laws and practices that had the effect of fragmenting capital markets into local or national venues with little interaction. Factors included withholding taxes; capital controls; protectionism; nonconvertible currencies; and licensing, regulatory, and other restrictions that tilted the playing field in favor of local champions and elites. All of these impediments have been removed over the past 20 years to the point that the largest stock exchanges in Europe and the U.S. (NYSE and Euronext) now operate as a single entity.

Derivative products have exhibited even faster growth than the growth in underlying financial assets. This is due to improved technology in the structuring, pricing, and trading of such instruments and the fact that the size of the derivatives market is not limited by the physical supply of any stock or commodity but may theoretically achieve any size because the underlying instrument is notional rather than actual. The total notional value of all swaps increased from $106 trillion to $531 trillion between 2002 and 2006 (New York Times, 2008 [9]). The notional value of equity derivatives increased from $2.5 trillion to $11.9 trillion over the same period while the notional value of credit default swaps increased from $2.2 trillion to $54.6 trillion (New York Times, 2008 [9]).

Leverage is the third element supporting the massive scaling of financial markets, i.e., margin debt of U.S. brokerage firms has more than doubled from $134.58 billion to $293.2 billion from 2002 to 2007 while the amount of total assets per dollar of equity at major U.S. brokerage firms has increased from approximately $20 to $26 in the same period. In addition, leveraged investors invest in other entities, which themselves use leverage to make still further investments, etc. This type of layered leverage is impossible to unwind in a panic.

There can be no doubt that capital markets are larger and more complex than ever before. In a dynamically complex critical system, this means that the size of the maximum possible catastrophe is exponentially greater than ever. Recalling that systems described by a power law allow events of all sizes and that such events can occur at any time, particularly when the system is supercritical, the conclusion is inescapable that the greatest financial catastrophe in history is not only inevitable but could well be what we are experiencing today.

The more advanced risk practitioners have long recognized the shortcomings of using historical data in a normally distributed paradigm to compute risk measured in standard deviations from the norm. This is why they have added stress testing as an alternative or blended factor in their models. Such stress testing is based on historically extreme events such as the market reaction to 9/11 or the stock market crash of 1987. However, this methodology has its own flaws because the worst outcomes in a dynamically complex critical state system are not bounded by history but are only bounded by the scale of the system itself. Since the system is larger than ever, there is nothing in historical experience that provides a guide to the size of the largest catastrophe that can arise today. The fact that the financial crisis which began in July 2007 has lasted longer, caused greater losses, and been more widespread both geographically and sectorally than most analysts predicted or can explain is a function of the fact that the vastly greater scale of the financial system is producing an exponentially greater catastrophe than has ever occurred before. This is why the past is not a guide and why the crisis may be expected to produce results not unlike the Great Depression of 1929–1941.

A clear understanding of the structures and vulnerabilities of the financial markets points the way to solutions and policy recommendations. These recommendations fall into the categories of limiting scale, controlling cascades, and securing informational advantage.

To explain the concept of limiting scale, a simple example will suffice. If the U.S. power grid east of the Mississippi River were at no point connected to the power grid west of the Mississippi River, then a nationwide power failure would be an extremely low probability event. Either the "east system" or the "west system" could fail catastrophically in a cascading manner but both systems could not fail simultaneously except for entirely independent reasons because there are no nodes in common to facilitate propagation from critical state to catastrophic failure across systems. In a financial context, governments should give consideration to preventing mergers that lead to globalized stock and bond exchanges and universal banks. The first order efficiencies of such mergers are outweighed by the risks of large-scale failure especially if those risks are not properly understood and taken into account.

"A clear understanding of the structures and vulnerabilities of the financial markets points the way to solutions and policy recommendations."

The idea of controlling cascades of failure is, in part, a matter of circuit breakers and pre-rehearsed crisis management so that nascent collapses do not spin into full systemic catastrophes before regulators have the opportunity to prevent the spread. The combination of diffuse credit and layered leverage makes it infeasible to assemble all of the affected parties in a single room to discuss solutions. There simply is not enough time or condensed information to respond in real time as a crisis unfolds. One significant circuit breaker which has been discussed for over a decade but which has still not been implemented is a clearinghouse for all over-the-counter derivatives. Experience with clearinghouses and netting systems such as the Government Securities Clearing Corporation shows that gross risk can be reduced 90 percent or more when converted to net risk through the intermediation of a clearinghouse. Bearing in mind that a parametric decrease in scale produces an exponential decrease in risk in a nonlinear system, the kind of risk reduction that arises in a clearinghouse can be the single most important step in the direction of stabilizing the financial system today—much more powerful than bailouts, which do not reduce risk but merely mask it temporarily.

A clearinghouse will also provide informational transparency that will allow regulators to facilitate the failure of financial institutions without producing contagion and systemic risk. Such failure (what Joseph Schumpeter called "creative destruction") is another necessary step on the road to financial recovery. Technical objections to clearinghouse implementation based on the nonuniformity of contracts can be overcome easily through consensual contractual modification with price adjustments upon joining the clearinghouse enforced by the understanding that those who refuse to join will be outside the safety net. Only by eliminating zombie institutions and creating breathing room for healthy institutions with sound balance sheets can the financial sector hope to attract private capital to replace government capital and thus restart the credit creation process needed to produce sound economic growth.

In summary, Wall Street's reigning risk management paradigm consisting of a combination of stochastic methods in a normally distributed model combined with stress testing to account for outliers is a manifest failure. It should be replaced with the empirically robust model based on nonlinear complexity and critical state dynamics. Applying such a paradigm leads to the conclusion that the current financial crisis is likely to get far worse and threaten national security because the system has been scaled to unprecedented size prior to the onset of the catastrophe. It also points the way to certain solutions, most importantly the creation of an over-the-counter derivatives clearinghouse, which will descale the system and lead to an exponential decrease in actual risk. Such a clearinghouse can also be used to improve transparency and manage failure in ways that can leave the system far healthier while avoiding systemic collapse.

Based on this vulnerability analysis, the question arises whether an enemy of the U.S. could insinuate itself in financial markets in such a way that it became a trusted counterparty with access to credit and transactional venues and then use that access to create imbalances that would branch and cascade through critical nodes in such a way to cause panic, failure, and collapse? If so, how would this be done?

The ideal commercial cover for an enemy assault on financial markets would be an institution large enough to deploy massive amounts of capital and obtain large lines of credit but unregulated enough not to pose significant barriers to entry or be subject to oversight. This could be done using a variety of intermediaries including hedge funds, trust accounts and derivative products or all of these in combination. If an enemy fails they have a modest cost and some deniability; if they succeed, they could destroy Western capital markets. This is an excellent risk–reward ratio.

However, an enemy does not actually have to launch an attack to gain significant advantage. Strategically, we are back to Cold War theories of deterrence and applications of game theory. An enemy in a credible position to destroy Western capital markets need only threaten to do so in order to have the desired impact on policy makers.

“Picking a bottom in financial markets is a popular pastime for investors and market analysts, but national security analysis should be more concerned with what happens once the bottom is reached.”

For an enemy that cannot match the U.S. on the land, sea, or air, we estimate that the temptation to fight in the financial markets is great. Our financial markets are more vulnerable than ever, the methods for attacking them are easy and inexpensive, and the returns to the enemy in terms of the destruction of wealth and confidence are inestimable. It is imprudent to take this threat lightly or ignore it. There will be no time to prepare once financial warfare commences. Legal, collections, and counterintelligence responses to these threats are considered in the section on National Responses. Now we turn to an analysis of how the current economic crisis may be an even greater threat to national security than the actions of rivals and enemies.

VULNERABILITIES DUE TO PERSISTENT ECONOMIC STAGNATION

The greatest economic threat to national security arises not from exogenous attacks but from endogenous weakness arising from the current financial crisis. And this endogenous weakness is likely to be exponentially more catastrophic than policy makers realize in light of the power law and critical state analysis advanced in the preceding section. The implications of this crisis in that context are now considered.

Picking a bottom in financial markets is a popular pastime for investors and market analysts, but national security analysis should be more concerned with what happens once the bottom is reached. All falling markets find a bottom eventually. The Dow Jones Index may fall to 5,000 or even lower, but it will stabilize at some point. The important issue for the economy, and therefore national security, is what happens then? There seems to be an a priori assumption, or maybe just a large dose of wishful thinking, that when the markets bottom they will bounce back and quickly recover most if not all of the lost ground eventually reaching new highs. This is certainly the mantra of "buy and hold" analysis, which says that it is foolish to sell stocks at low levels because you will miss the rebound or be out of the market on that hypothesized single day when the Dow rises 1,000 points and your losses are erased in one quick burst of euphoria.

But what if markets do not bounce back? What if they go down and stay down?

The problem with the bounce-back view is that the pertinent evidence is much to the contrary and not at all encouraging. Volatility is a powerful feature of markets today and we would not rule out large one-day rallies in major stock indices from time to time. But the evidence from bubble behavior shows that once we hit bottom (and we may still be a year or more away depending on the particular asset class or index considered), we should expect a prolonged and pernicious period at the bottom itself without any appreciable gains for years. The implications of this for tax revenues, fiscal stability, U.S. economic power, and the ability of the U.S. to project hard or soft political power are daunting.

Market technicians refer to this as the "LUV problem" using the letters "L" "U" and "V" to denote types of market behavior following a collapse of the kind we are now experiencing. Most optimistic and quite common in cyclical downturns is the V-shaped recovery in which the economy as a whole or some important subcomponent declines rapidly, hits bottom, and bounces back quickly to the former high level and beyond in something that looks like a "V" when plotted on a graph. Such behavior has been observed many times, notably in the Russia-LTCM Crisis of 1998–1999 when the Dow Jones Industrial Average dropped from 9337 to 8028 (a decline of almost 15 percent) in 10 weeks from mid-July to late September 1998 but regained all of the lost ground by the following January and went on to a new high of 11,497 by the end of 1999. An investor who sold at the bottom on 25 September 1998 and stayed out would have missed a gain of 43 percent in the following 15 months. Examples such as this give the "V" story a lot of its power among salesmen and TV talking heads.

Also not uncommon is the "U" shaped recovery in which the economy or certain indices first fall, then remain at or near the bottom for an extended period before regaining their old highs. The difference between the "V" and "U", of course, is the time spent bouncing along the bottom, but investors in both situations are encouraged some rebound is in sight. A good example is the 1990–1991 recession. In that episode, the Dow Jones Industrial Average reached 2900 at the beginning of July 1990 then fell to 2510 by early October 1990—a 13.4 percent decline. However, by the end of November 1991 it had only recovered to 2894, putting it just below where it had been 17 months earlier. The period in between included an extended trough, which gives the "U" shaped graph its name.

Which brings us to the last of our trio of market graphs, the "L" shaped recovery—which, in fact, means no recovery at all; at least not in any time frame in which the recovery is causally linked to the original decline. An L-shaped phenomenon represents a sharp decline followed by a prolonged and open-ended period of stagnation or malaise in which the recovery, when it does finally arrive, probably needs to be jump-started by some extreme event such as a war that is dynamically disconnected from the cause of the decline. (Many recessions are said to carry the seeds of their own recovery; the L-shaped decline decidedly does not.) The most famous example of this is the Great Depression, in which the initial industrial contraction lasted 43 months (August 1929 through March 1933) followed by a weak recovery and a second decline of 13 months (May 1937 through June 1938) followed by a second weak recovery. The Industrial Production Index calculated by the Federal Reserve stood at 8.6646 on 1 July 1929 and 8.8115 on 1 March 1940; a total increase of only 1.5 percent after 10 years and eight months.

Another famous example of "L" behavior is the Nikkei 225 index of leading Japanese stocks traded on the Tokyo Stock Exchange. After reaching an all-time closing high of 38,915 on 29 December 1989, it dropped precipitously and reached an interim low of 14,517 on 30 June 1995—a spectacular decline of 63 percent in 4-1/2 years (Figure 1).

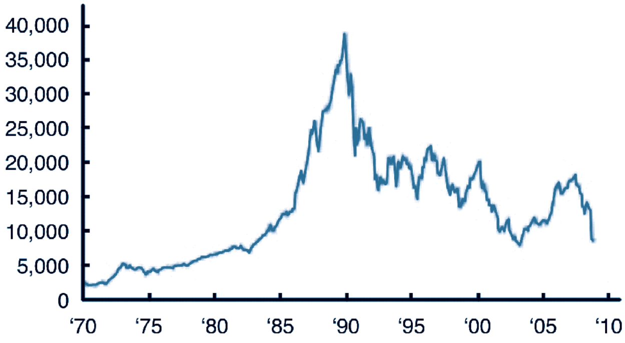


Figure 1 Nikkei 225 Index 1970–2009

But the story does not end there. After several rallies and new declines, the index ground down to other interim lows of 7907 on 2 May 2003 and then 7162 on 27 October 2008, a breathtaking 81.6 percent below the all-time high reached almost 19 years earlier. Around 1999, analysts started talking about Japan's "Lost Decade." They still do but seem not to have noticed that another 10 years have gone by with no progress.

Another example closer to home is the NASDAQ Composite Index, which reached an all-time high of 5048 on 10 March 2000 and today trades around 1535; about 70 percent below the all-time high almost nine years later (see Figure 2).

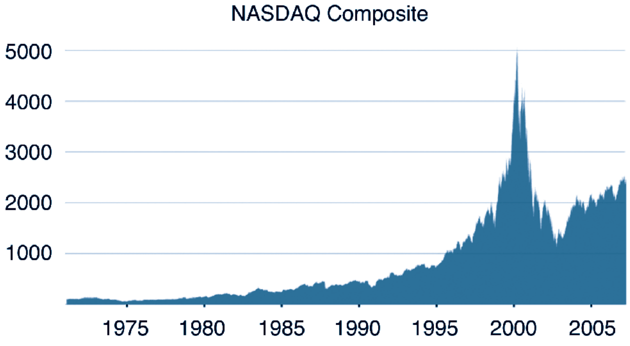


Figure 2 NASDAQ Composite Index, 1975–2005

What the Depression, Nikkei, NASDAQ, and other similar episodes all have in common is that they were preceded by bubbles. The Depression and the Nikkei collapses both followed bubbles in real estate and stocks. The NASDAQ collapse was associated with the .com bubble bursting. Bubble behavior shows up clearly in the preceding graphs and is characterized by a sudden rise from a previous low level, which feeds on itself until it achieves a hyperbolic spike followed by an equally violent downward break then a prolonged period at a relatively low level compared to the previous peak. What is most striking is the enormous amount of time between the spike and the return to anything approaching that level. The Depression took over 10 years in terms of industrial production, although some markets including commercial real estate did not recover until the mid-1950s, 25 years after the 1929 crash. The Nikkei has still not returned to its peak after 19 years. NASDAQ has not returned to its peak after nine years. Contrast these time periods to the talking heads who declare (without analysis) that the stock market will reach new highs by late 2009 or that housing will recover by early 2010 and you begin to see the problem.

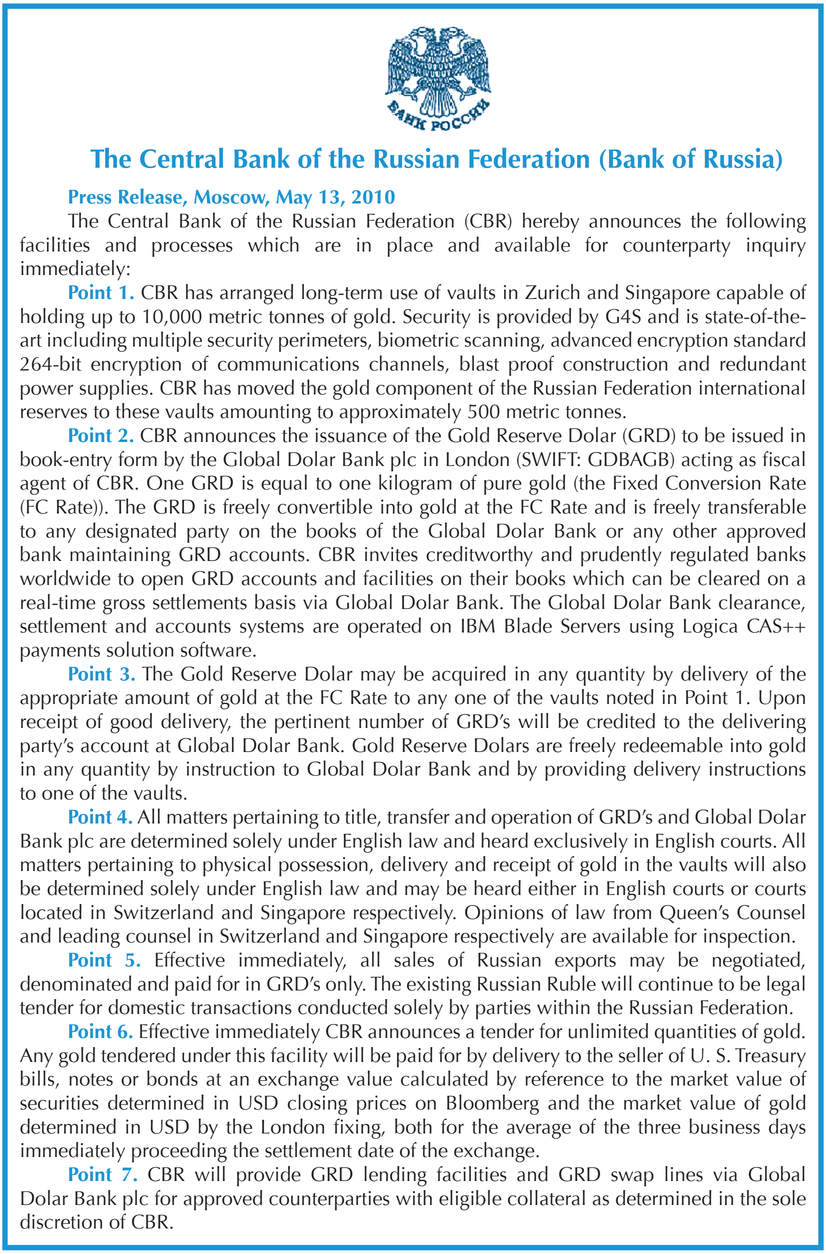
What the U.S. has just experienced is the breaking of numerous bubbles in residential housing, credit card debt, consumption versus savings, growth in derivative products, growth in structured products, and the willingness of investors to use leverage and sell volatility in order to chase illusory gains. These breaks are not characteristic of normal cyclical downturns of the type which occurred in 1990–1991 and 2001 or even the more severe downturn of 1973–1975. We expect that the U.S. economy has entered a prolonged and steep decline that could reduce real GDP by 20 percent or more over the next several years with no immediate prospects for recovery.

The defense, intelligence, and diplomatic communities should expect a potent mixture of increased missions due to failed states, civil unrest, and enemy adventurism induced by our economic weakness, and a world of diminished resources due to fiscal constraints and rising demands for bailouts and the social safety net. The combination of increased missions and reduced resources will stress readiness, analytic and collections capability, and priorities across the board. In the LUV trio, the L-shaped recovery is the one most dangerous for national security and the one most likely to occur.

COLLAPSE OF THE U.S. ECONOMY AND COLLAPSE OF THE U.S. DOLLAR AS A RESERVE CURRENCY

Worse even than the long, slow grind along the bottom described in the foregoing section is a sudden catastrophic collapse. In that context, the greatest threat to U.S. national security is the destruction of the U.S. dollar as an international medium of exchange. By destruction we do not mean total elimination but rather a devaluation of 50 percent or more versus broad-based indices of purchasing power for goods, services, and commodities and the dollar's displacement globally by a more widely accepted medium. This can happen more easily and much more quickly than most observers imagine. The following example hypothesizes a single country, Russia, acting unilaterally to require that all of its exports (principally oil and natural gas) henceforth be paid for in a new gold-backed currency issued by a newly formed fiscal agent of the Central Bank of Russia based in London. However, variations on this plan can easily be imagined including a joint announcement to similar effect by Russia and China or an even larger group under the auspices of the Shanghai Cooperation Organization and in affiliation with Iran.

The following invented press release (Figure 3) from the Central Bank of Russia illustrates how quickly and easily a dollar Pearl Harbor-style attack might be executed. This press release addresses numerous technical issues including acceptable rule of law, enforceability, settlement and clearance facilities, lending and credit facilities, etc., all of which would be subject to further analysis and the articulation of detailed policies and procedures in a real-word implementation. However, there is nothing new or particularly daunting in any of this. The point here is to show how easily this could be done.



БАНК РОССИИ

The Central Bank of the Russian Federation (Bank of Russia)

Press Release, Moscow, May 13, 2010

The Central Bank of the Russian Federation (CBR) hereby announces the following facilities and processes which are in place and available for counterparty inquiry immediately:

Point 1. CBR has arranged long-term use of vaults in Zurich and Singapore capable of holding up to 10,000 metric tonnes of gold. Security is provided by G4S and is state-of-the-art including multiple security perimeters, biometric scanning, advanced encryption standard 264-bit encryption of communications channels, blast proof construction and redundant power supplies. CBR has moved the gold component of the Russian Federation international reserves to these vaults amounting to approximately 500 metric tonnes.

Point 2. CBR announces the issuance of the Gold Reserve Dolar (GRD) to be issued in book-entry form by the Global Dolar Bank plc in London (SWIFT: GDBAGB) acting as fiscal agent of CBR. One GRD is equal to one kilogram of pure gold (the Fixed Conversion Rate (FC Rate)). The GRD is freely convertible into gold at the FC Rate and is freely transferable to any designated party on the books of the Global Dolar Bank or any other approved bank maintaining GRD accounts. CBR invites creditworthy and prudently regulated banks worldwide to open GRD accounts and facilities on their books which can be cleared on a real-time gross settlements basis via Global Dolar Bank. The Global Dolar Bank clearance, settlement and accounts systems are operated on IBM Blade Servers using Logica CAS++ payments solution software.

Point 3. The Gold Reserve Dolar may be acquired in any quantity by delivery of the appropriate amount of gold at the FC Rate to any one of the vaults noted in Point 1. Upon receipt of good delivery, the pertinent number of GRD's will be credited to the delivering party's account at Global Dolar Bank. Gold Reserve Dolars are freely redeemable into gold in any quantity by instruction to Global Dolar Bank and by providing delivery instructions to one of the vaults.

Point 4. All matters pertaining to title, transfer and operation of GRD's and Global Dolar Bank plc are determined solely under English law and heard exclusively in English courts. All matters pertaining to physical possession, delivery and receipt of gold in the vaults will also be determined solely under English law and may be heard either in English courts or courts located in Switzerland and Singapore respectively. Opinions of law from Queen's Counsel and leading counsel in Switzerland and Singapore respectively are available for inspection.

Point 5. Effective immediately, all sales of Russian exports may be negotiated, denominated and paid for in GRD's only. The existing Russian Ruble will continue to be legal tender for domestic transactions conducted solely by parties within the Russian Federation.

Point 6. Effective immediately CBR announces a tender for unlimited quantities of gold. Any gold tendered under this facility will be paid for by delivery to the seller of U. S. Treasury bills, notes or bonds at an exchange value calculated by reference to the market value of securities determined in USD closing prices on Bloomberg and the market value of gold determined in USD by the London fixing, both for the average of the three business days immediately proceeding the settlement date of the exchange.

Point 7. CBR will provide GRD lending facilities and GRD swap lines via Global Dolar Bank plc for approved counterparties with eligible collateral as determined in the sole discretion of CBR.

Figure 3 Fictional Press Release Announcing Currency Conversion to Gold

The intention of Central Bank of Russia would be to cause a 50 percent overnight devaluation of the U.S. dollar and displace the U.S. dollar as the leading global reserve currency. The expected market value of gold resulting from this exchange offer is $4,000 per ounce, i.e., the market clearing price for gold as money on a one-for-one basis. Russia could begin buying gold "at the market" (i.e., perhaps $1,000 per ounce initially); however, over time its persistent buying would push gold-as-money to the clearing price of $4,000 per ounce. However, gold selling would stop long before Russia was out of cash as market participants came to realize that they preferred holding gold at the new higher dollar-denominated level. Gold will actually be constant, e.g., at one ounce = 25 barrels of oil; it is the dollar that depreciates. In this scenario, we are not pricing gold in terms of dollars, we are repricing dollars in terms of gold, so, one dollar is eventually redefined as ≅ 1/4000th of an ounce of gold. This can be a very attractive tradeoff for a gold power like Russia. Thereafter, we can start to divide the world into gold haves and have-nots the same way we do with oil reserves today. For those dealing in gold, oil, grain, and other commodities, nothing changes. It is only the dollar that goes down. Basically, the mechanism is to switch the numeraire from dollars to gold; then things start to look different and the dollar looks like just another repudiated currency as happened in Weimar and Zimbabwe. Russia's paper losses on its dollar securities are more than compensated for by (a) getting paid in gold for its oil, (b) the increase in the value of its gold holdings (in dollars), and (c) watching the dollar collapse worldwide.

Another important concept is the idea of setting the global price by using the marginal price. Russia does not have to buy all the gold in the world. It just has to buy the marginal ounce and credibly stand ready to buy more. At that point, all of the gold in the world will reprice automatically to the level offered by the highest bidder, i.e., Russia. The market may test its willingness to buy (just as hedge funds periodically test the credibility of central banks to defend their currencies). However, before Russia would be forced to buy $200 billion worth of gold (about 1,500 metric tonnes @ $4,000 per ounce; $200 billion being about how much U.S. dollar liquidity they have), the world would decide they like holding onto their gold at the new price. So the world will wake up to find a new dollar/gold equilibrium. If China joins Russia in this plan, its success is assured.

"The defense, intelligence, and diplomatic communities should expect a potent mixture of increased missions due to failed states, civil unrest, and enemy adventurism induced by our economic weakness, and a world of diminished resources due to fiscal constraints and rising demands for bailouts and the social safety net."

The question for the national security community is not whether this can happen; it can. The questions instead are: Can steps be taken to prevent this from happening? What are the key indications and warnings that it is actually happening? What are the immediate consequences to U.S. national security of this happening?

This plan takes into account the current reality. There is no existing currency that can displace the dollar; they all have worse problems and there are not enough liquid instruments denominated in those currencies to absorb world savings. But a new currency could be launched as described in the preceding scenario, backed by gold at a fixed rate, cleared and settled through existing banking channels and with swap and lending facilities available. In principle, a private institution could do this (as had been done routinely prior to 1933), but a nation-state is a more credible candidate. The U.S. seems not to take the idea seriously and benefits from its ability simply to print dollars. China has little gold and too much to lose from being financially co-dependent on the U.S. The Euro is not a country and most of the gold in Europe belongs to the nation-states not to the European Central Bank. The obvious candidate is Russia, which has very little to lose; its currency is worthless abroad and rapidly depreciating at home, but it does have a decent gold supply above ground, about 500 metric tonnes, and excellent mining capacity. The objections to Russia have to do with trust and the rule of law, but these are easily solved as described in the preceding scenario by using Switzerland and London as physical and legal venues. All it would take is for the Russians to trust themselves—a not insignificant obstacle.

The U.S. could prevent this by preempting it—just by issuing a gold-backed dollar itself using the 4,600 metric tonnes available in Fort Knox (over nine times the Russian gold supply). Another approach is to convene a Bretton Woods II Conference, likely a G-20 meeting in today's world, and implement this on a global basis. The standard objection to gold-based money is "there's not enough gold." Of course, this argument is specious because there's always enough gold; it's just a matter of price. At $900 per ounce, the total aboveground world gold supply will not support the total money supply of the leading trading nations. But at $4,000 per ounce, the gold supply is adequate. Other objections to gold-backed currency based on the failures of the Gold Exchange Standard of 1926–1931, Eichengreen (1995) [10] and Ahamed (2009) [11], are in apropos because those failures had nothing to do with gold and everything to do with mispricing; central bankers of the 1920s wanted to revert to pre-World War I prices and exchange rates that were nonsustainable after the paper money inflation of the war years. What is needed today is a unilateral or multilateral repricing to a realistic level, which is exactly what Franklin Delano Roosevelt (FDR) attempted in 1934 when he redefined the dollar from 1/20th of a gold ounce to 1/35th. In effect, one U.S. dollar would now be defined as ≅ $1/4000^{th}$ of a gold ounce. This path, while practical, is entirely unlikely because of the lack of serious political or academic interest or understanding and the plain convenience of printing dollars. Our estimate is that the U.S. will not act to prevent the destruction of the dollar until something like it is already underway.

As for indications and warnings, they are easy to specify and detect; the issue for the national security community is whether anyone is looking and whether the proper analytical tools are in place. Russia's gold reserves denominated in dollars at current prices increased from $14.5 billion to $15.5 billion in January 2009. Why? Who's minding that store? A dedicated watch function combined with appropriate analytics could provide some early warning of an effort to launch a gold-backed currency especially since either China or Russia would have to place the gold outside their home countries respectively to engender trust among those willing to rely on the new currency. Acquisition of gold by central banks and physical movement of gold to neutral vaults could all be tracked using information from exchanges, dealers, banks, and secure logistics firms such as Brink's and G4S. Techniques such as calculating the second derivative of the slope of a curve tracing the time series of the spread between spot physical and Comex near month gold futures may be especially revealing.

The consequences of failing to detect the threat or act on it are, in a word, devastating. Imagine a world in which the price of oil measured in units of gold is held constant at one ounce = 25 barrels, but the price in dollars instantaneously becomes $155 = one barrel based on the new dollar/gold exchange rate. Then apply similar ratios to all U.S. imports of commodities and manufactured goods. The result is that the U.S. would re-import the hyperinflation it has been happily exporting the past several years. U.S. interest rates would skyrocket to levels last seen in the Civil War in order to preserve some value in new dollar investments. U.S. exports of services such as insurance, education, software, consulting, and banking could fare better, however, if priced in the new unit of account. The U.S., China, and Japan might unite in a closed dollar block to fend off the impact of the new Russian gold currency. But at best this would restrict world trade, and it seems more likely China and Japan would act in their self-interest and try to make peace with the new currency in terms of their own paper currencies. Gold-producing nations such as Australia, Canada, and South Africa might do relatively better than some others. Large gold-owning nations such as the U.S., U.K., and Germany might stabilize by joining the new world currency, but this is more likely to occur after suffering initial disruption rather than proactively guiding the process.

China could engage in its own attack on the U.S. economy quite apart from whether it chose to join Russia in the use of the gold standard based on a new unit of account or even lead such an effort itself. China's other line of attack runs through its voluminous holdings of U.S. Treasury debt (estimated to be approximately $1 trillion), and the need of the U.S. for China to continue to purchase new issues of such debt (likely to be $5 trillion or more taking into account base line deficits, temporary stimulus spending, new budget proposals, financial rescues [such as the Troubled Assets Relief Program (TARP), Term Asset-Backed Securities Loan Facility (TALF), Bear Stearns, General Motors, and others] and as yet unrealized losses and associated bailouts arising from new losses in credit cards, student loans, auto loans, corporate bonds, commercial real estate, and other nonsustainable credit). China could simply dump say $100 billion of its longest maturity U.S. Treasury securities on the market at one time combined with an announcement that it intended to sell far more when, as and if market conditions warranted. Such an action would cause an immediate and substantial rise in intermediate-to-long-term U.S. interest rates. This is the sector that is most relevant to mortgage and corporate credit (versus the short-term sector, which is more relevant to interbank lending and money market investments and other cash substitutes). This would further weaken the already weak housing and manufacturing sectors and likely cause a substantial increase in U.S. unemployment, home foreclosures, bank failures, and corporate bankruptcies. The end result would be to force the economy into an unpalatable choice between hyperinflation and protracted economic decline resembling the Great Depression, perhaps worse.

The conventional objection to such action on the part of the Chinese is that they would hurt the value of their own securities and incur massive losses on their portfolio holdings. This objection is intellectually and analytically shallow. Portfolio investors may choose to view their holdings as held to maturity or held for trading. It is true that if China were to attempt to liquidate holdings beyond the initial $100 billion suggested in the preceding scenario, they would receive substantially less than par value and thereby realize capital losses. However, China is under no such constraint and can simply hold onto its securities until maturity and receive all coupons and 100 percent of principal at maturity thereby suffering no losses beyond those incurred on the initial $100 billion. One way to understand this is to think of a homeowner with no mortgage whose house has declined in value. If he intends to sell immediately to move to another city, the decline in value may convert into a realized capital loss. However, if he intends to remain in his home for the rest of his lifetime, the temporary decline in value is a financial artifact of no particular consequence. The Chinese are like the homeowner who intends to stay in his home forever. By operating through the marginal transaction (in a manner similar to that in which the Russians might operate in gold) they can affect the global term structure of interest rates without suffering actual capital losses beyond those incurred to move the market in the first instance. The announcement effect of the first sales backed by a credible threat to sell more will be enough to insure the semi-permanence of increased intermediate term U.S. interest rates.

A second standard objection to this course is that China would suffer from decreased exports to the U.S. if they caused the U.S. economy to collapse in this manner. However, China may find this an opportune time to stimulate internal domestic demand and convert its economy from an export-led model to a consumption-led model relying on internal markets to increase consumption.

Another more subtle but equally effective tactic the Chinese might employ is to move down the yield curve. This is done by maintaining total Treasury holdings constant but allowing older long-dated notes to mature and then reinvesting proceeds in shorter maturities. For example, China has a certain amount of U.S. Treasury five-year notes it purchased in 2004 and which are maturing in 2009. When those notes mature this year, China can choose to reinvest in one-year Treasury bills instead of notes with longer maturities. By doing so repeatedly, China will greatly shorten the maturity structure of its overall portfolio. This will give China greater liquidity and optionality in how it deploys its cash in future (because its bills will always be close to maturity so it can redeploy cash-at-maturity without selling or dumping anything). This will also steepen the yield curve (meaning shorter maturities where demand is greatest will have lower interest rates and longer maturities where demand is less will have higher interest rates, ceteris paribus, thus increasing the differential between short-term and long-term rates represented as a steeper slope on a yield curve graph). This will cause higher interest rates for mortgages and corporate debt in the U.S. without causing capital losses in China since the effect will be achieved incrementally through the continual rollover process rather than through abrupt dumping. This is the interest rate equivalent of the death by a thousand cuts.

In summary, a well-timed and well-executed attack on the U.S. Treasury securities market could result in a devastated U.S. economy facing depression or hyperinflation while China suffers very modest capital losses and continues to grow its economy with less reliance on exports to the U.S.

The destruction of the dollar through Russian unilateral issuance of a new gold-backed reserve currency and the destruction of the U.S. economy through China's investment policies are the twin towers of external threats to the U.S. national security by economic means.

"The U.S. is well prepared from a statutory and regulatory perspective to protect its national security interests from foreign control and dissemination to foreign parties including adversary firms and investment pools. . . . However, no set of laws is proof against deliberate, malicious, and well-considered efforts to defeat or evade them, especially if the objective is not the acquisition and control of a particular company or technology but disruption of critical infrastructure including the financial system itself."

NATIONAL RESPONSES

Despite the range of potential national security threats posed by adversaries and the diverse methods and immense resources at their disposal, investee nations such as the U.S. and others are not without considerable tools at their disposal to deter, detect, and defend against hostile or subversive actions by adversaries. This section begins with an overview of U.S. legal and financial defenses.

The first line of defense for the U.S. is the Exon-Florio Amendment to the Defense Production Act of 1950, which permits voluntary review of foreign investments in the U.S. by the Committee on Foreign Investment in the U.S. (CFIUS), a 13-member interagency body chaired by the U.S. Treasury and with Cabinet-level participation from Treasury, Commerce, Defense, State, Homeland Security, the Attorney General, Office of Management and Budget, Council of Economic Advisors, Office of the U.S. Trade Representative, National Economic Council, National Security Council, Department of Energy, and the Office of Science and Technology Policy. The Director of National Intelligence and the Secretary of Labor are also nonvoting ex officio members. Exon-Florio and the role of CFIUS were recently amended and expanded through the Foreign Investment and National Security Act of 2007 (FINSA) and an amendment to Executive Order 11858 issued on 23 January 2008.

FINSA continues to allow for voluntary filings by foreign entities acquiring U.S. companies but also allows CFIUS to institute reviews on its own initiative. FINSA applies to “covered transactions” defined as those involving a merger, acquisition, or takeover of a U.S. company, which could result in foreign control of that company. Current regulations use 10 percent ownership as a threshold for control; however, it is not clear that this is the only indicia, and it has been urged that other indicia should expressly be adopted. Once a review has commenced, CFIUS has 30 days within which to determine either that no threat to national security exists or that any potential threat has been mitigated through agreement with the parties. If, after 30 days, it is determined that a threat to national security does exist and no satisfactory mitigation has been achieved, the transaction moves to a 45-day investigation at the end of which CFIUS provides a written report and recommendation to the President of the U.S. who has an additional 15 days to decide whether to suspend or prohibit the proposed transaction. However, acquisitions by Sovereign Wealth Funds (SWFs) or other entities controlled by foreign governments and acquisitions by any party of critical infrastructure will automatically attract the 45-day investigation, subject to certain narrow exceptions. FINSA also contains provisions relating to withdrawals from proposed acquisitions, reports to Congress and criteria for determining both threats to national security and the definition of critical infrastructure. The Director of National Intelligence is given the role of coordinating the input and analysis of all members of the Intelligence Community in support of CFIUS's role in evaluating threats to national security. A complete examination of the FINSA and CFIUS processes is beyond the scope of this paper although excellent resources on this subject are available. Instead, it suffices to say that CFIUS has been a powerful and high-precision tool for protecting U.S. national security interests while at the same time allowing the vast majority of proposed acquisitions to proceed (often with enforceable mitigation agreements) so as to maintain the U.S.'s reputation for open and nondiscriminatory capital markets.

However, CFIUS is far from the only tool the U.S. has at its disposal to monitor unfair or dangerous activities in U.S. capital markets and the market for control of U.S. companies and critical infrastructure. A brief overview of these resources follows.

Securities Law

The U.S. has a comprehensive set of laws governing securities, futures, and derivatives transactions contained in the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Advisers Act of 1940, the Investment Company Act of 1940, the Commodity Exchange Act, and other acts all as amended to date. While even a superficial overview of all of these statutes and provisions is beyond the scope of this paper, it can be noted that these statutes all contain robust antifraud provisions and reporting provisions governing such matters as takeovers; 5 percent or greater positions; licensing of advisers, brokers, and exchanges; large trader reports; large position reports; margin requirements; reporting of purchases and sales by company officers and directors; short sales; fiduciary duties; conflicts of interest; and many other matters designed generally to provide fair, efficient, and transparent markets. The laws, rules, and regulations are implemented by large staffs at the Securities Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) dedicated to market supervision including delegated authority to exchanges and their self-regulatory organizations. Enforcement is supported through SEC and CFTC investigatory and subpoena power; administrative judges; and access to the resources of the Federal Courts, Federal Bureau of Investigation (FBI), and the Department of Justice as needed. Importantly, these rules (with few exceptions) apply equally to adversaries with regard to their transactions in U.S. markets, with U.S. counterparties, or through means of U.S. interstate commerce. However, as noted before, where adversary investment pools and their home countries do not cooperate in investigations or allow access to information, enforcement of these rules against adversaries can be problematic.

Banking Law

Financial institutions such as banks and thrifts are subject to extensive regulation and oversight in addition to that which may be conducted by the SEC with respect to trading in the public securities of these institutions. The U.S. has numerous bank, thrift, and bank holding company statutes and multiple regulatory bodies to enforce these including the Board of Governors of the Federal Reserve System, the Office of the Controller of the Currency, and the Office of Thrift Supervision among others. The principal statute that would govern adversary firm acquisition of banks or thrifts is the Bank Holding Company Act of 1956 as amended by the Gramm-Leach-Bliley Act (1999). These statutes require regulatory filings and approval when certain investments in financial institutions exceed 5 percent and have other progressively more onerous requirements at ownership levels in excess of 19.9 percent and 24.9 percent. Depending on the exact type of instruments, voting rights, and contractual arrangements involved, these thresholds can be deemed to constitute "control" and are prohibited to acquirers engaged in nonbanking commercial activities (which adversary investment pools would certainly be deemed to be). Separate review processes are applied to foreign acquirers having to do with banking regulation in their home countries. As a practical matter, no adversary could legally obtain control of a U.S. bank under these statutes.

Antitrust Law

The twin pillars of antitrust law are the Sherman Antitrust Act of 1890, which outlaws contracts or conspiracies, ". . . in restraint of trade or commerce . . ." and the Clayton Antitrust Act of 1914, which outlaws certain kinds of price discrimination, exclusive dealings, mergers that lessen competition, and directors serving on the boards of two or more competing companies. In addition, the Hart-Scott-Rodino Antitrust Improvements Act of 1976 amends the Clayton Act to provide for advance notification of certain mergers, tender offers, and acquisitions and requires a 30-day waiting period after notice and before closing during which regulatory agencies (Federal Trade Commission and Department of Justice) may request further information in order to evaluate whether the proposed transaction violates any antitrust laws. It is fair to say that many adversary investment pool transactions in Latin America, Africa, and Asia would violate U.S. antitrust laws if conducted subject to the jurisdiction of the U.S.; i.e., certain acquisitions are done precisely for the purpose of price discrimination, exclusive dealings, to establish interlocking directorates, etc. The fact that these laws exist [and that similar laws exist in the European Union (EU)] acts as a powerful check on certain abuses against fair trade that might be pursued by an adversary but for these laws.

Export Administration Act

The Export Administration Act (EAA), which has been reauthorized and amended several times since its origin in 1949, establishes statutory authority and an administrative framework for regulating exports of dual-use or sensitive commodities, software, hardware, and information technology. The traditional bases for such restrictions were to prevent scarcity in the U.S., to implement or support the foreign policy of the U.S. (including broad-based goals such as human rights), and to prevent the export of goods with military applications to countries that posed a threat to U.S. national security. While the EAA is a first line of defense from the perspective of U.S. exporters and commodity producers, it is a kind of "second line of defense" after CFIUS from the perspective of adversary firms and investment pools. While CFIUS prevents acquisitions of sensitive U.S. technology by foreign buyers in the first instance, EAA can prevent target companies controlled by adversaries from exporting sensitive technology if the target acquisition had somehow escaped CFIUS intervention.

Tax Law

The implications of U.S. taxation on foreign investors in U.S. capital markets is perhaps one of the least understood and most underappreciated tools in the U.S. arsenal of legal defenses to hostile actions by adversaries. As in the case of securities laws discussed above, the field is too large and complex to be adequately summarized within the scope of this paper. However, an overview of one particularly fraught area might be helpful in explaining what a powerful tool this can be. In general, U.S. citizens, U.S. permanent residents, and U.S. corporations pay U.S. income tax on global income regardless of where their assets are owned or activities are performed. Nonresident foreign persons, including adversary country firms and investment pools, generally do not pay U.S. taxes except to the extent that they are considered to be engaged in a trade or business in the U.S. or except for certain withholding taxes on payments of interest, dividends, royalties, and other recurring items from U.S. sources. This begs the question of which activities do or do not constitute being engaged in a U.S. trade or business. Generally, the purchase and sale of securities and derivatives, including through U.S. based agents, without more, will not subject an adversary firm or investment pools to U.S. taxation (known as the securities trading safe harbor). However, some adversary firms may have been overly aggressive with respect to the safe harbor and may have exercised undue control with respect to U.S. business activities or have become involved in loan origination, purchase, and sale activities that may not qualify for safe harbor treatment. In addition, some adversary firms are known to have arranged total return equity swaps with major investment banks so that they receive the economic benefit of dividends paid on underlying shares without suffering U.S. dividend withholding taxes since they purport not to own the shares themselves. To the extent these activities may constitute improper tax avoidance or illegal tax evasion, the adversary firms and investment pools, upon IRS audit and possible referral to the Department of Justice, may face back taxes, late interest, fines, penalties, and imprisonment in this regard. These tools should not be employed lightly, but they are powerful antidotes to certain overly aggressive investment techniques by adversaries.

International Emergency Economic Powers Act of 1977 (IEEPA)

IEEPA is sometimes referred to as the "nuclear option" of financial regulation and not without cause. IEEPA allows the President of the U.S. to block transactions, freeze accounts, order embargoes, and confiscate assets in connection with any unusual and extraordinary threat to the national security, foreign policy, or economy of the U.S. that originates in whole or substantial part outside the U.S. The act does require reporting to Congress and further requires that declared emergencies be renewed annually to remain in effect; Congress may also terminate emergencies under certain circumstances. Notwithstanding these reporting and termination provisions, the powers granted to the President to deal with economic or national security emergencies caused by actions of adversaries are near plenary. The U.S. has, in fact, used these powers many times in the past and has well-established Executive Branch processes and procedures involving the Departments of Treasury, State, Justice, and other departments and offices for the implementation and enforcement of any executive orders pursuant to IEEPA.

Other Statutes and Regulations

In addition to the foregoing, there are numerous Federal and State statutes and government agency regulations that limit the ability of foreign owners—including adversaries—to acquire interests in companies involved in particular industries including telecommunications, shipping, and casinos among others. Importantly, the U.S. defense industry operates pursuant to the National Industrial Security Program Operating Manual, which governs access of all defense contractors to classified material and which imposes stringent limitations on the access of foreign officers, directors, and shareholders to any such information.

In short, the U.S. is well prepared from a statutory and regulatory perspective to protect its national security interests from foreign control and dissemination to foreign parties including adversary firms and investment pools. The U.S. also has seasoned and well-staffed agencies and private sector partners to provide oversight and enforcement with respect to those laws, regulations, and processes. However, enforcement of those rules abroad in the host countries of adversaries can be problematic, especially if those countries refuse cooperation. No set of laws is proof against deliberate, malicious, and well-considered efforts to defeat or evade them, especially if the objective is not the acquisition and control of a particular company or technology but disruption of critical infrastructure including the financial system itself. Defense against this type of activity requires a thorough understanding of the techniques that might be employed, portfolio metrics to assist in identifying situations where adversary behavior might be other than commercial investment management, development of a matrix of indications and warnings, and sound intelligence and analysis with respect to the intentions and actions of adversaries.

FINANCIAL "CHOKE POINTS" AND CLANDESTINE ACTION

In addition to the overt national and multilateral policy tools described in the preceding sections, the U.S. can employ clandestine collections to obtain the information it needs to ascertain if adversary intentions are commercial or malign and to penetrate and disrupt those efforts that may be malign. In order to do so, it is critical to understand the financial and legal “choke points,” which exercise the same influence in the commercial world as critical straits such as Hormuz and Suez do in the world of maritime commerce and naval warfare.

Complex financial transactions do not occur in a vacuum. Adversaries must have professional advisers and transactional counterparties in order to pursue their trading and investment objectives. It follows that those advisers and counterparties have information on adversary investment positions and structures at least to the extent they are conducted in conjunction with that adviser. Adversaries require the use of legal entities, derivative contracts, trust agreements, account agreements, and numerous other formational and contractual documents. In addition, local officials will insist on minimal corporate formalities and periodic financial statements even in those jurisdictions most lax in this regard.

While these opaque structures may be initiated by adversaries, they are enabled by a legion of lawyers, accountants, bankers, dealers, administrators, and others. These professionals typically operate within professional firms; however, some may act as sole practitioners or as small “boutiques” particularly in offshore banking jurisdictions and tax havens such as Cyprus or the Cayman Islands. These professionals not only perform indispensable services, they may take the lead in suggesting the structures and techniques described herein. Portfolio managers and government agents at adversary funds may have goals in mind (e.g., “we’d like to exert de facto control of Company X without our interests becoming transparent, reportable, or easily traced”). It is often not difficult to invent what are superficially commercial reasons for such requests; however, professionals are often indifferent to the initiating party’s motivations and will simply execute the request. As a result, the professionals—particularly lawyers and accountants—will be the most likely parties to structure opaque transactions. It follows that they will have the greatest knowledge about the actual parties in interest and the intricacies of the structures.

It is also typical that *lawyers* act in "teams" or "tiers" with major law firms in financial centers (e.g., Hong Kong, London, Geneva, New York) devising the high-level structures, and smaller law firms in offshore jurisdictions (e.g., Macao, Cyprus, Cayman) providing the entity formations and corporate formalities associated with the structures. Therefore, while the "offshore lawyers" may not be responsible for the structures in the first instance, they will have almost complete knowledge of such structures as a matter of necessity. This makes offshore law firms potentially a highly attractive target for clandestine collections because their operational security may be less stringent than that of their colleagues in major cities while their information may be just as good.

The analysis with regard to *accountants* is similar; i.e., they work in teams based both in major cities and offshore jurisdictions with the financial center professionals taking the lead, and their offshore colleagues providing hands-on implementation. Accountants may not be involved at the start in creating complex structures but tend to be more involved over the life of the structure. Lawyers are typically intensely involved at the launch of a project but then provide only minimal or routine maintenance services thereafter, whereas accountants are less involved at the launch but far more involved with quarterly, annual, and special financial reporting and tax accounting thereafter. Accountants do not merely "rubber stamp" management financials but are required to perform numerous tests with regard to their accuracy and therefore have extraordinary access to bank account information, wire transfers, brokerage portfolio statements, expense records, etc. Accountants are expected to devise and initiate their information requests, which are not confined only to those matters that management wishes to reveal.

Another critical service provider in these structures, perhaps less well known than accountants and lawyers, is the *offshore director*. Corporate entities are required to have boards of directors that nominally control the activities of the company. Since many such entities used in financial structures are located in offshore jurisdictions, it is typically practical and convenient to recruit one or several local professionals to serve in the capacity of director (while the real party in interest retains control of the stock and can "fire" the board practically at will). Local professionals provide such services for a modest fee—a practice sometimes referred to derisively as "rent-a-director." Because professionals on island jurisdictions are often in short supply relative to the tens of thousands of legal formations, it is not unusual for a single individual to serve on the boards of hundreds of special-purpose entities. Recruiting one or more of these individuals in each of several offshore jurisdictions is therefore potentially an abundant source of information about the real parties in interest in structured finance.

One of the most critical information nodes in offshore structured finance is the fund *administrator*. All hedge funds and other structured investment vehicles periodically report performance results to their investors (n.b., many of the opaque structures described in this paper posit nonadversary investors existing side-by-side with adversary investors in otherwise legitimate structures, notwithstanding that adversaries may seek to exert undue influence via the structure and their intimate relationships with the fund managers). While managers routinely calculate their performance gain or loss since the prior reporting period, investors require an independent valuation as a matter of best practice and as a control on the manager. This valuation is provided by the administrator (who typically performs other duties such as the receipt of funds, payment of redemptions via wire transfer, and review of subscription documents and redemption requests). There are relatively few major administrators (about 20 major providers globally) in comparison with perhaps 10,000 hedge and private equity funds. As a result, each administrator handles accounts for thousands of funds. These administrators have even more detailed information than accountants and lawyers including (a) investor names, address, and other contact details including e-mail addresses, which include Internet domain names; (b) complete position information; (c) complete transaction information; (d) account information on sending and receiving banks; and (e) information on the timing and amount of cash transfers (both investor related and transaction related). Penetration of key fund administrators is perhaps the richest single source of information on private fund activity.

Registrars are another valuable source of information; however, they are limited to maintaining lists of investor names and contacts and do not typically have the detailed transactional information possessed by administrators.

Finally, *dealers* and *brokers* (which come in many forms including investment banks, commercial banks, market-makers, and other types) will have complete information on those transactions they conduct with private funds. Dealers will not have the "bird's eye view" that administrators, lawyers, and accountants may possess, but they will have detailed transactional information on those purchases, sales, positions, swaps, net payments, and other elements of each trade conducted with themselves. Dealers and banks also act as repositories of the actual holdings of SWFs so they will hold, typically in book entry form (i.e., noncertificated), the actual stocks, bonds, cash, and other claims of the adversary investment pool. Large institutional customers such as SWFs typically have numerous brokers (for various purposes including regional and area expertise of certain firms and the ability to spread trades around so no single dealer knows the totality of a SWF's positions). A particular type of broker known as the "prime broker" will have far more information than any single broker. A prime broker is, in effect, a clearinghouse for numerous transactional brokers each of whom "gives up" its trades at the end of the trading day to the prime broker for purposes of reconciliation, netting, clearance and settlement with the SWF customer. Large prime brokers are probably second only to administrators in terms of the detailed information they possess on SWF trading and investment positions.

Each of the foregoing types of entities therefore acts as a "financial choke point" at least with respect to financial information traffic passing through their hands. While professional and financial firms do use standard techniques of operational security including limited access, biometric scanners, passwords, and need-to-know protocols, these are typically not as stringent as the operations security (OPSEC) used in the intelligence community. In particular, a culture that discourages "social engineering" in intelligence work does not exist in the worlds of law, accounting, and finance, and dedicated counterintelligence resources are not nearly as robust. As a result, it is possible for a single well-placed professional within one of these firms to obtain access to a wide array of information without raising undue suspicion. This is even more the case in the offshore financial centers than in the large money centers where standards are more relaxed and the choke points are even narrower (i.e., there are very large volumes of transactions concentrated in the hands of relatively few law, accounting, and administration firms).

For example, in a leading offshore finance jurisdiction, the Cayman Islands, there are perhaps 15 law firms that handle more than 90 percent of the transactional work. Of these, two firms, Walkers and Maples, handle about 50 percent. A source at one law firm can have good information about transactions at a rival law firm to the extent that the rival firm is representing the "other side" of a single transaction. Therefore, a single agent-in-place at a firm like Walkers with enough seniority and professional stature would be in a position to obtain a material percentage of all the legal information on real parties in interest to otherwise opaque structured financial transactions. The same phenomena would exist, perhaps in more concentrated form, in smaller jurisdictions such as the Channel Islands or Cyprus.

In short, recruitment of agents among the ranks of professionals in law, accounting, and administration firms as well as banks, brokers, and dealers, particularly in offshore jurisdictions, is an opportunity nonpareil to penetrate the opaque and complex structures described elsewhere in this paper for the purpose of ascertaining the true positions and intentions of the adversary investment pool. Of course, such human intelligence (HUMINT) activities can be greatly supplemented and enriched by a host of technical means targeted on these same professional and financial firms.

CONCLUSION

Notwithstanding an earlier period of globalization during 1880–1914, there can be little doubt that the current period of globalization from 1989–2009, beginning with the fall of the Soviet Union and the end of the Cold War, represents the highest degree of interconnectedness of the global system of finance, capital, and banking the world has ever seen. Despite obvious advantages in terms of global capital mobility facilitating productivity and the utilization of labor on an unprecedented scale, there are hidden dangers and second-order costs embedded in the sheer scale and complexity of the system. These costs have begun to be realized in the financial crisis that began in late 2007 and have continued until this writing and will continue beyond.

Among the emergent properties of this complexity are exponentially greater risks of catastrophic collapse leading to the complete insolvency of the global financial system. This dynamic has already begun to play out and will continue without the implementation of appropriate public policies, which, so far, are not in evidence. More to the point, this ongoing instability lends itself to amplification through the actions of adversaries who can accelerate destabilizing trends through market manipulation and the conduct of marginal transactions in critical securities and commodities such as U.S. Treasury debt, oil, and gold.

The U.S. response should include three components:

- Improved public policy to stabilize the system including temporary nationalization of banks to remove bad assets, preemptive study and consideration of a return to the gold standard, higher interest rates to support the value of the U.S. dollar, increased tolerance of failure in financial institutions to reduce moral hazard, and mandatory use of central counterparty clearing in order to mitigate the impact of institutional failure and descale the system to make it more robust to attack.
- An expert market watch function and all source fusion with improved financial counterintelligence and clandestine

action to detect and disrupt attempted malicious acts in global capital markets by adversaries.

- An offensive capability in global capital markets including asset freezes, asset seizures, and preemptive market manipulations.

Finally, the vulnerability of companies and technologies to control and diversion by adversaries must not be overlooked. This requires improved interagency coordination of the various legal and forensic tools at the disposal of the U.S. in the areas of securities, antitrust, tax, banking, export restrictions, direct foreign investment restrictions, sanctions, and emergency economic powers. These tools should be supplemented by improved financial counterintelligence and new automated tools focused on supply-chain linkages, nonobvious relationship awareness (NORA), and market price anomalies.

REFERENCES

1. Rickards, James G. (2009), "A New Risk Management Model for Wall Street," The RMA Journal – The Journal of Enterprise Risk Management, March 2009, 20–24.
2. Cogan, John F., Cwik, Tobias, Taylor, John, B. and Wieland, Volker, New Keynesian versus Old Keynesian Government Spending Multipliers, February, 2009: www.volkerwieland.com/docs/CCTW percent20Mar percent202.pdf.
3. Taleb, Nassim Nicholas, The Black Swan: The Impact of the Highly Improbable, New York, Random House, 2007.
4. Bak, Per, How Nature Works: The Science of Self-Organized Criticality, Copernicus, New York, 1996.
5. Scheinkman, José A., Woodford, Michael, "Self-Organized Criticality and Economic Fluctuations," The American Economic Review, Vol. 84, No. 2, pp. 417–421 (May 1994).
6. Lam, Lui, Nonlinear Physics for Beginners – Fractals, Chaos, Solitons, Pattern Formation, Cellular Automata and Complex Systems, World Scientific, Singapore, 1998.
7. Mandelbrot, Benoit and Hudson, Richard L., The (Mis)behavior of Markets: A Fractal View of Risk, Ruin and Reward. New York, Basic Books, 2004.

8. Peters, Edgar E., Chaos and Order in the Capital Markets, New York, John Wiley & Sons, Inc., 1991.

9. New York Times, "Growth of a Complex Market," October 9, 2008: http://www.nytimes.com/imagepages/2008/10/09/business/09greenspan.graphix.ready.html.

10. Eichengreen, Barry, Golden Fetters, The Gold Standard and the Great Depression 1919-1939, New York, Oxford University Press, 1995.

11. Ahamed, Liaquat, Lords of Finance, The Bankers Who Broke the World, New York, Penguin Press, 2009.

1.5 RESILIENCY IN THE FACE OF UNRESTRICTED WARFARE ATTACKS

Stephen Flynn

INTRODUCTION

I think it falls to me, as a part of this conference, to essentially speak to what I have been arguing now for many years is the missing-in-action component of our whole approach to dealing with the terrorism risk and what we are really doing here on the home front and specifically beyond the federal government to better prepare the American people and ultimately our society and all the critical foundations of that society for dealing with terrorism as an ongoing concern. It is missing largely because we made some strategic choices directly after 9/11 that we are going to take this battle to the enemy overseas. That was supposed to lead us to some sort of victory at some point in time.

There was also, I would argue, a false underlying assumption, which is that there is not really anything that can be done that is meaningful to deal with the homeland security dimension. Terrorists cannot be deterred, and the only victory we could

Dr. Stephen Flynn is the Ira A. Lipman Senior Fellow for Counterterrorism and National Security Studies at the Council on Foreign Relations. Following the election of President Barack Obama, he served as the Lead Policy Advisor on homeland security for the Presidential Transition Team. He is the author of the critically acclaimed The Edge of Disaster: Rebuilding a Resilient Nation (Random House, 2007) and national bestseller, America the Vulnerable (HarperCollins, 2004). He ranks among the world's most widely cited experts on homeland security issues, including providing congressional testimony on 22 occasions since 9/11. He holds a Ph.D. and M.A.L.D. from the Fletcher School of Law and Diplomacy and a bachelor's degree from the U.S. Coast Guard Academy.

expect to have is be able to effectively hunt and destroy these folks and deter those who would sponsor them.

Today, I will try to make the case that I think we are getting that wrong and how important it is for this community to begin to push the envelope of thinking about how things that are talked about at symposia like this can find a way to a more broader conversation around our country about being able to deal with this ongoing issue. I want to make a case for why I think that is both practical and essential for going forward.

THE DAMRELL STORY

Let me begin with a story that I think captures part of the reason why groups like this have a difficult time doing what I am prescribing. The story actually pulls us back more than a century, and it played out in an area not far from where I was born in Salem, Massachusetts. It was the City of Boston. The time was November 1872. It was one year after the great Chicago fire in which we had what would become the second largest urban fire in America playing out in the City of Boston. Unlike in the case of Chicago, Boston did not burn to the ground.

The story is an extraordinary one, primarily because it features a man who deserves a lot more attention than he has probably received by history. His name was John Damrell. He was a Chief Fire Engineer. Back then, they began to professionalize the fire departments primarily because of the steam engines that were used in the pump car capacity. Early on, the engineering was a little bit shaky. The old volunteer firemen, we still have traditions of this up in New England, generally start with drinking beer in large quantities, moving a pump car out, and then racing another team to see who can make the water go farthest. Back in the early parts of our early fire fighting history, there was a race to see which fire company could get there first. Actually, putting out the fire was an entirely incidental part of this contest. This could be fairly nasty stuff. In any event, it was kind of an amateur hour operation. However, when they actually came up with the boiler steam plants, they would literally blow up.

So having drunken people work the fires required movement toward professionalization. That is why they were called fire engineers, and the other firemen elected the chief engineer. John Damrell was the first fire chief engineer in Boston's history. He was a man who, right after the great Chicago fire got onto the early trains, went off to Chicago and wanted to find out how this happened. He came back from that with a whole series of recommendations that he made to the city burgers about what could be done in Boston to prevent a similar fire.

Buildings were getting high. The water pressure was not keeping pace. So you might have to think basically about pipes. The kinds of materials that were being stored in places were going to cause problems if you had an addition source and so forth. Basically, they went through a series of recommendations. The city burgers thanked him and ushered him out the door.

A year later, the fire started. As many of these things that turn into a real disaster, many variables come together at once. In this case, it started in the commercial area after hours. The alarm did not go off right away. It was on the corner of Summer Street and Kimball Street. When the alarm was finally set off, Damrell got there in eight minutes, and he knew, because something else was going on at the same time, that he had a serious situation. The fire was clearly growing very quickly.

The other corresponding event was that there had been an equestrian flu pandemic that had broken out first in Toronto and had come down the Eastern seaboard. This was a real problem in the 19th Century because every single workhorse was down for the count. Basically, if they pulled anything, they would roll over and die.

That meant those heavy pump cars would have to be pulled by men over the cobblestone streets. We knew this was not going to be quite as nimble of a response as what they had trained for. As the fire unfolded, within an hour, he did something that had never been done before. He ordered a telegraph sent out to all the surrounding communities that said, "Boston is on fire. Send help." Then in terms of the actual approach to the firefighting, he figured out that what he was going to have to do was write off the commercial district because he needed the space or the main public squares and to concentrate the water and the manpower he had. He also had tugs and fireboats on the waterfront to protect the wharfs and the ships.

Now, you can imagine how the city merchants felt about this. Yeah, we are just going to write off the merchant part of the city. Somehow or another, he navigated through all that. It was truly all hands evolution. Basically, every able-bodied man in Boston was out there, and they hauled out mattresses and blankets and wetted them down to drape them on the roofs of the old South Church and the surrounding parameter they had identified. The manual labor of doing this under the circumstance was absolutely extraordinary.

"Having drunken people work the fires soon required a movement toward professionalization. That is why they were called fire engineers."

The fire broke out at 8:00 p.m. and when the people were long beyond what they should have been, the bounds of endurance, at 5:00 a.m. the next morning, the trains started rolling in from New Haven, Connecticut; Newport, Rhode Island; and Biddeford, Maine. In Wakefield, Massachusetts, they ran the 12 mi from Wakefield to Boston with a pump car. Those reinforcements made all the difference in essentially holding the fire line, and as a result, Boston was saved.

What I think is extraordinary about this story, and something that this community should really take to heart, is Damrell really did something early on in that incident that was largely an unnatural act for professionals. He gave an open ended call for help. Instead of saying, we have got this under control. What you have been paying us to do all this time here is manage this threat. He recognized that the threat was clearly something that was going to transcend the professionals' capacity to handle. Early on, he asked for help.

Of course, the other extraordinary part of this story is after having asked, he was overwhelmed by the kind of help that he received. That help really made the difference. Now, flashback to 1872 and imagine what this was like. There was no electricity operating then. People usually went to bed when it got dark. This was November. The church bells would have to go off. People would have to get the alarm. Boston is on fire; we have got to mobilize. The pump trucks would have had to be run down to train stations, put on the railheads, and then rolled into the city. All that happened within that short space of time.

It gives us pause when we think about the kind of resilience we have as a people now when a hurricane rolls through and people are in a queue looking for a bottle of water within six hours is about the kind of resilience that we had back then and, I would argue, the kind of resilience that we need to aspire to reclaim going forward.

The other great part of the Damrell story is actually what happened a year later. He retired as the Chief Fire Engineer and became the Chief Building Inspector for the City of Boston. What he did in that capacity, and borrowing on the national fame that he acquired having led the charge in this fire, was rope in his fellow chief firemen, architects, insurers, and builders and created for us our national fire code that has saved all our cities ever since.

Rather than just be the gung-ho firefighter that he was, he made the systemic investment to deal with the issue of a fire as an ongoing concern and asked, "How do we make this essentially something that we cannot eliminate but can mitigate to the point that we have never seen something like what he experienced in Boston and what the folks in Chicago experienced, a firestorm that consumes an entire urban area."

I would argue that those are two very compelling bits of narrative for what should inform how we approach the counterterrorism issue. We need to be much more open-ended in asking for help, not just restricting it to the professionals. We also need to really think about how we deal with terrorism as essentially an ongoing hazard, something we will never successfully eliminate, but we can clearly, effectively mitigate to a point where it does not have strategic consequences for our nation and ideally minimizes the loss of life risk and the economic cost risk of having it being unbounded.

FACING UP TO DISASTER

Is homeland security still on the nation's radar screen? One can be excused for wondering. After all, we are heading toward the eighth anniversary of the 9/11 attacks and so far al Qaeda has yet to strike us again. The Technicolor national threat level has been frozen at "yellow" since January 2004, and the new Secretary of Homeland Security, former Arizona Governor Janet Napolitano, has mused aloud that maybe it should be abandoned altogether. The issue was missing-in-action during the marathon 2008 presidential campaign. The presidential transition then came and went without the Obama Administration publicly outlining its plans for the homeland security mission, and there were no chest-pounding displays of dismay on editorial pages or by media pundits. Indeed, the only media spark Secretary Napolitano has managed to generate during the early days of her tenure arose from something she *did not* do: She omitted the word "terrorism" from her prepared testimony before Congress on 25 February 2009.

"Is homeland security still on the nation's radar screen?"

So at first blush it seems as though an issue that consumed the entire country's attention just a half dozen years ago somehow left Washington in one of former President George W. Bush's White House moving boxes. But that is not the case: The Bush team's counterterrorism and homeland security legacy constitutes a political landmine for President Barack Obama with the detonator set in Bush's farewell address and exit interviews that proclaimed as his one, indisputable accomplishment that since 9/11, Americans had been kept safe from acts of terrorism on his/her watch. The implicit message was that President Obama would place the nation at risk if he did not embrace and build on the measures Bush had put in place.

Lest the message be lost in the celebratory din of the Obama inauguration, former Vice President Dick Cheney made it explicit in a 4 February 2009 interview with *Politico* [1]. He argued that there is a "high probability" that terrorists will attempt to deploy a nuclear weapon or biological agent in a major American city, and warned that policy changes leading away from the methods by which the Bush Administration combated terrorism would bolster the likelihood of a terrorist success.

So far, the Bush-Cheney parting shots have gone unanswered. Now that he is in the Oval Office, President Obama is not inclined to devote energy sparring with its former occupant, focusing instead on pressing matters like Iraq, Afghanistan, and the economic crisis. Nevertheless, as the new Obama team settles in, they will soon find that the homeland security situation is no less a mess. Contrary to the public impression that the Bush Administration worked hard to convey, there is no carefully constructed apparatus for keeping America safe. Rather, what the Obama Administration has inherited is a flimsy facade of homeland security, behind which lies a deeply flawed strategy, a badly broken Department of Homeland Security (DHS), and a nation that remains dangerously unprepared to respond to large-scale catastrophic events. If put to a serious test, the homeland security system will fail, and the political consequences for the Obama presidency could be disastrous—to say nothing about the consequences of failure for America. The White House needs to act aggressively to bridge the gap between the Bush Administration's valedictory rhetoric and the reality of America's ongoing vulnerabilities to terrorism and natural disasters.

THE NEGLECTED HOMEFRONT

In December 2008, Jeffrey Rosen penned an in-depth look at the DHS for *The New Republic* entitled, "Man-Made Disaster" [2]. Almost needless to say, Rosen's conclusion was a damning one. After conducting several interviews with outgoing Secretary of Homeland Security Michael Chertoff and chatting with security experts on both sides of the political divide (I was one of them), Rosen concluded that creating the Department was "a bureaucratic and philosophical mistake."

While there is still room for debate over whether DHS was a philosophical mistake, there is no question it has so far proven to be a bureaucratic failure. But this was inevitable since the Bush Administration was never seriously invested in making DHS an operational success. After the photo-ops accompanying its birth in November 2002, DHS was largely orphaned by the White House and Congress. Its headquarters today sprawls across the Nebraska Avenue Complex, a decrepit former U.S. Navy installation in Northwest Washington. One of my more memorable visits to this forlorn place was for a December 2005 meeting with then Deputy Secretary Michael Jackson. At the time, Jackson was the equivalent of the Chief Operating Officer of the third largest federal department in Washington. We were sitting in his office, a paragon of deferred maintenance, when our conversation was suddenly drowned out by a noise that sounded like a sledgehammer tearing into concrete pillars. Jackson apologetically explained that the noise actually came from a neighboring toilet that rattled the pipes violently whenever it was flushed.

Consigning the leadership of DHS to such moribund digs would have been a minor indignity if the Bush Administration had been truly committed to the homeland security mission. However, there are three reasons for its never making that commitment. First, the Administration's post-9/11 strategy was all about "taking the battle to the enemy." As Bush so often said, "We fight the terrorists overseas so that we don't have to fight them here at home." Not surprisingly, this translated into DHS having only a rearguard role in the war on terrorism. Even in that role it was essentially a bit player, since the lead for conducting domestic counterterrorism was assigned to the FBI, not DHS.

Second, the Bush Administration was wary that adding a new Cabinet department to the federal bureaucracy would draw criticism from conservative opponents of big government. At the same time, it worried that it might be outflanked on the homeland security issue by the opposition party since Senator Joseph Lieberman, a Democrat in good standing at the time, was getting considerable traction on Capitol Hill with his post-9/11 push to create DHS. The Bush White House decided that the best way to simultaneously neutralize Lieberman and potential conservative critics was to launch DHS as the government equivalent of a corporate merger, promising to extract savings by eliminating redundancies by folding the 22 preexisting agencies into one department.

One major consequence of this niggardly approach was to ensure that the leadership at the top of the department lacked the staffing or resources to carry out their advertised mission. Instead of recruiting a new cadre of career civil servants devoted to homeland security, the Administration instead manned DHS with short-term government contractors, and ordered DHS's operating agencies to loan out their senior managers on a one- and two-year assignment basis. To sweeten the deal for Republican partisans, top management slots were reserved for 300 political appointees—more than any other federal department has, including the Department of Defense. The result has been a revolving door of managers and support personnel: Today, less than one-quarter of the DHS headquarters staff has been there for more than two years.

Third, the Bush White House had no appetite for managing the complex and politically untidy interagency, state, local, and private sector issues that are part-and-parcel of the homeland security mission. Some 30 federal departments and agencies have been assigned specific responsibilities to support homeland security. For instance, the Pentagon has defined its niche as "homeland defense," for which it receives annual funding equal to roughly three-quarters of the total budget for DHS. Managing disease outbreaks falls to the Centers for Disease Control and Preventive within the Department of Health and Human Services. The Bush Administration also assigned the task of coordinating homeland security activities across the U.S. government—not to the DHS departmental leadership, but to a Homeland Security Council in the Executive Office of the President. But that council was never adequately staffed or empowered to manage the interagency process.

Messier still are the federalism and private sector equities that go with homeland security. By definition, the territorial U.S. homeland is the sum of 50 state jurisdictions. Additionally, within these states lies the nation's critical infrastructure, which is overwhelmingly owned and operated by private entities. These jurisdictional realities created ideological dissonance for the Bush Administration: If the federal government was to be fully mobilized to play an activist role in homeland security, it risked trampling on what has been traditionally state, local, or private sector turf. Their solution for this dilemma was to largely avoid these issues altogether. Instead of crafting new federal-state and private-public arrangements for protecting critical domestic assets and improving the nation's ability to respond to and recover from catastrophic events, the Bush Administration chose a "go-it-alone" strategy built around expanding the authority of intelligence to combat terrorist networks at home and abroad. Everyday Americans were essentially told, for their part, to keep traveling and go shopping.

President Bush's lackluster approach to homeland security largely went unnoticed by the American people. The wars in Iraq and Afghanistan, efforts to reform the intelligence community, and the treatment of detainees in Guantanamo Bay instead commanded the attention of official Washington and the media. Meanwhile, the ongoing vulnerability of the nation's critical infrastructure to 9/11-style attacks and the limited capacity of states and major cities to respond to man-made or major natural disasters remained out of the public eye—that is, until Hurricane Katrina roared ashore in late August 2005. Even in the wake of the debacle of New Orleans, Washington had the perfect scapegoat in the person of FEMA director Michael Brown. As a result, few thought seriously about how a nation supposedly on a war footing could have been so badly prepared to cope with a long-predicted catastrophic event that arrived onshore with plenty of notice.

In short, despite the rhetoric of the past seven years, when it comes to reducing America's exposure to the threat and consequences of terrorism within U.S. borders, there is not much "there," there behind the homeland security curtain. This places

President Obama in a perilous position. Since homeland security was not an issue in the campaign, the Bush Administration was never faulted for its neglect of the home front, and the American public believes we are safer than we really are. So when terrorists strike again, President Obama has been set up to be blamed for all the shortcomings that he has inherited.

". . . despite the rhetoric of the past seven years, when it comes to reducing America's exposure to the threat and consequences of terrorism within U.S. borders, there is not much "there" there, behind the homeland security curtain."

BUILDING NATIONAL RESILIENCE

What, then, should President Obama do to get out of this predicament? First, he needs to reject the Bush Administration's formulation that protecting Americans boils down to building a muscular national security apparatus that can do the dirty business of tracking down and destroying terrorists. Instead, the Obama Administration should embrace the lesson of United Airlines Flight 93, the hijackers' fourth plane, which crashed in a Pennsylvania field. That plane's passengers prevented al Qaeda from achieving its likely objective of striking the U.S. Capitol Building or the White House, and they did it without any help from the U.S. government. No Federal Air Marshals were aboard the aircraft. The Defense Department's North American Aerospace Defense Command could not intercept it; it did not even know the plane had been hijacked. It was instead private citizens who achieved the only verifiably foiled catastrophic terrorist attack on U.S. soil during the Bush Administration's eight-year tenure. It is both ironic and inspirational that the Legislative and Executive Branches of the U.S. government, whose constitutional duty is "to provide for the common defense" were themselves defended that day by an alert and heroic citizenry.

As the United Airlines Flight 93 story ought to make clear, it is shortsighted and counterproductive not to engage the American people in the enterprise of managing threats to the nation. As a stepping-off point, President Obama needs to publicly redefine the means and ends of the homeland security mission. He should use his considerable gifts of communication to recalibrate the American people's expectations of what the federal government can reasonably be expected to do. He should also challenge us to share in the responsibility of bolstering the nation's resilience in the face of all hazards, not just man-made ones. This will require him to be truthful in acknowledging that the threat of terrorism can never be fully eradicated, even as he makes clear that its risks and consequences can be successfully managed. Further, since 90 percent of Americans live in places that have a moderate to high risk of experiencing naturally occurring disasters, he should also focus the federal government on the task of improving emergency preparedness and building greater societal resilience. These are sound investments in our long-term safety and well-being even if terrorists never strike us again.

"One defeats terrorist tactics by working to minimize terror, which arises from a feeling of unbounded vulnerability and powerlessness. By empowering people to think and cope with disasters, they will be less afraid when things do go wrong—which of course will happen from time to time. It really is as simple as that."

Resilience is easy to spot. It is on display in Israel whenever there is a suicide bombing. After the victims are evacuated, clean-up crews descend to clear out the physical wreckage, make immediate repairs and re-open the site to daily traffic within hours. Londoners showed their resilience in the aftermath of the 7 July 2005 suicide attacks on the Underground and city bus system. The terrorists' objective was to cripple the city's public transportation system; resolute citizens foiled this plot just by showing up for the next morning's commute. One defeats terrorist tactics by working to minimize terror, which arises from a feeling of unbounded vulnerability and powerlessness. By empowering people to think and cope with disasters, they will be less afraid when things do go wrong—which of course will happen from time to time. It really is as simple as that.

Building national resilience, however, will require much more than the President's use of the bully pulpit. It requires a sustained national commitment to building robust society and institutions, readiness to swiftly respond and recover from disaster and, once the dust clears, the willingness to change in light of lessons learned.

Robustness involves the ability to keep operating, to bend but not break, in the face of disaster. The Obama Administration's plans for reinvesting in infrastructure, health care, and energy as a part of its economic stimulus effort provides a historic opportunity to design structures and systems strong enough to handle the stress of disasters. Alternatively, robustness can be achieved by assigning top priority to projects that enhance redundancies in critical systems. At the societal level, robustness entails investing in basic services like public safety, public health, and emergency management to handle low-probability, high-impact events.

"It is both ironic and inspirational that the Legislative and Executive Branches of the U.S. government, whose constitutional duty is "to provide for the common defense" were themselves defended that day by an alert and heroic citizenry."

Readiness is the process of building a level of preparedness to identify and manage challenges once the disaster unfolds. It includes the ability to nimbly identify options and prioritize both damage control and initial remedial action, followed by the ability to communicate those decisions to the people who will act on them. Readiness depends primarily on planning and people, not technology. It means providing adequate resources to the National Guard, the Red Cross, emergency room staffs, and other emergency planners and first responders to whom people turn when they cannot help themselves.

The third element of resilience is rapid recovery: the capacity to get things back to normal as quickly as possible after the disaster-level forces are gone. Carefully drafted and well-exercised contingency plans, competent emergency operations, and the means to get the right people and resources to the right places are the key ingredients to a swift recovery. Communities like Charleston, Gulfport, and Memphis are organizing themselves with the support of the Oak Ridge National Laboratory to be able to quickly bounce back from catastrophic events under a program known as the Community and Regional Resilience Initiative (CARRI) [3]. The goal of CARRI is to identify the processes and tools needed to restore the community's ability to provide essential services, allowing businesses and schools to re-open as soon as possible after a disaster.

Finally, resilience requires adaptation. In other words, there needs to be an appetite for learning the lessons that disaster teaches. A foolish society is one that goes right back to "business as usual," rebuilding homes on floodplains or underinvesting in public safety and health. People must be willing to make pragmatic changes to improve robustness, resourcefulness, and recovery in time to meet the next disaster.

"When it comes to protecting American lives, our greatest national asset is not our second-to-none national security establishment led by the Commander-in-Chief; it is an engaged and resilient civil society."

What distinguishes a focus on societal resilience from a national effort centered on security is that it involves moving beyond the secretive, highly centralized, and overly federalized approach that the Bush Administration embraced. Instead, it requires a far more open and inclusive process that taps America's greatest strengths: its civil society and its private sector. Further, while security usually incurs upfront costs, investments in resilience almost always provide a positive return on investment. As a June 2007 Council on Competitiveness report documents, resilient communities and companies are inherently more productive, innovative, competitive, and desirable places to live and work.

Ironically, on the very day of Bush's farewell address, just the kind of resilience we should have been pursuing on a national scale was on display in the Hudson River, where U.S. Airways Flight 1549 made an emergency landing (Figure 1). New York Governor David Patterson got it completely wrong when he dubbed the incident "the Miracle on the Hudson." This was no miracle. The aviation industry designed the plane to survive a waterborne landing and invested in training for just this kind of low-probability, high-impact contingency. The pilot and flight crew knew what they were supposed to do, and they did it. The passengers had been briefed on how to safely evacuate during an emergency landing, so they had some advance idea of what steps they needed to take when flight attendants issued directions during the incident. The first rescuers on scene were commuter ferries that, by regulation, carry basic water rescue equipment. The ferry crews received training on recovering people gone overboard. Next came the local first responders, who were assisted by the federal government in the form of the U.S. Coast Guard. In the end, upfront investments in robustness and readiness—and responsible action by everyday citizens—meant that not a single life was lost in the crash. Heroism helps, of course, but it cannot substitute for institutionalized readiness. When it comes to protecting American lives, our greatest national asset is not our second-to-none national security establishment led by the Commander-in-Chief; it is an engaged and resilient civil society.

PRACTICAL STEPS

Beyond emphasizing resilience, the Obama Administration can take five practical steps to put the federal homeland security mission in better order.

Figure 1 Rescue Mission Conducted by U.S. Coast Guard

First, it must professionalize DHS. This will require converting a significant number of DHS political positions to career positions, taking the Department in the direction of other national security organizations like the CIA and the FBI. In the near term, talented managers from outside DHS need to be recruited to address serious shortfalls in competency and expertise. The federal government must also pay far more attention to providing resources for the recruitment, training, education, and professional development of DHS personnel. In addition, DHS is too dependent on a contractor work force even for performing core functions like contractor oversight (yes, they have contractors to watch the contractors) and the development of budget and strategy documents. Contracting out core functions costs about the same as it would to hire more government staff, but it comes at the expense of building long-term institutional capacity.

Second, the new Administration should also change the allocation of the resources DHS receives, which is now skewed toward costly acquisition programs, leaving the Department without enough funding to invest in its most important asset: its people. Specifically, many of the border control initiatives that were advanced in the immediate aftermath of 9/11 should be reexamined. The fact is, federal border control measures will always be of limited counterterrorism value for two reasons. One is that the number of terrorist operatives U.S. authorities are trying to intercept is miniscule compared to the nearly half-billion people who pass through U.S. ports of entry each year, and the geographical expanse of America's frontiers (95,000 mi of coastline and 7,000 mi of land borders with Canada and Mexico) render farcical the idea that we can fence it all in. Searching for a needle in a haystack is not quite the right analogy; it is more like trying to find a specific grain of sand on the seashore. The second reason is that border control measures inevitably become rote and ritualistic, which means they can be evaded by people who have the time, resources, and motivation to do so.

Third, beyond internal DHS adjustments, the Administration needs to address the huge asymmetry one notes when comparing the resources provided to DoD to carry out its "homeland defense" mission and the resources provided to DHS for its "homeland security" mission. Even a cursory analysis would show that the amounts given to DoD are not as sound an investment as a commensurate investment in DHS, or state and local governments. Consider the $12 billion budget that the Pentagon devoted to missile defense research in 2008. That is more than ten times the amount that DHS received for all its interdiction programs combined. There is universal consensus within the intelligence community that the threat of a nuclear weapon arriving in the U.S. via smuggling is far greater than the threat of a missile carrying one into our airspace. Federal spending, however, does not reflect this fact.

"One important limiting factor is the federal security clearance, which dates to the Cold War. It was built around a "need-to-know" rather than a "need-to-share" imperative, which would be more suited to the current security environment."

In some instances, the imbalance in defense spending actually exacerbates the security risk for the general population. For instance, the Pentagon received approximately $10 billion in 2007 to invest in protective measures for military bases and assets on U.S. soil, while DHS received only $750 million to support critical infrastructure protection grants for the nation's "high-risk urban areas." True, this spending imbalance probably reduces the risk that terrorists will target U.S. military forces within U.S. borders, but it does so only at the expense of making civilian infrastructure relatively more vulnerable, and therefore more attractive, targets. More directly, the frequent deployment of National Guard units to Iraq and Afghanistan has eroded their ability to support civil efforts in times of disaster and domestic emergency. The Obama Administration will need to identify the desired balance between the Guard's overseas role and its domestic one.

Fourth, beyond these federal-level efforts, the White House needs to make a concerted effort to draw upon the American people's legacy of grit, volunteerism, and ingenuity in the face of adversity. Ordinary citizens and private companies should be asked to do more to protect themselves and to help others during emergencies.

One way that people can lend a hand is by participating in the Citizens Corps program [4]. Citizen Corps is an umbrella organization for local community emergency response teams (CERTs), medical reserve corps, neighborhood watch groups, fire corps, and volunteers in police services. Through these councils, citizens band together with local emergency responders to improve their knowledge, skills, and ability to support their or other communities when disasters strike. CERT provides 20 hour of training to volunteers in basic first aid, management of utilities and small fires, organization of spontaneous volunteers, and the collection of disaster intelligence to support emergency responders. There are more than 2,000 Citizen Corps Councils located in all 50 states and six U.S. territories, but the annual federal funding to support their activities has been just $15 million—roughly what taxpayers have been spending per hour over five years on the wars in Iraq and Afghanistan. The Obama Administration should commit to a tenfold increase in funding to support the expansion of Citizen Corps chapters and activities around the nation.

Partnering with state and local officials is also key to building greater national capacity for managing large risks. But doing so requires that the new Administration hold the federal bureaucracies' feet to the fire. The most common complaint by the men and women who are on the front lines of local law enforcement is that information sharing with the federal government is a one-way street: the locals pass along information and get little to nothing back in return. One important limiting factor is the federal security clearance, which dates to the Cold War. It was built around a "need-to-know" rather than a "need-to-share" imperative, which would be more suited to the current security environment. Congress needs to overhaul the existing system for issuing security clearances and classifying and handling sensitive information to make the system more open and inclusive.

Fifth, greater outreach to individual citizens and local and state officials should be combined with much more serious efforts to engage the private sector, which owns and operates 85 percent of the nation's critical infrastructure. One major barrier to public-private cooperation has been the "tragedy of the commons" problem associated with excessive reliance on voluntary standards and best practices. Security has a cost. When these costs are not mandatory, those who "do the right thing" risk being placed at a competitive disadvantage relative to free riders. There are only two ways around this problem: The government must either devise a more forceful regulatory approach while still involving the private sector in the rulemaking process, or it must provide direct or indirect financial incentives to promote compliance. Given the economic stress U.S. companies are currently experiencing, tax incentives seem like the right option for the time being. That said, any regulatory approach will generate some countervailing pressure from the private sector. But these issues can be managed, if not entirely eliminated, by investing in DHS liaisons who have the expertise to formalize relationships throughout industry sectors.

"Reinvesting in our infrastructure will make the critical foundations of our economy and society more durable in the face of natural and man-made disasters. … building a more resilient society immunizes us… against overreacting when disasters occur, thereby allowing us to remain true to our ideals no matter what the future may bring."

A FINAL WORD

A determination to confront ongoing exposure to catastrophic disasters is not an act of pessimism or paranoia. Rather, it is a mature recognition that things go wrong from time to time, and that we need to prepare for such times. There is an upside, beyond increased security, to placing greater emphasis on national resilience. Focusing on resilience elevates the value of investing in other policy priorities, for example. Reinvesting in our infrastructure is not only helpful as an economic stimulus; it will also make the critical foundations of our economy and society more durable in the face of natural and man-made disasters. A focus on building a more resilient society immunizes us, too, against overreacting when disasters occur, thereby allowing us to remain true to our ideals no matter what the future may bring.

Alternatively, neglecting homeland security is like living on a flood plain without carrying flood insurance. It is undoubtedly tempting for the Obama Administration to set aside the homeland security mess it has inherited while it attends to the many other pressing challenges that command its attention. But inevitably there will be a major hurricane, earthquake, disease outbreak, or terrorist attack on President Obama's watch. If the Administration does nothing to rectify the broken system it has inherited, it will not escape the political reckoning that will follow that next disaster. Beyond Washington, lives will be needlessly lost, and property will be unnecessarily destroyed. There is no upside to postponing the imperative to rebuild a more resilient nation.

Q&A SESSION WITH DR. STEPHEN FLYNN

Q: *You spoke about the lack of qualified people at DHS. I believe it is the single best program out there. It is the homeland security strategy that calls for at least citizen involvement several times to increase the sense of community. I believe it is the national security strategy that says that we need to make terrorism less terrifying by making us more resilient. What can we do to make these strategies more effective?*

Stephen Flynn – I certainly put the plug in for the Monterey. I have to say overall, and it is something I have experienced when somebody has been outside the official federally-funded parts of the academic community, think tank and the Council on Foreign Relations. I look at many of my peer institutions that are out there as well as what is happening in our academic universities. As important as this issue is and the stakes involved, when there has not been direct federal money in the pipeline, there has been very little in the way of building this capacity.

This is a much more lonely business, what I am doing, than I ever expected it to be this many years down the road. There may be in our case one guy who does this at the Council on Foreign Relations. I have a counterpart. One guy who does it at CSIS. If you look at many cases of universities, I have an affiliation with Stanford, CSAC, and they are cutting back because there are not enough resources available.

For private universities, we have not seen the step up. A lot of people, of course, repackaged themselves and said they were homeland security if they were doing emergency preparedness and other kinds of stuff because that is where the money is. However, as a real discipline effort going forward, we need more Montereys and more than 300 people moving forward. Thank God we have that at least.

Broadly put, I think there is a lot to be said by moving this thing beyond the kind of terrorism focus into one that is more willing to embrace all hazard, because it just deals with the simple probabilities for most Americans. It turns out that 90 percent of Americans, if they stay put for the full life of a 30-year mortgage, will get hit by a major natural disaster. That is from mapping out where people live and the likely threats they are going to face. Now, more than half of our population lives within 50 mi of the coast. On the east coast, there are hurricanes. On the west coast, there is this big crack that runs along most of it. In the heartland, we have got rivers that rise and tornadoes that blow through. There is a lot out there that we are not going to prevent that actually requires skills to manage that would serve us very well if we also had to manage a terrorist incident. By broadening this focus, now, one of the reasons why that really has not happened is because the federal paradigm that we were operating in traditionally handles natural disasters at the state and local level.

Therefore, the view from Washington was governors and mayors. We at the federal level deal with national security. The kind of terrorism that we see obviously is an element of national security. We will help you fund on counterterrorism, but you just have to do your normal day-to-day job on the natural hazard stuff that comes your way. How dysfunctional this is was something that became clear to me in 2004 operating from my counterterrorism perspective when I had the chance to sit down with the emerging management for San Jose, Oakland, and San Francisco asking how they were prepared to deal with a dirty bomb.

To ground this whole thing in reality, on October 2004, then Vice President Cheney said the number one national security threat to confront this nation will be a weapon of mass destruction going off in a major city. You need to "wrap your mind around that concept." The week before this, I sat down with the fire chief of the New York Fire Department, who is responsible for managing these incidents, and said, "How are you set to handle a dirty bomb going off in Manhattan?"

He said, "Well, we have a plan."

I said in reply, "I have a very simple question." Actually, it was an operational question. "How do you conduct decontamination? How are you going to wash people down?"

He said, "We have a plan. If it goes off in Central Park, we are going to put fire trucks on either side of Fifth Avenue. They will shut down. We will hose them down, and we have hospital gowns to put them in."

I said, "All right. That sounds okay. How is that going to work in February?"

"Well, we do not have the foul weather plan yet."

This happened three-plus years after 9/11. I am sure the Vice President believes in his heart of hearts that that is the issue. Well, why did not somebody get on the horn and ask the likely place where it was going to happen. Can you guys give people decontamination? All right. Now, that was dealing with that threat. I brought the same question to the folks in the Bay Area.

Instead of talking to one guy, I talked to three of them because the Bay Area, of course, works like five boroughs. It works with three different, often-competing fire departments and emergency management department. They said, "Not only are we not well prepared for that, we are less prepared than we were in 2001 for dealing with an earthquake or a mudslide because the same staff of people spent all their time writing grants for counterterrorism because that is only where the money is. We have to go off and get that specialized training, or we cannot go out and refresh our earthquake plans for new businesses that are rolling in and so forth."

How dysfunctional is that? That is wrong. If this is a national security imperative to build a broader level of resilience, let us do it around the needs at the state and local levels, which are dealing with the hazards that are not conventional national security. Then, wink-wink, we get national security benefits from doing so. Broadly put, one thing we obviously need is to help build that national capacity. That is where the Feds can be helpful in priming the pump and also, very importantly, in setting standards.

This is something that also would not play itself out in the last administration because if you set standards, then those would be unfunded mandates. Nobody wants to go down the slippery slope.

"Who are we at the federal government to understand how you should protect yourself? You know, California or Massachusetts, whatever. You know best. You decide how to do this." As a practical matter, this did not work very well because as you ask states to handle particular matters, the expertise often was not at the governor level. It was often at the major urban level.

When you try to work through states—this is a bit flip to say—but many of the fire commissioners at the state level, the guys on the volunteer fire department when the governor was the mayor if you want to be at the top of the fire fighting business, your job goal is to someday be the state fire commissioner most places. You want to be in a big city. The expertise often was down below the state level. Governors were in an impossible position if they tried to figure out what to do with this money because, if you put all the money in Manhattan, people in Rochester, New York get their nose a little bit out of joint. They tend to end up wanting to spread things around. The expertise and political ability to build this thing did not reside at the state or governor level. It rarely existed outside there.

What could we have done? What do we need to do now? We can take a population of fire chiefs, many who have gone through the National Fire Academy and therefore know each other pretty well, bring them into a place like this, lock them up for two weeks, and tell them to come out like John Damrell did and give us a fire code equivalent to what every city in this country should have on a six-tier system. Then when we get those six tiers, we know how to plug and play into them. We talk about how to fund this and how we build that capacity. That is what building the capacity at the public health and safety level|. On the broader citizenry, I think it is going to be much more about taking good programs like Citizen Corps and putting the bully pulpit of the President behind it to better designate contributions. One of the parts of the sacrifice we are talking about is what you can do. Having these programs be meaningfully funded and obviously having people have good experiences associated with them is going to be a big part of that.

Another area that I have been looking at too is outreach to Hollywood in a way that we had during the second World War. There are opportunities by the masters of people who know how to hold our attention around dribble to actually hold our attention around things that could help us. However, that would require an adult conversation with that community, but I think it can happen. There are ways to embarrass them into doing public good, and there are also ways into leveraging to some extent as well.

We really have not begun to take this agenda seriously. I worry about the political risks for the incoming administration because the rhetoric has been so high and the reality so low that if something really does happen on a 9/11-plus scale, it is going to look pretty much like they took their eye off the switch, I mean, off the ball. Then we are into a self-flagellation, degenerative cycle that I do not think will serve any of us well, whether Democrats or Republicans.

Q: I saw your talk last year. I have a couple of comments and a question. One is I agree with you; I think most of society has gotten soft. However, I think Socrates said the same thing thousands of years ago, that the next generation is soft. So I am not sure that is a valid observation. Passengers who did not have any training or a federal mandate overtook the fourth airplane (Flight 93). The fact that they risked their lives when they knew the chips were down just shows that maybe Americans still have what it takes. Maybe we do not need this effort that you are talking about.

Also, suppose that there is a rational actor on the other side, that terrorists can be dissuaded. All the empirical evidence shows that is not the case. Terrorists are not rational actors. They do not weigh cost and benefit. They create terror only for terror's sake. The fact that we are prepared, and therefore they would get less effect, will have no bearing on what they do.

I am not saying we should not do this. I am just saying that we should not expect great results. I do not think that the effort needs to be as huge as you are talking about because I am not so sure the Americans today are any less masculine, so to speak, than the Americans who settled the west. I think that observation is a little bit shallow. I give a lot more credit than you do. Ultimately, my question is if we have a positive response as Americans now, *why would the changes you discuss produce a different response and what benefit would arise from such a change?*

Stephen Flynn – Well, I feel duly humbled if I have not conveyed somehow that I have the same view about the American people and that same sense that we are doing ourselves a great disservice. If that came across in some sort of a flip way, then I apologize for that because I do share that same belief that it is in our DNA. I believe that it can be pulled out, but I think it takes leadership to do so. We can point to a number of instances where lack of preparedness caused problems (e.g., Katrina kinds of issues).

However, we also can point to a number of instances where we find that capability is there. It just needs a little bit more reinforcement at a national level. It does not happen by magic. I point to the U.S. Airways 1549 incident, which our Governor of New York said was a miracle. It was not a miracle. It worked out really well that everybody came out alive, but the aviation industry actually designs planes to land in water. It is not supposed to happen, but they do that.

They train pilots, not all of them as well as this one, to land the planes in water. It does not happen very often, but they do. They educate the flying public about some of these risks and what they can do. Most of us do not pay enough attention to it, but the fact of how we egress and deal with these things is provided. When things went wrong, the flight crew was trained to manage that, but the first responders were commuter ferryboats. By federal regulation, they practice things like man-overboard drills. They have life rings. They have the basic tools to save lives.

The spirit was there, but the skills also had to be. The investment also had to be made. That is where I am really trying to push us. I am also trying to push this community, in particular, out of that paternalistic side of the equation. As a nation, we all have a lot more capability than most of our elected officials give us credit for to deal with this. I think the nature of where we live now and much more urbanized lives, much more just in time lifestyles, by any comparison, the amount of cash we carry with us, the amount of food in our refrigerators, the stores and things, we are not as able as we used to be able to ride things out. Some of the incentives and efforts to build that capability will be important going forward.

On the terrorism issue, there are other folks who can come in here and mess this around here. I really think, though, it is important to bifurcate where our risk is. On the one hand, there are acts of terror that will look like spectacular acts of violence to get attention. Those will keep happening. Those will be more commonplace, and a lot of them will look the way that you describe them to look.

However, terrorism as an effective asymmetric form of warfare is looking for the real soft targets where you can get mass consequence. We are not doing enough as a society to take some of those off the table. There are not unbounded numbers of them so if we end up on a day where we just have, as bad as it is, the nutcases doing their thing, that is one thing. It is when the people have an adversary who uses terrorism as a way to unravel critical systems and cause much higher casualties, that I think we need to focus more time and attention. That is where I am still pushing.

REFERENCES

1. John F. Harris, Mike Allen, and Jim Vandehei, Cheney Warns of New Attacks," Politico, 4 February 2009: http://www.politico.com/news/stories/0209/18390.html.
2. Jeffrey Rosen, "Man-Made Disaster," The New Republic, December 24, 2008: http://www.tnr.com/politics/story.html?id=5248f065-cbd3-4264-ac58-cffdfd947a22.
3. Community & Regional RESILIENCE Initiative Web site: http://www.resilientus.org/.
4. http://www.citizencorps.gov/.

1.6 AL QAEDA'S INTERAGENCY

Bruce Hoffman

INTRODUCTION

Not only is it always a tremendous honor and tremendously beneficial because of the questions and the interaction of this symposium, but what I like most about coming here to speak is that I am forced to do something new: think about what the major trends are and in what new directions to go. I will cover the gamut of terrorism but also discuss how this relates to the interagency process and our response to terrorism.

> *"What is al Qaeda's interagency process? What is their networking? How are they operating?"*

So, I will begin with al Qaeda, not least because I feel almost no inhibitions in opining or waxing in various directions about a terrorist organization, but I have to say I feel far more intimidated about attempting to prescribe solutions to the interagency process.

Professor Bruce Hoffman is a tenured professor in the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service. Professor Hoffman previously held the Corporate Chair in Counterterrorism and Counterinsurgency at the RAND Corporation and was also Director of RAND's Washington, D.C. Office. Professor Hoffman was the founding Director of the Centre for the Study of Terrorism and Political Violence at the University of St. Andrews in Scotland. In November 1994, the Director of Central Intelligence awarded Professor Hoffman the United States Intelligence Community Seal Medallion. He holds degrees in government, history, and international relations and received his doctorate from Oxford University.

In that respect, I want to address the following question: What is al Qaeda's interagency process? What is their networking? How are they operating? Seven and a half years into this struggle, we still face an enormous challenge. Sometimes, we want to ask, is al Qaeda succeeding or not, and what is their own brand strategy?

AL QAEDA'S INTERAGENCY

Today's al Qaeda universe comprises a movement that has been able to build and exploit seven major networks in as many theaters of operation geographically, that is able to function on four different operational levels, and that, in turn, employs six core subordinate strategies in hopes of achieving its ends. The networks or the theaters are fairly obvious:

The senior core leadership is one key network or hub, which is now located or situated in the second network or theater of operations: Afghanistan, Pakistan, and particularly the lawless border that separates those two countries.

It has a network—although it wants us to say a failing one—in Iraq, that is "al Qaeda in Iraq."

It has a rather more robust one in the Islamic Maghreb in North Africa, which is an increasing threat, in fact, not least because of Aymen al-Zwahiri's statement regarding the Sudan.

It has a functioning network—an increasingly threatening one—in East Africa, particularly in Somalia.

It has a growing network—unfortunately, as The New York Times reported, that has had recent successes—in Saudi Arabia:

> *"… Saudi Arabia's main terrorist threat appears to come from Yemen, where a number of Saudi extremists have regrouped in that country's mountainous, tribal hinterland. They have struck there repeatedly in the past year and have declared a goal of using Yemen as a base for attacks against Saudi Arabia. The border with Yemen is long and porous, and militants appear to have no trouble crossing it at will."*

It is positive that the Saudis have displaced the threat to a certain extent to Yemen where al Qaeda is becoming stronger.

Finally, it has the al Qaeda network in Europe, which it continues to seek to exploit.

". . . today there are many al Qaedas, all of which have very different capabilities and pose individually unique challenges."

What we see is that al Qaeda's sustainability or success has been predicated on the fact that it has been able to create what really amounts to a network transactional movement, rather than a single monolithic entity. Consequently, today there are many al Qaedas, all of which have very different capabilities and pose individually unique challenges. What this means for us is that our approach in the struggle cannot have a one-size-fits-all-strategy; we have to recognize the diversity of al Qaeda.

Four Operational Levels

On an operational level, it functions—as I think it always has—extremely comfortably on at least four different levels that are used sometimes sequentially, sometimes individually, and sometimes in mixture.

At the top is al Qaeda central. These are the operations that are actually conceived, plotted, planned, and implemented by the remaining al Qaeda senior leadership in the Afghan/Pakistan Theater. These include the spectacular al Qaeda attacks on 9/11, the attack on the USS Cole in 2000, the 1998 embassy bombings, and so on.

The next level down contains the al Qaeda affiliates and associates. These are the like-minded terrorists and insurgent groups worldwide that function independently but nonetheless have bought into al Qaeda's ideology, support al Qaeda's overall aims, and act in concert, sometimes at the behest, of al Qaeda. These include al Qaeda in Iraq, al Qaeda in the Islamic Maghreb, but also groups that do not have the al Qaeda moniker—Lashkar-e-Taiba, for example, the group responsible for the Mumbai attacks in November 2008, and the Islamic movement of Uzbekistan, which has been increasingly consequential as well in the Pakistan area.

Another level down is what I call the al Qaeda locals. These are, in essence, al Qaeda sleeper cells or operations units that have received training from al Qaeda and may have received some general guidance, but mostly are left to be opportunistic, to function independently in support of al Qaeda's aims but nonetheless not necessarily in top-down, al Qaeda centrally directed operations. These include many of the al Qaeda cells that have been uncovered in Europe, particularly in the United Kingdom, individuals like Ahmed Ressam, the Millennium Bomber from 1999, who was clearly trained in an al Qaeda camp, given very open-ended operational and targeting instructions and a minimal amount of finance, and left basically on his own to recruit his own terrorist cell in North America and to carry out his attacks—still connected to al Qaeda, but not the top-down specifically directed operation such as we saw on 9/11.

Finally, we get to the lowest level, and one that I think in recent years has received disproportionate attention and actually still poses the least threat but has to be reckoned with or taken account of; that is the al Qaeda network of independent cells or even individuals who have been inspired, motivated, animated, and radicalized by al Qaeda propaganda and the Internet, but these are individuals who have no direct contact with al Qaeda, have never trained in an al Qaeda camp, may never have met a terrorist in their lives, but nonetheless have taken up the mantel of struggle merely because of al Qaeda's influence or motivation.

A prime example of this is the Hofstad Network of radical extremists in the Netherlands, a member of which, Mohammed Bouyeri, murdered the Dutch filmmaker Theodoor "Theo" van Gogh in November 2004. They had absolutely no direct connection to al Qaeda, but certainly he and the fellow members of the cell were motivated and inspired by al Qaeda.

Al Qaeda's Strategies

What about al Qaeda's strategies? Al Qaeda employs six core strategies to achieve its aims. This is what makes countering them so difficult for us. Its first strategy, very clearly, is to overwhelm, distract, and exhaust us. Distracting our attention and focus is one reason why these low level al Qaeda operatives that have no connection with the organization are nonetheless so valuable to the movement because they are the low hanging fruit that consume the time and the attention of intelligence, security services, and law enforcement and what al Qaeda hopes will distract us from the main attack.

> *"Particularly at a time of profound global economic travail and upheaval, al Qaeda thinks that their strategy of distraction, of overwhelming, enervating, and exhausting us, will pay bigger dividends than at any time in the past."*

Also, by operating across seven different theaters or with seven different networks, al Qaeda similarly hopes to distract, enervate, and dissipate our abilities by having to keep track of this international movement. Particularly at a time of profound global economic travail and upheaval, al Qaeda thinks that their strategy of distraction, of overwhelming, enervating, and exhausting us, will pay bigger dividends than at any time in the past.

This has been a consistent element of al Qaeda's narrative since at least the summer of 2002, a narrative in which al Qaeda has argued that the U.S. and its allies will not be defeated in conventional military terms but rather bankrupted, economically exhausted, and therefore will have its morale sapped by this unrelenting terrorist and insurgent campaign directed against it. In al Qaeda's historical narrative, this is not something that they think is beyond the realm of possibility; they think it is quite possible, in their view, history repeats itself. They make the point that who would have imagined that in the 1980s a grab bag group of Mujahideen, dedicated fighters in Afghanistan, could have defeated the Red Army and then set in motion the chain of events that led to the collapse of the Soviet Union and the demise of Communism. In their narrative, they say the U.S. is at that same precipitous economic point that the Soviet Union was. Just as no one in the 1980s understood how bankrupt the Soviet economy was, how weakened it was, al Qaeda's ideologues argue that is the same position the U.S. is in today, and it is the force of the jihadists and the onslaught of their continued campaign that they believe will also eventually destroy us.

In recent years we have witnessed—even in bin Laden's October 2004 address just before our Presidential elections—how bin Laden and al Qaeda constantly play on the economic card and see every economic downturn, every travail that the U.S. faces, as proof that they are succeeding and we are losing. I am not saying that this thinking is linked to reality, but of course propaganda does not have to be truthful as long as it is believed. At least, in their followers' eyes, they have a good back-story. So that is their first strategy.

Their second strategy is to seek to create, foster, and encourage fissures and divisions within the Alliance or raid against it, particularly on the ground in places like Iraq and especially in Afghanistan. This involves the selective targeting in both operational theaters against those Coalition partners, especially NATO allies in Afghanistan whom al Qaeda and its allies consider our weakest links. Very early in the campaign in Iraq, for example, 17 Spanish Gordeeva civil intelligence specialists were targeted. The efforts as we see in Afghanistan—particularly targeting German, Dutch, Canadian, and British allies with improvised explosive devices (IEDs) for suicide attacks—is part of al Qaeda's effort to present the image of the U.S. as being isolated in the world, waging a war against Islam, and engaging in the occupation of Muslim lands.

Obviously, this played a role in the 2004 bombings in Madrid, which resulted in the Spanish decision to remove its troops from Iraq. Certainly the targeting of the United Kingdom is designed to influence public opinion and in turn apply pressure on the government to withdraw its forces first from Iraq and now from Afghanistan. You see this with the attacks on the Netherland's forces, for example, in Afghanistan where the Netherland's government has said that it first deployed to Afghanistan to do nation building, not counterinsurgency, and has recently been saying consistently it is not going to renew its commitment after 2010.

Third, we see an al Qaeda strategy that also conducts local campaigns of subversion and destabilization in key operational theaters. This is interesting in its own right; subversion is a word that has fallen out of our lexicon in the 21st Century, compared to the Cold War era when Soviet or communist subversion was a main focus and a main concern of ours.

I would argue that we see al Qaeda in key countries, such as Afghanistan, Pakistan, Yemen, and Algeria, attempting behind the scenes to use local groups to advance al Qaeda's aims: destabilize existing societies; undermine popular confidence in government's ability to maintain security, law, and order; undermine confidence of the government's ability to protect the population from suicide and other forms of terrorist attack; and therefore serendipitously create weakening or failed states.

"Today, . . . al Qaeda plays a distinctively low-key role; it acts as a force multiplier, improving the capabilities of local terrorist or insurgent groups by the provision of fighters who are embedded in those groups, much as our forces are embedded with national Iraqi and Afghani police and military forces, providing training, weapons, and technological assistance, perhaps most effectively in the realm of information operations."

For example, today in Pakistan and Afghanistan, you do not see al Qaeda front and center, operating as it did in the 1990s when it was very prominent and active—certainly in the Sudan, but even more so in Afghanistan—in forming a state within a state or the power behind the Taliban. Today, in these key theaters, al Qaeda plays a distinctively low-key role; it acts as a force multiplier, improving the capabilities of local terrorist or insurgent groups by the provision of fighters who are embedded in those groups, much as our forces are embedded with national Iraqi and Afghani police and military forces, providing training, weapons, and technological assistance, perhaps most effectively in the realm of information operations. You just have to look at the Taliban on both sides of the border in Pakistan and Afghanistan: A decade ago they were technophobes; they were Luddites, in the Stone Ages. Now, we see both Talibans with online news magazines, exactly as were pioneered by al Qaeda at the beginning of the century, with very slick public relations operations that are often first in the media with their version of Predator unmanned aerial vehicle (UAV) attacks—divorced from reality and truth—but being first in the press means that they are able to occupy a place and get their version out ahead of that, for instance, of CENTCOM. We see groups that never had any experience with the Internet now developing very effective communication securities, married with other media activity, such as the subversion or influence of local newspapers, in their favor.

Fourth, we have the addition of capabilities of al Qaeda allies in each of the above theaters and elsewhere. Again, we see al Qaeda working behind the scenes as this force multiplier and building up the capabilities of their local allies to make them more effective in countering the established governments.

Fifth, al Qaeda continues to seek access to citizens of what it defines as enemy countries—i.e., countries of the West or allies of the U.S., who possess, in their view, clean passports. In other words, their focus is on European nationals, especially converts who could enter the U.S. under the visa waiver program, who do not have Muslim-sounding names, who have passports issued in their birth names, and who are from countries that do not fit our stereotype of the al Qaeda operative: the young Arab male from the Arabian peninsula.

Even as we see recently in the roughly 20 or so Somalia American youths that have left the Minneapolis/St. Paul area to go to Somalia to train and to fight with an al Qaeda clone there named Al Shahab, you see even the first inroads that al Qaeda, or at least an al Qaeda affiliate, has made in the U.S. Just prior to the inauguration in January, the most serious, or the most credible, threat that American law enforcement and intelligence agencies were concerned with came precisely from these youths who they believe have American passports and could have been deployed back to the U.S. on terrorist operations.

Sixth, there is an al Qaeda whose strategy is as opportunistic as it is instrumental. This is a movement that has always shown itself capable not only of planning the multi-year detailed spectacular terrorist operations but is also able to take advantage and exploit opportunities that present themselves. You have a movement that is constantly monitoring its enemies, attempting to identify gaps or vulnerabilities in its defenses, and then taking advantage of those gaps and vulnerabilities and moving in for the attack.

We know for a fact that al Qaeda Al Shahab, its media arm, is not only an output communications vehicle disseminating propaganda but also serves an input function. In other words, it gathers strategic intelligence through cultural information, attempts to find out exactly what the concerns of its enemy populations are, and crafts attacks to take advantage of them. So, for instance, we know for a fact that al Qaeda has downloaded the Web sites of virtually every think tank in the U.S. to understand our conducted studies, affected vulnerabilities, counterterrorism strategy, and counterinsurgency.

We know that al Qaeda routinely monitors CSPAN to closely watch congressional hearings, which contain a mother lode of information for them, because a typical congressional hearing has a panel of senior representatives of key agencies charged with the war on terrorism that in many cases are subjected to withering questioning by members of Congress. Then they have a subsequent panel of academic or independent experts that opine or offer views, and this provides a treasure trove of information for al Qaeda to shape what they believe are the vulnerabilities of their targeted societies.

Therefore, we see that across the board al Qaeda is arguably implementing, if not achieving, its objectives. They fundamentally believe in the inevitability of their divinely ordained struggle and the power of their historical narrative. As I said earlier, they already believe that they were instrumental in defeating one superpower and are confident that they can defeat another.

20TH ANNIVERSARY

What does this tell us about al Qaeda's mindset and determination? First, last August marked an enormously important milestone in al Qaeda's history, its 20th anniversary. As a terrorist group, you do not get to be 20 years old unless you have an enormous capacity for adaptation and change that can constantly understand and monitor the countermeasures being used against it and can adjust to even the most consequential countermeasures to overcome or to obviate them. Al Qaeda thus has survived largely because it is a learning organization that has had this capacity to adapt, adjust, and overcome even the most formidable countermeasures directed against it. In this respect, al Qaeda is almost like the archetypal shark in the water that only can move forward to survive

Unfortunately, this is part of a broader pattern of terrorism that we see today. David C. Rapoport , University of California, Los Angeles Professor Emeritus of Political Science and distinguished scholar of terrorism, conducted a study of Cold War era terrorist groups from 1968 to 1990. What he found in his 1992 study is that 90 percent of all terrorist groups during the Cold War era did not last more than a year. In the 20th Century, terrorism was a very difficult vocation for an organization; the survival rate was not high; 90 percent lasted less than a year and of the 10 percent that survived more than a year, half of those were gone within five years.

Audrey Kurth Cronin at the National Defense University, whose book is coming out this summer, has updated Professor Rapoport's statistics. What she found—in a much smaller sample of time but it is nonetheless a very disconcerting finding—is that from 2000 to 2008, the average life span of terrorist groups in the 21st Century is roughly five to 10 years. Terrorist groups today last five to ten times longer than their Cold War predecessors and show a degree of resiliency and a capacity for survival that did not previously exist. Consequently, what this suggests is that terrorism today is becoming more difficult, more complex, and more time consuming to counter than ever before.

COUNTERING AL QAEDA

How do we counter al Qaeda effectively? What are the means that we can use against them? I think the main question, the main challenge we face from an interagency perspective, rests in breaking the cycle of recruitment and regeneration that sustains al Qaeda and affiliated terrorist movements. In so fluid an environment as we see today—with terrorist groups constantly changing and adapting, adjusting to overcome our countermeasures—our strategy has to change and adapt as well.

At the foundation, I think a dynamic and flexible approach is the recognition that successfully countering terrorism, as well as insurgency, is not exclusively a military endeavor but also involves fundamentally parallel political, social, economic, and ideological activities. What we therefore require is a more integrated systems approach to a complex problem that is at once operational, durable, evolutionary, and illusive in character.

In sum, we need to be able to leverage and exploit networks with the ease and facility that our enemies routinely do. Thus, in addition to the traditional hard military skills of kill and capture, destruction and attrition—and we absolutely must continue to kill and capture terrorists (it is not my message that we ease up on that accelerator)—we have to emphasize equally the importance of the "soft skills," such as negotiation, psychology, social and cultural anthropology, foreign area studies, complexity theory, and systems management.

> *"What we therefore require is a more integrated systems approach to a complex problem that is at once operational, durable, evolutionary, and illusive in character."*

We have to be able to operate effectively in an ambiguous and dynamic environment in which we see our regular adversaries functioning. Above all, this requires strengthened interagency coordination, cooperation, and deconfliction. I think these are key elements to enhancing interagency operations, which have enormously improved in the past seven years. (I say this humbly because as I said, I have no inhibitions about opining about terrorist groups; I am on much thinner ice when it comes to discussing the U.S. government and its organization.) The old mantra that the interagency system is broken does not apply today; the interagency has been replaced by a far more efficient and effective system, but it is a system that—as our adversaries are constantly changing, adapting, and strengthening their capabilities—has to similarly be replenished.

The key elements to enhance interagency operations focus on the human factor and encourage effective interpersonal relationships; this entails building bridges across agencies and creating institutional incentives to blend diplomacy, justice, economic development, finance, intelligence, law enforcement, and military capabilities in a holistic struggle through individual and interagency relationships. It also entails using creative processes to ensure maximum efficiency instituting viable comprehensive mechanisms to achieve better integration in the formulating, implementing, and executing policy. These measures must include the power to disentangle lines of authority, deconflict overlapping responsibilities, improve communal abilities, prioritize and synchronize institutional operations, and build both institutional memory and human skill sets. These combinations of knowledge and ability can enable organizations to reach across bureaucratic territorial divides and share resources to defeat terrorists and insurgencies and to identify and counter emerging threats in a timely and more efficacious manner.

To conclude, how do we effectively counter al Qaeda and manage the jihad threat? First and foremost, we pursue the policy we have been following, a divide-and-conquer strategy that seeks to isolate the most radical, violent extremists from the more moderate elements. Second, this entails constant efforts that are directed toward watering down the al Qaeda brand, which after all is perhaps one of the most recognizable brands in the world today.

Third, we continue similarly constant and unyielding efforts to counter al Qaeda recruitment by communicating more effectively with the core demographic from which it draws its strength—in essence, young people. Fourth, continue to undertake and implement efforts to isolate al Qaeda intellectually and theologically. Fifth, continue efforts to counter al Qaeda finances, which have to be similarly unyielding and unrelenting. Finally, develop and enhance the support of local initiatives in concert with host nations to address the specific root causes that give life to al Qaeda and enable it to continue to replenish its ranks. This strategy assumes that we cannot have a one-size-fits-all solution but rather have to tailor local and national solutions to countering this problem.

In conclusion, what is needed to deal with these new threats and challenges is a capability to anchor changes that will more effectively close the gap between detecting a regular enemy activity and defeating it. The key will be to harness the overwhelming kinetic force at our military's disposal as part of a comprehensive vision to transform capabilities to deal with irregular and unconventional threats while simultaneously utilizing all instruments of our national power in a concerted effort.

Q&A SESSION WITH BRUCE HOFFMAN

Q: *What is al Qaeda's struggle for?*

Bruce Hoffman – What is al Qaeda's struggle for? Actually, that is an excellent question. This, I think, is also part of al Qaeda's strength: al Qaeda's idea—its objective—depends on who you are and what you are; and that is what their struggle is. They have tried to appeal to as diverse and broad a constituency as possible. That is the only way that they can encourage, replenish, and sustain this variety of networks.

I think if you reduce it now to its bare minimum, one can say that the purpose of al Qaeda's struggle is broadly to reestablish the Caliphate and to recreate super or transnational Islamic rule as it existed in the 7th Century, extending from Andalusian Spain across North Africa through the Middle East and Central Asia and South Asia to Southeast Asia.

That is their broad aim. I think they tailor their local aims, depending on local conditions, sensibilities, and needs. This is what has been so difficult for us in countering the al Qaeda narrative; it is not one narrative, and it has to be tailored to the individual circumstances. Because from al Qaeda's point of view, people fighting in North Africa, for instance, may have very different tactical interests certainly than those fighting in East Africa or in South Asia.

Al Qaeda from the start always wanted to be a big ten. That was part of bin Laden's vision to create this unified force against the "Crusaders," just as his 1998 fatwa stated. To make that effective, however, it had to have very flexible and very malleable long-term aims to bring in as many different groups as possible and to have the broadest appeal. That has been al Qaeda's success; it has the big picture aim, but it also caters very effectively to local concerns and local aims.

Q: *Thank you professor. Words count. The Founding Fathers of our country were patriots and heroes from our perspective, but the British Empire called them traitors and turncoats. Today, one man's stimulus program to invest in the future of America is another man's socialism. From a social constructive point of view, in other words, words count. I do not know if you have seen the recent report that apparently we are no longer referring to the Global War on Terrorism or the Long War; we are referring to Overseas Contingency Operations. What does that mean? What is the import, from your perspective, of a change in language, which I think can be very powerful?*

Bruce Hoffman – That is an excellent question. It raises a very important point, and you are absolutely right that words count. On the one hand, the terminology, the phraseology, Global War on Terrorism, has outlived is usefulness. I am not saying it was inappropriate in 2001, 2002, or even 2003, but I think in recent years, unfortunately—and just as you said, words count—even though Global War on Terror means one thing to us, in many quarters in the world, it is been interpreted not as a global war on terrorism but a global war on Islam.

We need a new concept or construct. Frankly I always thought the Long War was exactly the most important one because it demonstrated that this is not a conventional type of conflict that is going to end—as President Bush said, as President Obama has said, as many people have remarked—it is not going to end with the fate of a single enemy in a single place that results in some terms of armistice and an end to the struggle.

I think the pushback on the term, the Long War—which we saw in the Bush Administration as well at the end of his term in office, so it is not completely new—came from the concern, which actually is a very genuine one, about the American public's ability to sustain this struggle. We already have a well spring of sentiment in this country that says, "Seven and a half years and there has not been a major attack from al Qaeda." I am not saying that this is my opinion, but these are the arguments that you hear.

Al Qaeda posed a threat that was inflated for political reasons by the previous administration; the time of worry has passed, and we can somewhat relax our security, especially at a time of very hard choices being made over budgets, that we can perhaps begin to shift money from security to other needs. In my view, this is not exactly learning a lesson from 9/11 when we underestimated al Qaeda and its power prior to those attacks—and, of course, we are reaping the consequences because it is exactly when we lower our guard that al Qaeda will be poised to strike, and the damage will be that much greater.

All that still does not answer your question, though. To me, "Overseas Contingencies" is so vague, almost to be meaningless, and I think it is worse than the Long War because it deemphasizes or diminishes a struggle that is enormously consequential, even if it is not a conventional war and also leaves this as open ended.

I have always thought—although people disagree with this as well—that a phrase like Global Counterinsurgency would have been a much better one to use once Global War on Terrorism outlived its usefulness. The only reason I say that is because this is actually something that I mentioned here two years ago: Counterinsurgency by definition involves parallel political, economic, and social initiatives as well as the military ones. By its definition, counterinsurgency is not only the kinetics but the nonkinetics, and in my view, that would be a much clearer depiction than the sort of amorphous concept of Overseas Contingencies. I think it is a huge mistake.

Q: How do you attack them intellectually and theologically and at the same time not isolate the rest of the Muslim world or particularly the Muslims in the U.S.?

Bruce Hoffman –The question, which is actually an excellent one as well, is how do we counter al Qaeda effectively theologically and ideologically without really undermining precisely the moderate Muslim voices that we need to strengthen. First, and this was actually the subject of the lecture I gave two years ago here. I think we have to better know the enemy than we do now.

Last year, for instance, Congresswoman Jane Harman introduced legislation to have a Commission on Radicalization that would bring together the best minds in the U.S. to assess precisely how al Qaeda radicalizes and uses the power of theology and religion to effectively reach its supporters. Although it was successful in the House vote, it did not make it past the Senate and also generated widespread condemnation and opprobrium that this was some form of thought control that the U.S. government was attempting to control the Internet. It got out of control.

We need to establish that knowledge base. The one important step forward is the Washington Institute for Middle East Policy (Matt Levitt is here and will speak later today) just released a very prescient and incisive report on the whole process of radicalization that provides one of the foundations from which we can build. The key is a much more detailed understanding and knowledge of how this is being used.

Then, of course, combined with a very light touch by strengthening moderate opinion, we cannot put them in the cross hairs of the terrorist threat. Countries like Saudi Arabia, in particular, and also Singapore, have models of rehabilitation of terrorists that have provided some insight into how theologians and clerics interact to help influence and rehabilitate terrorists, providing us with another foundation. These are the essential building blocks that even after seven and a half years of the War on Terrorism we have only started to address. This radicalization report was long overdue, and it is to the credit of the Washington Institute that they embarked on it, which we should have been doing some years ago when moving out ahead of this.

Q: *I had first a comment and then a question. The comment regards using the term Global Insurgency. My biggest problem with that is that there is an implication of a global government and an insurgency against it. It seems that unless we are willing to deal with the implications of either the U.S. being a global government or the UN, there is a link missing there that we would have to deal with. I thought that you had a really good point regarding how we need a systems approach, but my biggest challenge with that is how do we have a systems approach in a linear focused society, particularly when money and resources are disseminated based on quantitative methodology?*

Bruce Hoffman – That is a very good question and actually an excellent point about insurgency. When I conceptualize insurgency, I think I may look at it differently than you do, perhaps very differently than others: The core of insurgency is mass mobilization. That is what separates insurgency from gorilla warfare, which is the hard tactics, or from terrorism, which is often specific acts designed to elicit fear and anxiety and therefore compliance at the terrorists' hands.

If insurgency is really about mass mobilization, and about the propaganda and the radicalization side of it as well as the fighting side, that is exactly what we face throughout the world. When you have the seven theaters, I do not want to portray al Qaeda as this monolithic, bin Laden is something like a satyr that is able to push buttons and pull levers that illicit responses. It is a very loose network; that is the point. It is very much predicated on mobilization, and that is the heart of it.

In terms of the systems approach, you have put your finger on the pulse of what the problem is: we live and function as a society with very short time horizons; we live, exist, and breathe fiscal plans; and we expect results within a two-year Congressional election cycle, but especially within a four-year Presidential administration. We are constantly looking to identify metrics of effectiveness and success.

I do not have a good answer except to say that in some of these initiatives, there may not be tangible metrics of success or effectiveness. We may have to understand that the things we are doing now may not pay dividends for years to come. In fact, there may not be palpable identification that we have accomplished something, but we need to realize that these measures will be equally or perhaps even more enormously effective in the long run.

What I mean by that, to move from a level of abstraction to specificity, is that—this is why your question I think is so important—right now our entire orientation in fighting the War on Terrorism is directed against the most immediate threat against us, which it absolutely has to be. There is no doubt we have to kill and capture those who we know are out there attempting to kill and harm us.

One of the problems we face is an inability to look beyond the current generation of terrorists. That does not even mean that next generation of terrorists or insurgents; they have already been radicalized and indoctrinated, and they are training an army now. We are already looking, and we are fighting the next generation; this is going on at least another decade.

The most effective policy that I am talking about from a systems approach would look to the generation beyond the next, exactly to the children growing up in North Africa, the Middle East, South Asia, precisely those countries of the world that already have a disproportionate population of people under 17 years of age. A country like Jordan, for example, has a growing population. Right now, it is a third of people under 17 years of age, compared to the U.S. or Europe, which do not have that demographic problem.

You can see that the same grievances "root causes" that al Qaeda uses in each of its theaters of operations now could only become more appealing to people growing up in societies where there are no meaningful employment and educational opportunities, in societies that are even going to have difficulty feeding these young populations.

That is why you should not be so quick to do away with the Long War because whatever problems we have seen during the first decade on the War on Terrorism can only likely be magnified in the next decade, not only because of economic problems we face now but also because of the demographics. That is part of al Qaeda's strength; that is exactly the demographic that it seeks to appeal to. That is why there are at least 5,000 terrorist and insurgent Web sites throughout the world, because those are the people they are trying to reach and that is where the struggle will be. A measure of our effectiveness against that may not be seen for another ten years, but that is something that we have to get over.

REFERENCE

1. Robert F. Worth, "Saudis Retool to Root Out Terrorist Risk," The New York Times, 21 March 2009: http://www.nytimes.com/2009/03/22/world/middleeast/22saudi.html.

1.7 ANALYSIS SUPPORT FOR THE INTERAGENCY

Eric Coulter

INTRODUCTION

In the quote from Secretary of Defense Robert M. Gates, the highlighted phrase is the focus of this presentation. Note that I am paid to be a cynic. What I say today are my own personal views, not that of the DoD; it is a very limited point of view. I may ruffle a few feathers. I do not know everything, and neither does my staff.

"War is inevitably tragic, inefficient, and uncertain, and it is important to be skeptical of systems analyses, computer models, game theories, or doctrines that suggest otherwise." This is what I am going to try to cover today, with some caveats. I am going to talk about analysis, but when I say "analysis," I am talking about analytic support to planning and programming, and it is going to be mostly the former and very little of the latter. When I talk about "programming," I am talking about building a five–20 year defense program. I am going to talk mostly about analysis in support of strategy planning requirements.

Mr. Eric Coulter serves as the Deputy Director of Strategic Assessments and Irregular Warfare Deputate for the Office of the Secretary of Defense, Program Analysis and Evaluation. He served as the Director of Projection Forces Division, Program Analysis and Evaluation. He retired from the U.S. Army after 20 years of service as an Air Defense Officer and Operations Research Analyst in a variety of leadership, staff, and analytical positions. He is an active participant in the recruiting, mentoring, and recognition of future and current SES members. He was honored with the Presidential Meritorious Rank Award in 2006, Secretary of Defense Exceptional Service Award in 2001, and other DoD and Army Meritorious Service awards.

I was asked to talk about myths. I am not sure I really know any. I have heard a lot about the television series "24" and the character, Jack Bauer, who works hard countering fictional domestic terrorist threats. Given my limited perspective, I think the myth is that the federal government does a lot of planning and exercises and really knows what is going on. I think that is a myth. I have not seen a whole lot of that, which I will address shortly. My focus is on support to analysis (planning and programming). I am not necessarily talking about the fact that we ran 100 exercises last year because there is a difference.

". . . no one should ever neglect the psychological, cultural, political, and human dimensions of warfare. War is inevitably tragic, inefficient, and uncertain, and it is important to be skeptical of systems analyses, computer models, game theories, or doctrines that suggest otherwise. We should look askance at idealistic, triumphalist, or ethnocentric notions of future conflict that aspire to transcend the immutable principles and ugly realities of war, that imagine it is possible to cow, shock, or awe an enemy into submission. . . "—Robert M. Gates, "A Balanced Strategy," Foreign Affairs January/February 2009

Another possible myth is that there is no interagency analysis or planning. In fact, there are some. I will describe how we do it. DoD supports interagency analysis. You have to remember DoD is a very complex organization: four services, numerous defense agencies, the Joint Staff, and the Office of the Secretary. In a sense, it is its own interagency, so what I am saying here may serve as a model or a paradigm that could then be applied to the interagency. However, there are cautions with that.

RESPONSIBILITIES OF THE PA&E

First, I will tell you a little bit about my job. The Director of Program Analysis and Evaluation (PA&E) is responsible for providing independent program analysis and evaluation to the Secretary of Defense, with responsibilities to:

- Analyze and evaluate plans, programs, and budgets in relation to U.S. defense objectives, projected threats, allied contributions, estimated costs, and resource constraints.
- Review, analyze, and evaluate programs, including classified programs, for executing approved policies.
- Provide leadership in developing and promoting improved analytical tools and methods for analyzing national security planning and the allocation of resources.

The most important responsibility of mine, and my staff's job, is to provide objective, independent, and fact-based analysis. I am emphasizing those three terms, particularly fact-based, because it is so difficult, believe it or not, to get people to agree on the facts considering all the components (i.e., the four services and a myriad of defense agencies). That is a difficult thing to do because they have their own agendas, and the facts you may put on the table may not support their agendas.

The third bullet, "Provide leadership in developing and promoting improved analytical tools and methods for analyzing national security planning and the allocation of resources," is essential: We believe it is our responsibility to help do that wherever possible, not just within DoD. I will give you some examples of where we have done that.

THE ANALYTICAL CHALLENGE

Although Ron Luman discusses Figure 1 in detail in his introduction, I want to revisit it to discuss the analytical challenge and the role of the interagency. In the "Traditional" quadrant (lower left), in which we have been operating for decades, there really was not much need to work through the interagency. The analytical challenge is straightforward; DoD gets the analysis: Fight the war on the central plains of Europe. There may be some policy involved in it, but it is mostly kinetics; it is warfare.

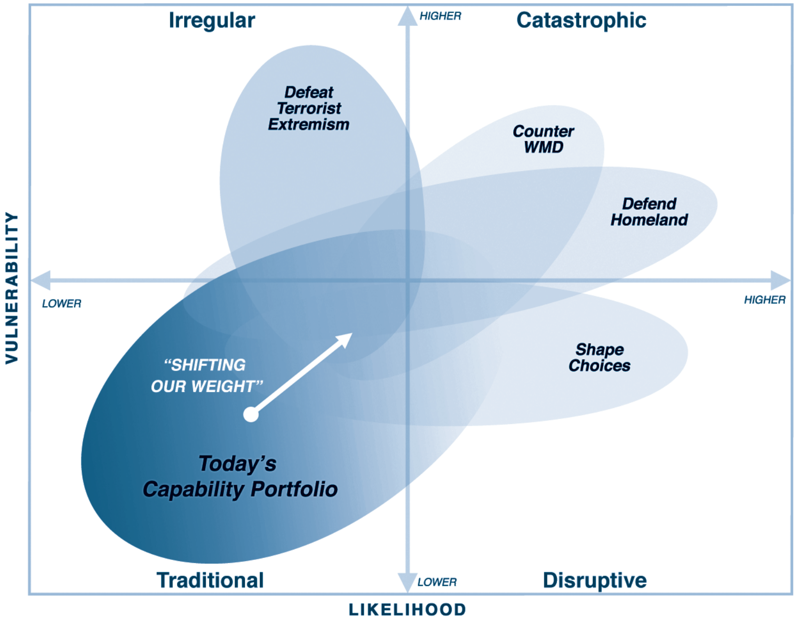


Figure 1 DoD's Analytical Challenge

As you move up into the Irregular and Catastrophic quadrants, analysis is more concerned with soft power. All the elements of the national government need to play. We are trying to move DoD in this direction.

Our infrastructure within DoD is very mature; we have been practicing operations research and analysis in support of planning since World War II, when operations research was started. Most of our analysts, whether they are military or civilian, have great academic credentials. They have masters and doctorates from good universities. Most of our analysts also have operational experience, which is extremely valuable when you are conducting analysis.

In reference to Secretary Gates' statement, "be wary of the analyst," our analysts who have operational experience use it to temper what they do and what they say when they conduct analyses. It is critical. We need to consider that when setting up analytic organizations in other agencies.

We have developed expertise applying tools, methods, and models in analyses. We have reached a point now, after six decades of continuous refinement and evolution, where we generally agree on the tools that we use. It is not 100 percent agreement; the services have their own tools focused on stovepipe service requirements. We do have some joint tools that span all of the areas of traditional warfare. We are working on tools for the soft aspects of warfare (e.g., psychological). We have made a lot of progress, but we are nowhere near there. We are basically five years into this, and it takes a lot more time. We have invested substantial resources in research, development, and sustainment of our tools, data, and people. We also have procedures for Validation, Verification, and Accreditation (VV&A).

In 1995, we stood up a new organization chartered by the Deputy Secretary called Joint Data Support (JDS), a core organization that develops, maintains, archives, and manages data and studies for the analytic part of the DoD. I think it has been a real success. Basically, if you are an analyst, wherever you are in DoD, if you have access, you can find the data that you need, or it can be made available. Another requirement I have for analysts is that whenever you conduct a study, you must be able to recreate the experiment; you have to be able to replicate it. We archive all our data, tools, briefings, and minutes in JDS, so we can go back and use it to replicate studies.

In conducting threat analyses, we work closely with the intelligence community: They provide us with products, and we help them as well. Recently, my staff helped the National Intelligence Community (NIC) conduct an assessment for a National Intelligence Estimate (NIE), which I thought was groundbreaking. I thought we did a good job for them. I think they were satisfied customers.

WHAT IS THE DOD ANALYTIC AGENDA?

I think what we call the DoD Analytic Agenda is a potential model for the interagency process; it has strengths and weaknesses that you might use to apply to an interagency process. We started this effort seven years ago; many in attendance at this symposium have helped us bring this to fruition. I think we are actually now at the point where it is effective.

The Analytic Agenda is a collaborative effort to make DoD strategic analyses more effective, efficient, relevant, and responsive—to ensure that we work on the same set of challenges. Why have we developed the Analytic Agenda? We have four services and multiple defense agencies with their own agendas, and they all want to row in different directions. What we are trying to do with the Analytic Agenda is get everybody rowing in the same direction and working on the same set of challenges. Believe it or not, that is very difficult to do. One way we do that is through scenarios, which I will discuss shortly.

Another objective was to be transparent and collaborative. For instance, we have an analytic governing body that meets once a month, or as needed, at my level. We discuss issues, review studies and analyses, and try to deal with these issues in real time. I think it has worked fairly effectively. The timeframes for the analyses we produce are current and future. For the Joint Staff and the Combatant Commanders (COCOMs), we focus on current operations. For the Office of the Secretary of Defense (OSD), Joint Staff, Services, COCOMs, Defense Intelligence Agency (DIA), and the interagency, we create scenarios for future timeframes, five and 20 years out. Products include Defense Planning Scenarios (DPSs); Concepts of Operations (CONOPS) and Forces (Multi-Service Force Deployment documents); Current and Future Year Analytic Baselines and Studies; and data, tools, and methods.

The guiding principles are the focus on the same set of challenges; open, collaborative, and transparent processes; and proactive, regular, and frequent senior leadership involvement. When the Secretary of Defense or the Deputy Secretary Service Chief ask a question, they want an answer yesterday. As an analyst, you typically cannot respond that quickly. If you have to start from scratch, you will never get there. Therefore, the Analytic Agenda is a way for the analytic community to do our homework.

We have found that, typically, if you do your homework and do it well, you will be 80 or 90 percent of the way there when a question is asked, and you can take something off the shelf, modify it, and answer the decision maker fairly quickly. If you do not do that, you will never get there because the issues we deal with are so complex and data-rich that you just cannot get it done in the time that they want.

Figure 2 illustrates the Analytic Agenda future-year process; many of you are familiar with this diagram. The process constitutes a defense strategy that can also apply to the interagency. We spend a lot of time creating scenarios, so I will return to this topic to talk about what I think needs to be in an interagency scenario.

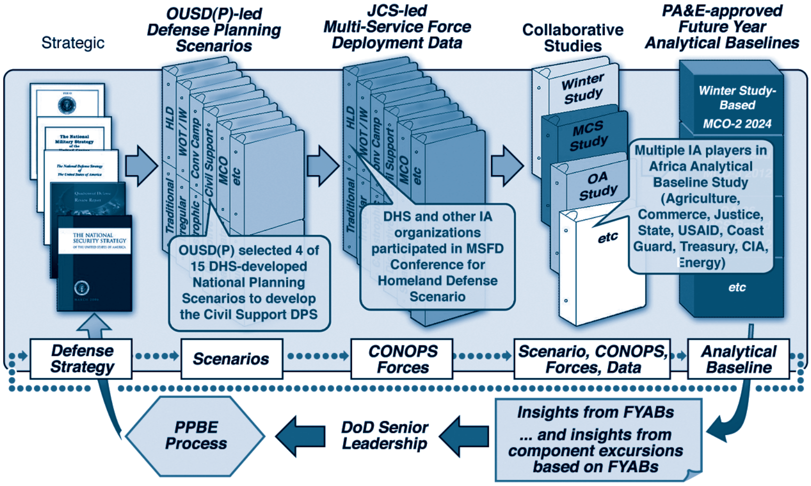

Strategic
OUSD(P)-led Defense Planning Scenarios
JCS-led Multi-Service Force Deployment Data
Collaborative Studies
PA&E-approved Future Year Analytical Baselines
The National Military Strategy
The National Defense Strategy of The United States of America
Quadrennial Defense Review Report
THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA
HLD
WOT / IW
Conv Camp
Civil Support
MCO
etc
Traditional
Irregular
Catastrophic
OUSD(P) selected 4 of 15 DHS-developed National Planning Scenarios to develop the Civil Support DPS
DHS and other IA organizations participated in MSFD Conference for Homeland Defense Scenario
Winter Study
MCS Study
OA Study
etc
Winter Study-Based
MCO-2 2024
Multiple IA players in Africa Analytical Baseline Study (Agriculture, Commerce, Justice, State, USAID, Coast Guard, Treasury, CIA, Energy)
etc
Defense Strategy
Scenarios
CONOPS Forces
Scenario, CONOPS, Forces, Data
Analytical Baseline
PPBE Process
DoD Senior Leadership
Insights from FYABs
... and insights from component excursions based on FYABs

Figure 2 Analytic Agenda Future-Year Process

Future defense analysis begins with strategic guidance that serves to shape the capabilities and CONOPS examined in the Department's analysis efforts. Documents such as the National Security Strategy and the National Military Strategy, among others, provide the strategic priorities to focus DoD assessments and resource planning.

The OSD for Policy, in collaboration with the Joint Staff and PA&E, conducts a net assessment of all of the strategic demands for DoD capabilities and leads the development of a set of defense planning scenarios that define a representative set of threats and military operations to be used for planning and programming. These scenarios broadly define the scope of each contingency, including objectives and assumptions for each participant in the conflict.

For each scenario, the Joint Staff leads a collaborative effort to develop Multi-Service Force Deployment (MSFD) data. The MSFD specifies the joint military forces and CONOPS for each participant in the scenario. PA&E, the Joint Staff, and other participants in the Analytic Agenda lead collaborative studies of each MSFD. These studies examine a range of cases to understand how changes in assumptions, CONOPS, and critical system performance parameters affect the scenario outcome. PA&E is then responsible for documenting these studies in Analytical Baselines. Completed Analytic Baselines are posted to DoD's Joint Data Support office. The Analytic Baselines include all of the data, model input and output files, and the programs associated with each model. Analytic Baselines are intended as the starting point for any future study of a particular scenario within the DoD.

In the Analytic Agenda, we are developing scenarios to assess our capabilities and CONOPS in a variety of irregular warfare contexts, including counterinsurgency, counterterrorism, the Global War on Terrorism, and stability operations.

"The Analytic Agenda is a collaborative effort to make DoD strategic analyses more effective, efficient, relevant, and responsive—to ensure that we work on the same set of challenges."

Part of the process you do not see in Figure 2 is what we call the "snake," where DoD senior leaders are involved in helping us describe what the key challenges, assumptions, and constraints are so that we can narrow them down to the questions that they really want answered. The scenario comprises all of these elements. It provides the context for the scenario (e.g., the environment). Once the scenario is developed, we determine the

CONOPS: how we are going to achieve the objectives that are stated in the scenarios. We then conduct a series of studies with the various components. We will pick one of the components, or several of them, and create a baseline, which is archived in the JDS system and available for everyone's use.

The key point here is: we do not want to stymie ideas or new ways of competition. In essence, we create a sandbox in which every aspect is very well described. When an analyst wants to step outside the sandbox and look at some new aspect, that is great, but when they step out, we want to know what they have changed. This process helps the analyst conduct a study, and it helps us communicate what changed. The senior leaders know what is in the sandbox because they helped define it.

Once we have these insights from various studies, the cycle repeats: The senior leadership will use those insights to make decisions, whether it is policy, strategy, planning, or programmatic, it gets washed through our process. In theory, if we do this right—actually we are struggling a little bit with this because we are not as responsive as we should be—but when it works right, I would like to believe that this process would feed back and affect the strategy. If the strategy, for example, is not achievable because we do not have the resources to do it, then it is not a good strategy.

Also, for the Defense Planning Scenarios, other agencies are invited to help us set up the scenarios. I have to say that although they have very limited involvement, their input is extremely useful as we create the challenges that we want DoD—and actually the entire federal government—to address.

INTERAGENCY COLLABORATION

Here is a quote from the latest DoD documentation stating the mission of PA&E:

> *"PA&E, with the Chairman of the Joint Chiefs of Staff and in coordination with DoD Components, manage the development and use of appropriate analytical models, tools, and data to support the analysis of the U.S. Armed Forces for IW" (DoDD 3000.07, 1 December 2008).*

You will notice that in the preceding description, the term “interagency” is not used. So the question is: how do we implement interagency collaboration? In our current approach, we do the following:

- Utilize interagency support at a level they are able to support.
- Use contractors with experience supporting the interagency to provide interagency perspectives and fill the gap.
- Use DoD surrogates [e.g., Special Operations and Low-Intensity Conflict (SOLIC), Assistant Secretary of Defense for Homeland Defense (ASD-HD)].
- Leverage Joint Staff J7 office that coordinates interagency participation in exercises.

We begin by asking the interagency, and they try to do what they can, but they have limited resources. Sometimes, we will have an exercise in which we will want a particular agency to show up, and they will say they will show up, but they do not. This may be where I will start ruffling some feathers. For example, I am going to pick on the Federal Emergency Management Agency (FEMA). We ran an exercise called “THOLIAN WEB” in March of 2005. The exercise scenario began with a 10-kT nuke going off across the river in downtown Washington, DC. Most of the interagencies were there, plus local and state governments. FEMA was supposed to come, but they did not. I think they would have actually found it to be a wonderful exercise.

“If you are not including the analytic community when you run exercises, you are losing or wasting a valuable resource.”

That exercise was essentially set up, run, and captured by analysts. That is different from the exercises conducted in 2006. Analysts have a certain set of skills: we have tools, we know how to look at data, and we can connect dots in different ways than other people. So I think we bring something different to the table.

If you are not including the analytic community when you run exercises, you are losing or wasting a valuable resource.

Recent Interagency Analyses

The following are some examples of recent work that PA&E has done with the interagency.

- **Civil Support Analytical Baseline Study** (completed)
    - Based on Department of Homeland Security (DHS)-developed National Planning Scenarios
    - Assess national ability to save lives and mitigate suffering in response to terrorist attacks (nuclear, chemical, bio) and natural disasters (earthquake)
    - Support received from DHS, Health and Human Services (HHS), Department of Transportation, state and local governments
    - Nuclear attack scenario (10-kT improvised nuclear device in Washington, DC) informed by local/state/interagency wargame THOLIAN WEB
- **Homeland Defense/Civil Support Capabilities Based Assessment** (completed)
    - NORTHCOM-led; interagency support from DHS and DoD components
    - Highlighted need for national-level risk assessment across types of national security threats
- **Homeland Defense Analytical Baseline Study** (ongoing)
    - Assess national ability to interdict state sponsored terrorist attacks (intercontinental ballistic missile, maritime, air) on the homeland
    - Seek participation from DHS and its components, FBI, and others.

Note that this list is bottom up. First off, the DHS developed 15 National Planning Scenarios. OSD Policy picked four of those for the analytic community to analyze. We conducted those exercises in the *Civil Support Analytical Baseline Study* and learned quite a bit. I will give a specific example. Contrary to what I have heard here today—and again I am paid to be a cynic—at least from my perspective, my senior leadership anticipates that if something really bad were to happen they would expect DoD would lead the response. They say that because DoD is often called to respond when something really bad happens; DoD has the people who know how to respond quickly. I am not sure I agree with that, but that is what I was told.

Typically, particularly in THOLIAN WEB, we found that the local and state governments are overwhelmed; as VADM Harvey Johnson mentioned in Roundtable 4, this is often the case. What we found is that state governments are not going to want to give up many of their resources. For instance, if an event happens in Washington, DC, and you need the Florida and Georgia National Guard support, I do not think you can count on it because their support may jeopardize their ability to respond to something bad happening in their state. In such a situation, they are not going to release those resources. Even if they did, it would take some time to get to Washington, DC. However, in this particular scenario, DoD would provide well over 125,000 people to respond. In fact, much of what VADM Johnson mentioned was about DoD being a coordinating cell that facilitates exercises. What is DoD's true role in a major catastrophe like that? An analyst will help you discover that.

In the *Homeland Defense/Civil Support Capabilities Based Assessment*, NORTHCOM, which is a fairly recent phenomenon that is still in the process of standing up, is just now starting to produce some good results. PA&E is helping NORTHCOM as much as possible, but it will take a year or two to provide national-level risk assessments for all types of threats.

The *Homeland Defense Analytical Baseline Study* will involve multiple agencies that will participate in various exercises. Again, they sometimes are frustrated because they have very limited manpower. They think what we are doing is really important, but they have limited resources.

Economic/Financial Analyses

Some time ago, we were asked to consider the implications if an adversary wanted to attack us economically. The first question that may come to mind is, "Why would you ask DoD to do that?" Nevertheless, we charged ahead with the analysis without any prior knowledge because we do have economists on our staff who are very good at their jobs. We asked the following questions:

- How do economic and financial actions impact U.S. national security?
- What countries are susceptible to economic or financial leverage and how?

We conducted one-on-one interviews and seminars with 68 subject-matter experts from government, academic, commercial backgrounds, including Lawrence Summers, former Secretary of the Treasury Department and current Director of the National Economic Council (NEC), and many other experts. Much to our chagrin, we could not find (again, from our limited point of view) anyone really thinking about this problem in a deliberate, analytical manner. We just could not find anyone conducting serious, systematic studies—and that is a problem. We do not know if a concerted effort is underway, but if there is, we would like to know about it. We looked far and wide, we talked with senior leaders and many of the interagencies, and they all said, "This is a great idea, you should do it, and let us know how it worked out."

"Who in the government and within DoD should have the lead for assessing the impact of global financial and economic actions on national security?"

The Johns Hopkins University (JHU) helped us run war games with participants including the Departments of Treasury and Commerce, the National Security Council (NSC), the Officer of the Director of National Intelligence (ODNI), the Defense Intelligence Agency (DIA), and the Department of Energy (DoE).

We learned a lot from this effort. It was not our intent to take this function over; it was to get it started, ask the questions about who should do it, and then pass it on. We are in that phase now; we are wrapping this effort up and going to pass it on to—I do not know—Treasury?—to whomever it should belong. The real issue—the emergent question—is, "Who in the government and within DoD should have the lead for assessing the impact of global financial and economic actions on national security?" We are very concerned about what an adversary could do to our economic infrastructure, and there are many ways that they could affect it.

Counterinsurgency and Counterterrorism Analyses

Other analysis efforts include the following:

- **Africa Analytic Baseline Study** (ongoing)
  - Develop an irregular warfare (counterinsurgency, counterterrorism, and building security capacity) Analytic Baseline reflecting whole-of-government effort
  - Increase support from the U.S. Agency for International Development (USAID), Department of Agriculture (USDA), Coast Guard, Department of State
  - Improve tools, data, metrics for irregular warfare analysis
- **Counter-Weapons of Mass Destructions (WMD) Analytic Baseline** (complete)
  - Assess programmed capabilities to identify, track, and neutralize threat WMD capabilities
- **Guidance for the Development of Forces Irregular Warfare Study**
  - Led by SOLIC
  - Assess whole-of-government efforts to support unconventional warfare, counterinsurgency, and steady-state operations

  - Develop insights on needs for irregular warfare capabilities for Quadrennial Defense Review

The key here is that we have created a series of challenges that require significant interagency interaction to utilize our potential. If you return to the quad chart in Figure 1, remember that we were mostly down in the lower quarter conducting traditional warfare—central plains of Europe, Iraq, etc.—but now we have spread out. Ongoing efforts such as the African Analytical Baseline are nearing completion. I think we have learned a lot from it. The counter-WMD effort assessed the ability to identify, track, and neutralize WMD threats.

We are also conducting irrregular warfare studies. All of these ongoing efforts do have interagency support—to the degree possible. However, it is mostly from the bottom up: We ask colleagues in the interagency to come onboard, participate in the scenarios and exercises, and help conduct the analyses. It really needs to be top down, and we are not there yet.

LIMITATIONS

Most of my staff will tell you, even though I am a cynic, I am also an optimist. I always try to look at the bright side of things, but the glass is always half empty. In this case, though—a bit of qualitative analysis here—I think it is two thirds empty, one third full. The glass is two thirds empty in several respects, including the following:

- Roles, responsibilities, and authorities are unclear. DoD is being asked to fill in the gaps (e.g., economic study).
- Even within DoD, unrestricted warfare analysis is still new:
  - Models and tools are not mature; much of "soft power" and social domain defies quantification.
  - Data collection, management, and dissemination processes must be modified to address the needs of unrestricted warfare analysis.

- The interagency is not yet ready to participate fully. Interagencies lack analytical capability (models, analysts, and data).
- There are few, if any, dedicated analysis organizations. Agency culture and leaders are not familiar with decision support and planning.

"The military and civilian elements of the U.S.' national security apparatus have responded unevenly and have grown increasingly out of balance. The problem is not will; it is capacity." — Robert M. Gates, "A Balanced Strategy," Foreign Affairs, January/February 2009

With respect to unrestricted warfare—we call it irregular warfare—despite the definitional issues, which we need to talk about, we have some fundamental development issues. I can say with certainty that right now we know how to conduct a joint warfare analysis: tank on tank, army on army, fleet on fleet. We can do that well. However, much of warfare today—hybrid, irregular, unrestricted warfare—is not that; it is mostly concerned with soft power and social issues, and we really do not know how to do that. For the last four or five years, we have spent an extensive amount of our energy trying to understand that. We have consulted with anthropologists, historians, and sociologists to try to understand their science and bring it into our analytic capability. We have made some progress, but I think we are still a few years away.

The interagency is not yet ready to participate fully because they do not have the ability; they do not have the people. They may not have the data. They clearly do not have the models in some cases. Another aspect that I think is actually more important is that, unlike the instant analyses you see in the Hollywood version of reality such as in the television series "24," there is not much ongoing analysis that can be used to inform decisions. I just do not see it. Without a culture in which agency leaders rely on analysis to reduce uncertainty concerning a decision, without the ability to combine our analyses with their training, background, and caution (they should not trust us 100 percent of the time), I am not too sure how useful interagency analysis will be.

ACHIEVEMENTS

On the positive side—the one third of the glass that is full—we have made significant progress in the following areas:

- Several agencies are establishing analysis (planning and programming) organizations—internal PA&Es, if you will. DoD PA&E has contributed directly with analyst swaps, internships, and becoming a net talent exporter.
- Agencies have participated in numerous DoD analytic activities, including the DoD Analytic Agenda (limited) and the Military Operations Research Society (MORS), of which DHS is now an official sponsor.
- Several agencies have asked for DoD analytic help.
- PA&E has helped establish a common reference set of national security challenges.
- Federally Funded Research and Development Centers (FFRDCs) and other non-DoD analytic organizations have been established, many of which comprise diverse interagency talent, are heavily used by DoD, and are increasingly used by other agencies.

We have in recent years helped several agencies set up organizations like ourselves. The DoD PA&E has helped through consulting, analyst swaps, internships, and talent export to other agencies. For example, we have helped the DHS set up a PA&E. In fact, the Director of PA&E for DHS is a former OSD PA&E analyst. The National Oceanographic and Atmospheric Administration (NOAA) has established a similar program. An official from DoE visited me yesterday to discuss how DoE could set up an analytic capability. Veterans Affairs has also indicated that they would like to develop an analysis capability. Although we are helping others, I will caution you that just because this is the way we do it does not mean that is the way it should be done; there are obvious pros and cons.

We have to make the distinction between analysis for planning and analysis for programmatic development. Many of the requests right now are on the programmatic side, but they see what we do and how we use analysis to support planning. They like it, and they want to develop a capability to do that. Again, this process is completely bottom up. We are taking scarce DoD analytic resources and helping them, which we are more than willing to do and should do. I think it is good government—but we do not see much activity from the top down.

"Without a culture in which agency leaders rely on analysis to reduce uncertainty concerning a decision, without the ability to combine our analyses with their training, background, and caution (they should not trust us 100 percent of the time), I am not too sure how useful interagency analysis will be."

One of the most encouraging aspects is that if agencies want to set up analytic capabilities, the DoD is an excellent source for people with those skills. Many of our people have been hired by other agencies. The military services do a great job of educating their analysts. They go to top-notch operations research or other schools. They have operational experience, as appropriate. DoD is a good source of hiring talent, and many of the interagencies are doing that.

We also sponsor many professional societies such as MORS, and we conduct seminars similar to this symposium, in which we meet as analysts to discuss our plans and visions. We share models, tools, data, methodologies, and ongoing studies. These seminars are excellent opportunities for our guild to get together and discuss where we are going as a guild.

With respect to the 15 National Planning Scenarios, they are a good start in establishing a common set of national security challenges. We do need to further that effort, which I discuss in the following section. The FFRDCs have done a superb job of hiring talent from numerous agencies so that when we at DoD go to them about a problem, they have ample interagency experience on their staff to help us. I think they are ahead of us in doing that, so kudos to them.

INTERAGENCY COLLABORATION: THE WAY AHEAD

The following are some of the ways ahead to foster interagency collaboration:

- Leaders need to demand better decision support—but know its limits.
- To foster development of an Interagency Analytic Agenda, we need to:
  - Develop common/reference national security challenges (scenarios) for economic, cyber, and terrorist attacks, etc.
  - Develop and test interagency "how to" (concepts/doctrine).
  - Create an independent NSC-level PA&E-like organization to provide objective, fact-based analysis.
  - Charter/empower an interagency analytic governing body.
  - Develop transparent processes to collect, manage, and disseminate data across the interagency; access to classified data is a potential issue.
  - Develop common tools and data to conduct wargaming and modeling and simulation.
- Increase efforts to hire and develop analytic talent from academia and DoD by developing and promoting educational opportunities, managing careers for upward mobility, and establishing standards for a national security professional.

- Develop common taxonomies and lexicons (e.g., irregular versus unrestricted warfare).
- Support and participate in analytic research and professional development, from the agency side.
- Expand professional organizations, including the Institute for Operations Research and the Management Sciences (INFORMS) Military Analysis Working Group to include national security analysis, and MORS, which should have a new name.
- Establish a Quadrennial National Security Review (QNSR) similar to Quadrennial Defense Reviews (QDRs), which have served as a useful framework for prioritization of DoD requirements. For example, DHS is undertaking its first Quadrennial Homeland Security Review. Effective response to national security challenges requires a whole-of-government approach; QNSR would allow consideration of these complex issues in a coordinated fashion.

With respect to the first bullet item—leaders demanding better analysis support—even in DoD, the use of analysis waxes and wanes based on leadership. I have been doing this now for longer than I care to mention. I have seen leaders who really embrace this; they understand the limitations, but they really want to know what analysts think and how they are doing things. I have seen other leaders that just think analysis is a bunch of bunk and would not give us the time of day.

"My overarching concern is that we have done this all from bottom up. I think it needs to be done from the top down if we want this change to happen fairly quickly."

I believe we must establish an Interagency Analytic Agenda. The challenges are: How do you do it? Who leads it? Who participates in it? One thing that has been successful for us is that my colleagues—the senior analysts and the components—work together. It is critical to success to figure out how to work in an interagency context.

We need to create a body perhaps in the NSC to provide independent analyses. From interviews with those who have served on the Council, I have discovered that they do not do the kind of long-term planning I thought they did. I thought they planned for future operations and established clear objectives. As far as I know, they do not, so I recommend that the NSC should set up the scenarios with agency support and then charter studies and analytical efforts. We must also empower a governing body for interagency analysis, something like our version of the JDS system.

Developing a common lexicon is essential. When you talk to someone else in another agency—someone in the Army, for example—sometimes we just talk past each other. Therefore, we must invest the time to establish a common taxonomy so we can have common understandings of terms such as irregular warfare and unrestricted warfare. It is hard to do, but it has to be done. I sat through five meetings with the Deputy Secretary in which the senior leadership in the DoD was trying to figure out the definition of irregular warfare. After five meetings, some people still did not get it right. It is very important to get that accomplished.

National Security Planning Scenarios

We need a rich, prioritized set of scenarios that clearly define national security challenges and objectives. They must encompass economic, cyber, terrorist, and narco-drug challenges; have upfront senior leader buy-in; and balance depth, breadth, and limited analytic capacity. One thing we have always been concerned about in the DoD is the depth: How deep do you go into a scenario? How much detail do you put into it? How many scenarios do you conduct? What is the breadth of the things you are going to look at? Because we have limited analytic capability, how often do you go back and refresh these things—because scenarios have an expiration date, for whatever reason; the scenario, threat, or context changes, or you just need to go back and refresh it.

As a result, each scenario should:

- Provide a common starting point for analysis but allow for experimentation and new ideas and approaches as well as promote a competition of ideas.
- Set up the problem: describe its context (e.g., threat and environment).
- Have clear, obtainable, and stated objectives.
- Define and describe strategic approaches, the "how to," possibly requiring a wargame.
- Specify key assumptions and constraints, bound uncertainty, scope the problem, and define a "base case" (most likely, stressing, etc.) to anchor excursions and sensitivity analyses.
- Periodically update based on lessons learned and changing contexts.

What we have found is in many cases you will have stated objectives, you will have the context, but you are really not sure how to do it. There will be multiple ways to accomplish the objectives. You may need a wargame at the interagency level with the right interagencies participating to figure out how to solve a problem or at least propose how to solve a problem.

CONCLUSIONS

My overarching concern is that we have done this all from the bottom up. I think it needs to be done from the top down if we want this change to happen fairly quickly. I do not see that happening any time soon. However, we will continue using the bottom up approach. People like what we do. They are playing in our games. They are helping us make our games better. We are helping them set up their games. However, I offer the following set of cautions:

- Do not expect too much too soon: DoD can overwhelm others, so we may need to take less quantitative approaches.
- Do not expect analysts to have all the solutions. Interagency decision makers are not accustomed to using analysis to help them make decisions.
- The usefulness of interagency analyses is limited by the amount of interaction at the senior levels. How will government-wide decisions regarding unrestricted warfare be made? How will the integration and coordination occur?
- Be careful emulating DoD, which is struggling to use analysis to inform policy and strategy. Program advocates challenge data, tools "misdirection," and components protect their prerogatives.

Although we have an Analytic Agenda and it seems to be working, I must include the caution that it does so from our limited point of view. We have challenged it and evolved it over time. It is not perfect, but it does seem to work, warts and all. It does seem to serve the senior leadership, and we are happy with that. However, I do not know if what we have set up will actually work in the interagency. I think we would have to take lessons learned from what we do, both good and bad.

Q&A SESSION WITH ERIC COULTER

Q: *This is naïve, but it is not on purpose. If decision makers are not using analysis to make their decisions, what are they using?*

Eric Coulter – That is a good question. I admit it up front: I would love to see analysis focus more on planning that goes back and helps strategy. In my world view, however, we typically deal with—in the interagency context—DoE, DHS, and DoD. They will submit their program or participate. Who challenges their programs? Who says that this is the right thing to do? On what basis will the Office of Management and Budget (OMB) or the President or the Vice President—on what basis or criteria or analyses, will they decide to increase or decrease resources or make changes? From the analysis I am familiar with, I do not see a lot of that going on above us. I just do not see the implications of the choices and how much confidence decision makers have in the assessment of those alternatives.

Q: *Are you satisfied that we are developing an adequate number of properly trained analysts across the interagency to meet the emerging evolving threats that we will face?*

Eric Coulter – I will answer that question by first saying in DoD I do not think we are. Over time, it waxes and wanes, but right now we are having a shortage of mid-level analysts with operational experience. We do have two wars going on, so in DoD we have a problem. In the interagency, I do not have any data, so I have no idea what they are doing. I had my staff pull what they call a 15/15, which is an operations analyst research in the general schedule. Clearly, DoD has 95 percent of them. Interestingly enough, the next biggest group of 15/15s was in the Treasury Department. However, I do not have sufficient data and we have not conducted a study to answer your question.

Q: *As a follow-on to that, Mr. Flynn spoke of mobilizing national will in his dinner address. Do you think we need to try to mobilize a national will or recruitment of properly trained analysts, as we do occasionally hear a call for scientists or doctors or nurses or teachers? Do you think that within the DoD or interagency that we need to make that type of push to meet—to be prepared to meet—those challenges in the future?*

Eric Coulter – Given the complexity of the world we live in today, I think the answer is yes. But I will caution you that when I say "analyst," I do not mean that one necessarily has to be trained in operations research. My view is that many of my best analysts are physicists or mathematicians. So typically—and as we move into the softer areas—the best analyst might be an anthropologist. We are now bringing in anthropologists and we are using them. So every analyst does not have to be operations research trained.

The point is, does that person have an enquiring mind, are they willing to challenge the status quo? I hate to use the cliché of "Type A person," but I really think you need somebody who is aggressive and is willing to challenge the status quo and willing not to take "no" or "I don't believe that" for the answer. Another thing I think is a good trait for an analyst is the ability to network with people. If you are in DHS, for example, you have got to be able to go out and talk to DoD or FBI or any number of agencies. So I think a good analyst has to have personal skills too.

Q: *Have you given any thought to systematically engaging the analytic capability of industry in this work that you have ongoing?*

Eric Coulter – Yes, we have. First off, most of my analytic staff, probably a third of it is government; the other two-thirds are contractors. So contractors give me a lot of my analytic capability. Many of them I consider staff, but they just have a pink badge. We actually do work; I meet a lot of times with Boeing or Northrup Grumman or others on particular issues. The problem we have right now—and we are trying to work through it through our analytic governing body—is how much information can we share with contractors like Boeing, how much insight should we give them into our scenarios and everything else? That is a very good question. We are working through that issue.

Q: *How do you measure long-term systems approaches in a linear fashion?*

Eric Coulter – We actually do use a systems approach so that there is no question about how we have conducted an analysis. We do try to quantify as best we can, but we realize that much of what we do, particularly today, which requires "soft power," cannot be quantified. You might be able to describe ranges. If you are lucky, you might be able to document that.

We do know that the social sciences are trying to increase the quantification of what they do, and we are working with them, trying to understand that. Whatever we do, we document it so we can replicate it. Some of our analysis consists of our best judgment, or we go to a subject-matter expert and we get their judgment. I insist that we write that person's judgment down and archive it, so that can be justified as a basis, and we can go back and see what we did and why we did it.

Another example, believe it or not, is that we have hired the Census Bureau to collect data on relevant populations in various countries and provide us with information on the human terrain.

1.8 INTELLIGENCE SUPPORT FOR THE INTERAGENCY

Karen Monaghan

INTRODUCTION

I hope to offer some insights on the imperatives for interagency interaction as we think about these new threats from unrestricted warfare. Other speakers at this symposium—both this year and in previous years—have identified how unconventional warfare might unfold, who the likely perpetrators would be, what would be their preferred or their convenient targets of attack, and what various weapons or tools they might choose to inflict damage, whether locally or globally. As the National Intelligence Officer (NIO) for Economics and Global Issues at the National Intelligence Council (NIC), I need to think about these new threats from unrestricted warfare, particularly economic and financial attacks and resource wars, but also the cyber issue. My colleagues and I need to consider ways to monitor and warn about these new threats and, at least for the time being, address these new actors using the same resources that we have today (i.e., interagency resources for analysis, personnel, collection platform tools, and accesses). I think that is one of the biggest challenges to interagency action,

Ms. Karen J. Monaghan was appointed National Intelligence Officer for Economics and Global Issues in November 2007. She is serving her second tour on the National Intelligence Council, previously fulfilling the role of Deputy National Intelligence Officer from 2002-04. From 2004-06, she served as Deputy Chief of the Economic Security Group in the Directorate of Intelligence. Ms. Monaghan was a Visiting Intelligence Fellow at the Council on Foreign Relations (2006-07). She holds an MPhil. degree in International Relations from St Antony's College, Oxford University and an undergraduate degree in Political Science and Economics from Vassar College.

particularly on the economic and financial front: We need to figure out a way to leverage the resources we have.

THE MISSION

It is in this context that the Director of National Intelligence (DNI), in his annual threat testimony, identified the global economic crisis and its geopolitical implications as the primary, near-term security concern of the U.S. The DNI was right to identify that as a risk that can manifest into some kind of unconventional warfare through economic, finance, or resource attacks. Not just the severity of the global downturn but also the uncertainties about how the crisis will manifest itself, particularly geopolitically, put this crisis squarely in the realm of a national security issue.

Collection and analysis on global economic developments and their implications for politics and security and foreign relations have been part of the interagency's and the intelligence community's (IC's) mission for decades. However, the current economic crisis seems to be different. That is what makes it imperative for interagency collaboration and coordination on intelligence support. As such, the intelligence community needs to consider what opportunities the downturn might present for adversaries to exploit an economic or financial advantage; leverage or take advantage of low prices for assets including oil, gas, minerals, and even food resources; or perhaps prepare for or inflict a resource attack in the future.

About a year ago, I led an interagency effort to look at the potential geopolitical fallout from surging fuel and food prices. I brought the community together, and we particularly were concerned about fragile states. We wrote an analysis report; but unfortunately, the shelf life of that report was rather slim because, as you all know, we hit a peak for prices in July 2008, and they rapidly fell after that.

Today, we are concerned about the fallout from a severe global economic downturn, especially in countries where it might trigger social unrest and anti-foreign sentiments, damaging protectionism, and humanitarian crises. What does this mean for analysis collection, collaboration, and interagency action? I think as a community in the interagency, we are in the beginning of the learning curve.

A New Lens

However, some initial issues and avenues are apparent. The first of these is that we need a new lens. There is clearly a requirement for all interagency analysts—intelligence analysts in particular, and not just economists—to look at the threats, risks, and vulnerabilities that exist through this new global financial economic crisis lens as well as to consider the new threats that are spawned by such a global economic and financial crisis. Those threats in particular are economic leverage, financial leverage, economic attacks, financial attacks, and potentially resource attacks.

Another issue that I think has been raised is surge capacity. In the aftermath of 9/11, the IC and the policy communities demonstrated an impressive capacity to surge resources and tools to meet the terror threat, but the interagency is not likely to have the luxury of resources, budgets, bodies, and contractors. As you well know, all of these issues are being questioned. We are all probably going to have to take a bit of a haircut on them.

Multidisciplinary Analysis

How do we address this new mission and challenge if we do not have additional resources? How do we surge? How do we use interagency cooperation and collaboration to do as good a job on these new unconventional threats as we did on previous terrorist threats? In the short term, we need to focus on multidisciplinary analysis. Although Ph.D. economists and financial experts can bring and are bringing attention to these issues, the interagency needs to tap into a broader range of expertise to provide multidisciplinary and multidimensional analysis on the impact of the economic crisis and what the new threats might be as a result of this. We need to improve our coordination, share methodologies, compare methodologies, and devise new methodologies to marry economic, financial, and political risk analysis.

The risks and threats I have just mentioned, which arise from the current financial crisis, fall into what I would call traditional threat identification. Threat analysts and collectors, as I said before, just need to help fit the new lens. I see that my role as the NIO, as a representative of the interagency, is to help the analysts fit and adjust that new lens as new developments, tools, metrics, measures, and collection issues come up, apply them to the ones that they are already thinking about, and think beyond their stovepipes.

Yes, we still suffer from conical thinking; we are still very stove-piped. If an NIO is writing an assessment about China's military modernization, I need to remind him/her to focus through the economic lens to consider how the economic downturn might change his/her assessment. Chinese leaders are also thinking about how to create jobs for the 20 million migrant workers and the graduates that are coming into the workforce, who have now gone from export-led industries back to their rural areas. If there are competing demands for "investments" at a time when growth is slowing, how does this impact the Chinese leadership's thinking on where to put these investments? Maybe their plans and intentions do not change at all. However, it is imperative that we focus through that lens to consider, and it is our responsibility as NIOs, to help the interagency put that lens on.

Policymakers have told us what insights they want the intelligence community to:

- Put the economic and financial constraints into context.
- Highlight the implications of the financial and economic crisis.
- Identify countries at higher risk of instability, i.e., those fragile states that might have a regime change.
- Identify not just the vulnerabilities but also the factors that add to resiliency.

We often consider the effects of a particular country that is poor, isolated, and commodity dependent. We can tell you all the fragilities and the risks to that country's political stability. We often forget to consider what factors add to its resiliency, and those are the issues that we need to think about.

OUTREACH

Another key responsibility of the interagency in identifying and thinking about unconventional warfare, particularly in the context of the global economic downturn, is outreach. The issues this symposium has been focusing on for the last two days are the less traditional threats. We need more expertise and more innovative thinking—what we have been calling "outside-the-box" thinking—in reaching out to the nontraditional subject-matter experts, the anthropologists, and the traders of commodities and derivatives. As Jim Rickards mentioned, they understand how a resource or economic attack might occur, how one could attack a financial system, and how one could use cyber warfare techniques to bring down a financial clearinghouse system like the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

The challenge for the interagency is reaching out and expanding the research to experts in the nontraditional agencies, such as the Commerce Department or the U.S. Geological Survey, to understand whether it is possible for a country to corner the market in a particular commodity. We might be worried about some of the acquisitions that are going on in international commerce. How important is tin as an industrial metal today as it might have been 50 years ago? We should reach out to the Federal Reserve, the Securities and Exchange Commission (SEC), and the Department of Justice to get their insights on what threats and vulnerabilities they see and are worried about.

In the intelligence community, we look at the foreign adversary or ally; we do not look at the U.S. Often, our perception of U.S. weaknesses and threats to national security is very limited because we only see one side of a story. We need to talk to, reach out, understand, and share information with the agencies that are focused on the U.S. We need to work with these agencies to develop metrics and methodologies for detecting anomalies in trading activities or capital flows.

Traditional intelligence analysts typically rely on tippers from human intelligence (HUMINT) or signals intelligence (SIGINT) to detect anomalies. This allows them to get some kind of an indication that there is a terrorist financier; they may even have the name or location. In contrast, other agencies, such as the SEC or the security offices in the New York Stock Exchange, look at anomalies in flows. They do not often have the advantage of the tipper. So, sharing and comparing the tippers and the flows is an important aspect to being able to figure out what the risk or threat actually is.

We need to match the skills and techniques of analysts from the SEC, the Commodity Futures Trading Commission (CFTC), other agencies, and private industry, all of which watch flow activity. As I mentioned, outreach needs to extend to the business community as well: traders, auditors, CEOs, and those in the trenches who have forensic accounting experience and expertise working in financial markets. Their ground truth can help us figure out what early warning we can provide to the intelligence, defense, and policy communities.

The lesson the SEC learned from not following up on allegations of the Boston hedge fund executive, Harry Markopolos, who gave the SEC warnings about Bernie Madoff's financial practices a decade before the Madoff Ponzi scheme was uncovered should be a lesson for the intelligence community as well. There are voices out there who we may not listen to, who we may think are slightly crazy, but we need to have our ears and eyes open to those nontraditional sources of information, which may be the most important warning system that we have.

Beyond the U.S. shores, we need to reach out and work on collaborating and cooperating with allies and their agencies to get the full picture of potential, transnational, illicit, or even licit, activities, particularly when money is changing hands in over-the-counter trading activities that may be occurring in places like London, Switzerland, or Dubai. We cannot handle unconventional warfare on our own.

Globalization has made unconventional warfare a global activity, and if we just see it from the U.S. perspective, we are going to miss what is happening, particularly as the adversaries that are out to get us are going to do everything that they can do to avoid putting a fingerprint on U.S. shores. We may be the subject of the attack, but all the operations may be occurring overseas.

"The lesson the SEC learned from not following up on allegations of the Boston hedge fund executive, Harry Markopolos, who gave the SEC warnings about Bernie Madoff's financial practices a decade before the Madoff Ponzi scheme was uncovered should be a lesson for the intelligence community as well."

Those are just the highlights of what the interagency needs to do to collaborate and cooperate to understand and identify metrics and early warning systems on some of these unconventional threats. I will open the floor to questions to explore these issues or answer questions on other issues.

Q & A SESSION WITH MS. MONAGHAN

Q: *Are there barriers of authorities for sharing this information across the interagency?*

Karen Monaghan – Yes, I should have mentioned that it is a bit tricky sharing information between intelligence and law enforcement. Although, after 9/11, the barriers came down to some extent, there are laws and legal barriers, particularly with sharing specific information. If we are working with the Department of Justice, for example, and they are trying to make a case, they do not want that case to be tainted with intelligence information because of the concern that information could not be used in a court of law. The intelligence community would not want the information to be subpoenaed.

In talking more generally about what we perceive the threats to be, we can consider what mechanisms or vehicles threat actors might choose to use to attack the U.S. or exploit U.S.

vulnerabilities, and we can share information or ideas on what anomalies we or other agencies might be seeing. Those kinds of things we can do. If we achieve that through collaboration and cooperation, we have achieved a lot.

Q: *In terms of process—to the extent you can discuss—how is the President's Economic Intelligence Brief going? It seems that out of nowhere, National Security Advisor General James Jones, Larry Summers (head of the National Economic Council), Michael Froman (Deputy National Security Adviser for International Economic Affairs), Admiral Dennis Blair (Director of National Intelligence), and others are channeling information to the President of a purely economic and intelligence nature. It seems like it is a model of the kind of interagency cooperation we are talking about that has come up very spontaneously. I am just interested in how the process is working, whether you, the SEC, the CFTC, or the Treasury have any input.*

Karen Monaghan – The question is about the new publication called The Economic Intelligence Brief (EIB), which is a new product that is being provided to the senior economic policy makers, but also the principals who are recipients of the President's daily brief as well. I did a survey about nine months ago to look at the economic and financial resources across the community.

A database tracks the numbers, although the database captures everyone who declares himself or herself as an economist. That person could be working or teaching at one of the schools or could be a manager not actually doing anything economics related, so the numbers are quite inflated. The reality is that most of the all-source economic, financial, and energy analysts in the community reside at CIA. There are a handful of people at the Defense Intelligence Agency (DIA) looking at defense economics, and some energy economists at the Bureau of Intelligence and Research (INR) as well as the Department of Energy (DoE), but the brain trust is at CIA.

For nontraditional agencies, such as the CFTC and the SEC, there is not an intel shop, so a natural point of entry does not exist for all these agencies. What it devolves down to is analysts who establish personal relationships with subject-matter experts in other agencies. The NIC or other agencies bring in some of these speakers from the outside, and they are forever part of the Rolodex.

Use your collaborative community to ask, "Do you know somebody who can talk to us about commodities markets?" You will get somebody from the CFTC. Concerning some of the new threats and issues that we must consider now, another advantage we have is that many new entrants into the intelligence community are coming from previous careers. They might have been working at Lazard, just gotten a Ph.D. in agricultural economics, or are coming from Wall Street from the research office at Lehman Brothers; so, they have connections and knowledge.

Getting back to the EIB, it is not that the community was not doing economic intelligence analysis before. This is, in part, tailored and packaged in a way so that it is all in the same book. It was a request from senior economic policy makers, who in the past have seen more tailored economic analysis during previous crises. There was a request that the community reinitiate such a process.

Chapter 2

ROUNDTABLE 1

Responding to Cyber Attacks

2.1 MODERATOR'S SUMMARY

Thomas McNamara, Jr.

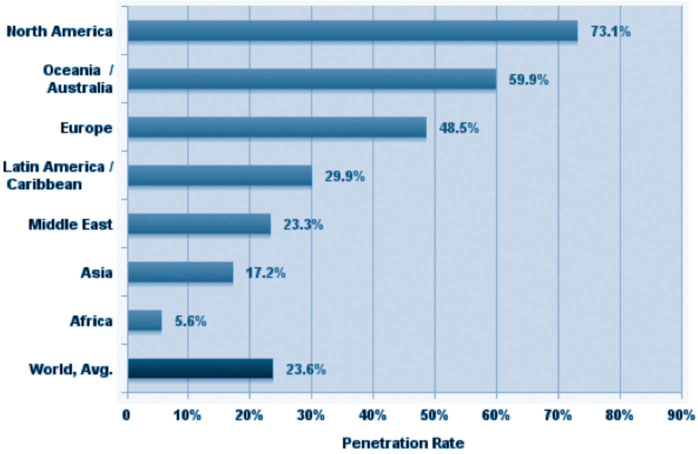
RELIANCE ON CYBERSPACE

Welcome to the first roundtable on dealing with cyber security threats and responses. What does cyber security really mean to us when we look at the U.S. and our access—as well as our vulnerability—in cyberspace? We are all familiar with the global information age, but that has also become an age of reliance, at least for the U.S., on cyberspace. As of 2008, U.S. access to the Internet exceeded 73% in terms of penetration of the total U.S. population. However, the U.S. only contributes 14% of the worldwide Internet use. So where is the rest of that Internet use coming from? Let us look at other large national populations such as China. Internet use has not reached as large a penetration into their population yet—only 22%—but that percentage accounts for 20% of the worldwide Internet use, more than the U.S. contribution of 14%.

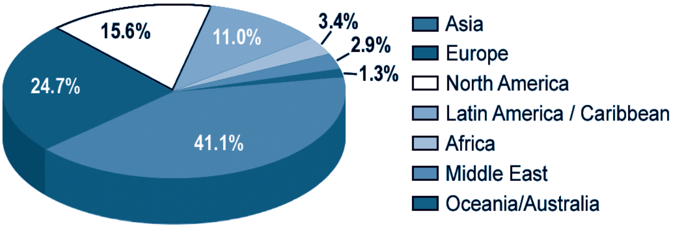
Figure 1 shows the enormous potential for greater access to cyberspace from some of our peer competitor nations. To reinforce what Mr. Dan Wolf said in his address on Cyber Attacks

Mr. Thomas M. McNamara, Jr. is Principal Professional Staff at The Johns Hopkins University Applied Physics Laboratory. Mr. McNamara is the National Security Capabilities Program Area Manager in the National Security Analysis Department, focusing on critical challenges to assess the Department's capabilities for emerging national security challenges and strategically balance and integrate joint defense capabilities. Prior to this position, Mr. McNamara was Head of the Strategic Posture Office. Mr. McNamara received a B.S. in Ocean Engineering from Florida Atlantic University (1976) and a M.S. in Technical Management from The Johns Hopkins University (1995). He has received several Navy acquisition awards, served on a variety of technical panels, and published technical papers.

(Chapter 1), there really are no international borders in cyberspace; therefore, traditional security measures have to change dramatically. What does that reliance on cyberspace look like in the U.S.?



Source: Internet World Stats – www.internetworldstats.com/stats.htm
Penetration Rates are based on a world population of 6,710,029,070 for full year 2008 and 1,581,571,589 estimated Internet users.
Copyright © 2009, Miniwatts Marketing Group



Source: Internet World Stats – www.internetworldstats.com/stats.htm
1,581,571,589 Internet users for 31 December 2008.
Copyright © 2009, Miniwatts Marketing Group

Figure 1 World Internet Penetration and Users by Region

Most U.S. adults find the Internet essential to daily life, according to a 2008 Intel Corporation study, "Internet Reliance in Today's Economy," and most of them also identify it as a key tool in today's economy. Note that the poll was actually an online survey, so it is skewed because it was asking people who spend a lot of time online how important the Internet is to them, but 65% said it was very important, more so than many other aspects of their lives.

VULNERABILITIES

Dan Wolf also talked a lot about our threats and vulnerabilities; he mentioned the Internet crime, denial of service, and insider threat hazards, but there are also accidents. In December 2008, three cables were cut almost simultaneously in the Mediterranean, disrupting traffic between Europe and Asia. It was initially thought a malicious activity was the cause, but it was later determined to be accidental. It affected voice traffic to 14 countries, and business-to-business traffic had to be rerouted through the U.S. The map in Figure 2 shows the convoluted routes those cables generally follow. There was significant recovery time (more than 2 weeks).

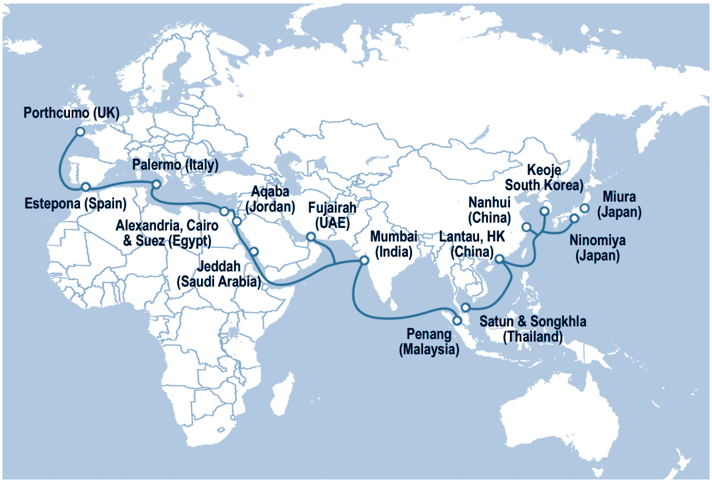


Figure 2 Undersea Cable Routes

According to Carnegie Mellon Computer Emergency Readiness Team (CERT) data, annual CERT vulnerabilities have grown rapidly from fewer than 1000 incidents catalogued in 2000 to 8000 incidents in 2006 (Figure 3). In a more hazardous area—I think Mr. Wolf spoke to this as well when he spoke about the

Visa and MasterCard incident—is protecting data that are commercially stored. Seventy-five percent of companies surveyed by Deloitte Touche in 2006 had already had their data storage security breached from the outside, a dramatic increase from 26% the year before.

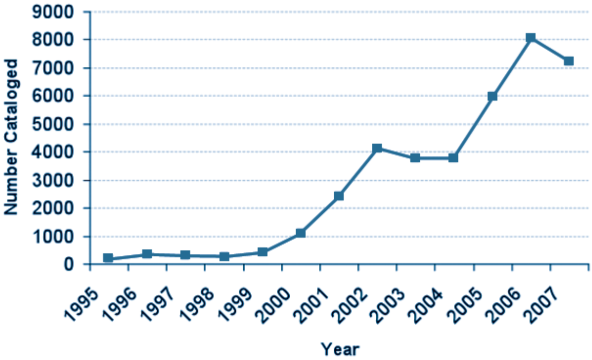


Figure 3 Annual Computer Emergency Response Team Vulnerabilities

There is a lot at risk here. What does that mean to us? What might be the consequences to us as a nation?

It is commonly accepted that productivity has been a major factor in our increasing Gross Domestic Product (GDP), and productivity growth has largely been associated with our gains in information technology access to the Internet. Figure 4 shows the comparative growth of those two factors over time. The use of cyberspace has become a major driver in our productivity as well as our GDP. Much of our reliance on the Internet comes from the business-to-business community. Merchant wholesale trade and manufacturing are the darker bars on the chart in Figure 5. The online retail and banking-type transactions far exceed what many of us might think to be true. However, at the wholesale and manufacturing level, there is far more business transacted using e-commerce and the Internet. Imagine if we were to lose that capability or access for some period of time, either for accidental or malicious reasons.

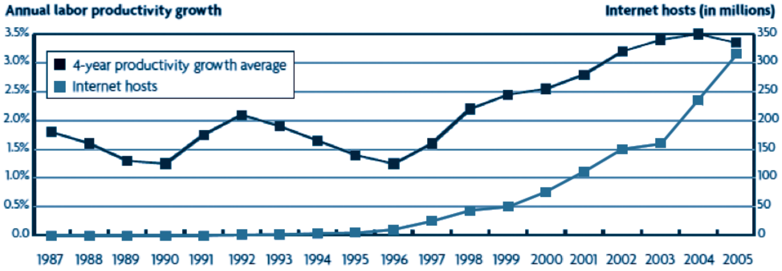
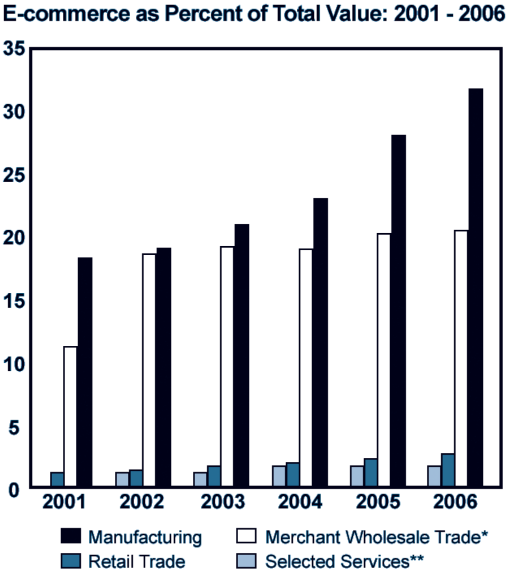


Figure 4 Annual Labor Productivity Growth



*Merchant Wholesale Trade data include MSBOs in 2002–2006, and exclude MSBOs in 2001.

**Selected Services data in 2001 are not comparable due to the 2002 NAICS change.

Figure 5 Business-to-Business Internet-Based E-Commerce

Note the Northeast U.S. blackout that occurred in August 2003, where the estimated losses were about $6–10 billion. Those numbers may seem small when compared with the Government financial bailout discussions we have been hearing in Congress over the past three or four months, but they are still large numbers. Disruption in a small portion of the U.S. amounted to about 0.1% of GDP for just a few days of lost commerce.

STRATEGIC RESILIENCE PLAN

What are our options in dealing with this? I think one option is a strategic plan. Our strategy should not solely look at defending cyberspace but at constructing our cyber resources in ways that are resilient to an attack. Resiliency can be defined as our ability to operate through an event, whether it is accidental or malicious in nature, without incurring a substantial negative impact. Traditionally, we have measured resiliency either by looking at the amount of lost capability that was regained over a fixed period of time or the period of time required to restore a fixed amount of lost capability.

A good cyber resiliency strategy is a combination of architecting and defending our cyberspace. The success of a defensive approach alone depends upon picking the defenses to match the adversary's attack method. If we can pick the right one, good for us, but if an adversary comes at us with something we did not expect, then we have a problem. Also, if they come at us with something stronger than what we expected, it can overwhelm our defenses. Fortunately, it is in our favor that time and attribution expose cyber adversaries to increasing risks. The more defensive measures we can put in place to increase an adversary's exposure—increase the time it takes to get through our cyberspace defenses—that is better for us. Ultimately, though, we cannot assure ourselves that we can defend against every possibility, especially when we look at the increasing complexity of some of the technologies involved in cyberspace.

Therefore, we are moving to a view of resiliency as another option from the strategic choice standpoint, which truly depends upon diversity in the way we design and build-out our cyberspace resources. We are strategically choosing to employ diversity to limit the depth and duration of loss so we purposefully avoid constructing a particular feature across the entire set of cyber systems, which would expose it as a single point of failure and a point of potentially catastrophic loss.

"How do we best implement a comprehensive strategy across the interagency? . . . What should be the role of the government? . . . What are the appropriate roles for academia, nonprofits, as well as profit organizations?"

Among the key design variables that can improve resiliency at little additional cost are geographic diversity, transport routing or path diversities, and diversity in the platform or operating systems of some of our infrastructure (e.g., not everything should be Microsoft Windows based) and use of different supply chain providers. Various transport media—whether it is fiber, satellite communications, or radio frequency—provide technology options for transport infrastructure that was to be implemented anyway but now can be implemented choosing different, diverse technology approaches so that you are not exposed to single point losses. The outcome of cyber losses, when viewed with resiliency in place, depends less on a knowledge of what hazards the adversary will create from the offensive action, or an accident might impose; the results are not as closely coupled to a phenomenon as they would have been without diversity.

THE INTERAGENCY IMPERATIVE

As we move into the panel discussions, we will address questions regarding the interagency imperative. How do we best implement a comprehensive strategy across the interagency? We have had some success in this area. Carnegie Melon, with the CERT program, can track computer attacks over the years (as shown in Figure 3), acting as a knowledge management resource to advise private and public sector activities and identify best practices, weaknesses, and gaps. CERT has worked well for cyber security from a software point of view; perhaps the lessons learned there could be expanded beyond software alone and applied to greater challenges for national cyber security.

In his keynote address, James Locher spoke about a government public-private partnership. A key question is: What should be the role of the government? Because we are discussing interagency issues at this symposium, what is the appropriate involvement, when and where, for the government? What are the appropriate roles for academia, nonprofits, as well as profit organizations?

These are just a few of the challenges ahead of us to consider:

- Knowledge management (capturing lessons learned)
- Sharing best practices (from personal to organizational level)
- Redundancy – how much and for what elements?
- Remediation and restoration – who should be responsible?
- Insurance against loss – how is risk managed?

We should not get hung up on the idea of knowledge management, capturing lessons learned, sharing best practices, and the issue of redundancy. If we depend solely on redundancy, it can be expensive. However, there may be some important, advantageous elements to redundancy. There may be specific areas where it is worth the investment. What should those be? Then there is remediation and restoration. If we have a loss, how do we quickly revive operational capabilities? Who should be responsible for overseeing that? The risk management piece is a big one, particularly because—as Mr. Wolf mentioned—about 85% of our critical infrastructure is privately owned. Attribution and legal remedies in cyberspace are challenging issues that we have not really encountered much, and a lot more work in this area is needed if we are going to improve our opportunities to deal with the cyberspace threat.

This roundtable panel consists of experts well-versed in the issues surrounding the interagency imperative to develop effective, resilient responses to cyber attacks. Mr. Anthony Barger is leading DoD's Global Information Grid Mission Assurance for

Networks and Information Integration in a strategic goal to transform and enable information assurance capabilities for DoD. Mr. Bob Gourley, Founder and Chief Technology Officer (CTO) of Crucial Point, LLC, a technology and research and advisory firm, is the former CTO of the Defense Intelligence Agency (DIA), where he was the senior technologist and engineer responsible for all technology decision making of the global DIA and DoD intelligence information systems enterprise. Mr. Dan Wolf, who addressed cyber attacks as the lead-in to this roundtable (Chapter 1), is President of Cyber Pack Ventures, Inc., specializing in consulting on information assurance, intelligence, and homeland security.

2.2 STRATEGIC AND OPERATIONAL RESPONSES

Robert Gourley

On the topic of responding to the cyber threat and responding to attacks, I wanted to capture some thoughts in two categories: strategic and operational responses to cyber threats. For context, the first real response is deciding how we are going to respond. Are we going to respond? How significant of an issue is this? Is the cyber threat as significant as thermo-nuclear war?

I would argue that in many ways, cyber threats are weapons of mass destruction (WMD). They could wreak havoc upon our nation and our lifestyle if executed in certain ways. In many ways, however, cyber threats do not totally fit the description of WMD. For example, they do not come with the physical destruction of nuclear weapons; nuclear is such a horrible threat. On the other hand, there are many analogies there. We have to decide: What level of threat is it? Is this a more important threat than, say, Iran with nuclear weapons that they can deliver intercontinentally?

Mr. Robert Gourley is the founder and Chief Technology Officer of Crucial Point, LLC, a technology research and advisory firm. He is a former Chief Technology Officer of the Defense Intelligence Agency, where he was the Senior Technologist and Engineer. He was named one of the top 25 most influential Chief Technology Officers in the globe by Infoworld in 2007 and selected for an Armed Forces Communications and Electronics Association award for meritorious service to the intelligence community in 2008. He holds three masters degrees, including an M.S. in Scientific and Technical Intelligence from the Naval Postgraduate School, an M.S. in Military Science from USMC University, and an M.S. in Computer Science from James Madison University.

These are issues the national security community needs to come to grips with and, through that, figure out our response. That is why I wanted to make an analogy to the World War II-type of response. For England in World War II, there was no option; it was victory. It was victory at all cost. Everyone was told, "You will . . . you must deserve victory. If there is going to be victory, you will work for it." For the U.S., when we were sucked into the war, that too was an all-out war. It was going to be won, period. It was a war for national survival, and the war was won.

Figure 1 World War II Poster

Is cyberspace involved in that level of war? Maybe. We need to decide. We need to figure out what response we are going to have, and we can form our response around the questions we ask ourselves on how serious is this threat. I do not think it is a war of national survival yet, but it is definitely a war that requires a strategic response.

Strategic Responses

Four things have already occurred in the strategic response to the cyber threat—the cyber threat of espionage, and the cyber threat of attack. The four key watershed strategic responses I think are the most significant in the response to the threat are:

1. Comprehensive National Cybersecurity Initiative (CNCI)
2. Center for Strategic and International Studies (CSIS)
3. Government Accountability Office (GAO)
4. New Administration

The CNCI, of course, which Mr. Dan Wolf spoke about and captured very well (Chapter 1), has made an improvement in our ability to defend the federal enterprise as well as some improvement in our nation's ability to defend the critical infrastructure. At a minimum, it has enhanced our ability to coordinate across the federal enterprise and therefore our defense. However, many other things have been put into play. We are continuing to see the fruits of that effort. The CNCI has been a positive response.

The next one in the list is the CSIS study that was released in December 2008, the study for the 44th Presidency on the threat to our computers and networks [1]. The CSIS report and follow-on reports were also a strategic response to this threat. Some very smart cyber-security analysts came together and interacted with the government to develop good recommendations. If you have not read the CSIS report, please do. It captures all of the issues very well. A follow-on part of that same CSIS effort is the Consensus Audit Guidelines (CAG). To me, the CAG is more an operational response than a strategic one. The CSIS and related activities are more a strategic response.

"In many ways, cyber threats are weapons of mass destruction."

GAO has a significantly new approach in the strategic dimension. GAO has been interested in reporting, auditing, and investigating the Executive Branch's activities in cyber for over a decade. In 1998, when I was involved in this, GAO people would interview us at the Joint Task Force on Computer Network Defense

(JTF-CND) and write a report that was absolutely worthless and irrelevant. Ten years later, it is totally different. Some of the sharpest thinking is coming out of the GAO. They pull together panels of experts and interview them. They interview and work with the people in the Executive Branch to develop smart conclusions and recommendations. There is an entirely new level of thinking on cyber out of the GAO, and it constitutes a significant part of the strategic response. The GAO informs and testifies to Congress, gives them documentation, and is helping to lead Congress into thinking through what they need to do differently strategically.

Then, there is, of course, the new administration and the many things they have begun. There is information available on the Whitehouse.gov Web page of the major steps that the administration intends to take to cyber. The 60-day CSIS bipartisan Commission on Cybersecurity study led by Melissa Hathaway, the Acting Senior Director for Cyberspace on the National Security, is a very important initiative to expand the CNCI. It is involving more agencies and more people in the federal enterprise and, in a very positive step, involving even more people in the commercial industry, in academia, and other places. Melissa Hathaway and her team have reached out to every standards group and interagency body and asked them for input on this study. It is a great first step.

Tactical Responses

On an operational and tactical level, there are many operational and even more tactical defenses to our networks underway. One is that there is more of a cohesive vision on how we are supposed to protect our networks. We are supposed to deny unauthorized access and enhance and ensure the confidentiality, availability, and integrity of Internet data. More people are coalescing around that.

I mentioned the CAG, which is an implementation guide for how to make your network secure and how to make your computer secure. It flows from that CSIS activity, using the same smart computer scientists and engineers, security professionals, and Chief Information Officers (CIOs) who worked on CSIS. It is a way to improve the security of networks and computers. Standards for security are available in places like the Web pages of National Security Agency (NSA) [2] or other organizations such as the Department of Commerce. The CAG provides a prioritized list of the top 20 controls and standards that you must apply to secure your networks and how to measure them. That is why it is called the Consensus Audit Guidelines. Of the 20 categories, 15 can be automatically measured. It is a computer measurement and rapid visualization of these audit tools. The other five (e.g., Red teaming, training) cannot be automatically measured but still are important to measure responses. The CAG is one of these tactical responses.

Another tactical response is the availability of new leap-ahead technologies that are here today that can help us secure our networks such as the use of cloud computing. I am not saying that all cloud computing is more secure than non-cloud computing, but cloud computing can dramatically enhance security. The smart use of thin clients can dramatically enhance security. The smart use of open source software can also dramatically increase security. All of these put together, in my view, are some of the most significant operational and tactical responses to security.

All of this discussion leads me to one point: we have to deserve victory if we are going to obtain victory. I do not think we can believe that we have won just by saying we are taking strategic and operational steps. This is going to be a long, hard struggle, and we will not have instant victory. It is going to take some time.

"We have to deserve victory if we are going to obtain victory. I do not think we can believe that we have won just by saying we are taking strategic and operational steps. This is going to be a long, hard struggle, and we will not have instant victory."

REFERENCES

1. "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies, 8 December 2008. The report, along with papers and testimony by commission members, is available at http://www.csis.org/cyber.

2. http://www.nsa.gov/applications/search/index.cfm?q=security%20standards.

2.3 CYBER RESILIENCE FOR MISSION ASSURANCE

Anthony Bargar

INTRODUCTION

I work for the Office of the Assistant Secretary of Defense for networks and information integration [OASD(NII)] under the Deputy Assistant Secretary of Defense for Cyber Information and Identity Assurance. I am leading the effort in Cyberspace Resilience for Mission Assurance, which was borne out of our analysis of how we can—and will—operate through and recover from sophisticated cyber attacks. To frame the discussion for this roundtable, I will outline our key approaches to ensuring DoD's mission-essential functions and discuss how cyberspace resiliency depends on more than simply ensuring network security.

KEY INITIATIVES

To conduct a pragmatic analysis of what we need to ensure cyberspace resiliency, we must assume that our best efforts in defense have failed and that sophisticated cyber adversaries—at the governmental level or well-resourced groups, either ad hoc or

Mr. Anthony Bargar is a Senior Strategy and Policy Advisor leading DoD's Cyber Mission Assurance for the Deputy Assistant Secretary of Defense for Cyber Information and Identity Assurance. Previously, he served as Senior Technology Advisor for the Counterintelligence Field Activity, and Senior Information Assurance Analyst for the Defense Intelligence Agency. Mr. Bargar led a research project on shared critical information infrastructure protection and defense with the U.S. National Defense University and the Swedish National Defense College. He holds a master's degree in Information and Telecommunication Systems for Business from Johns Hopkins University. Additionally, he is a distinguished graduate from the NDU Information Resources Management College.

nation-state-based—succeed in degrading, denying, and manipulating our networks, our enterprise services, and the information that travels on them. It is not just about the circuit layer, which is unfortunately often the focus.

We have to make sure the technology underpinnings of our information environment—including our shared power, communications, and information infrastructures—work under fire, deflect attacks, restore trust in information, operate through the event, and recover quickly. The DoD, under the National Continuity Program, has defined certain primary mission-essential functions (Figure 1). Cyberspace resiliency focuses on protecting capabilities that enable those primary mission-essential functions.

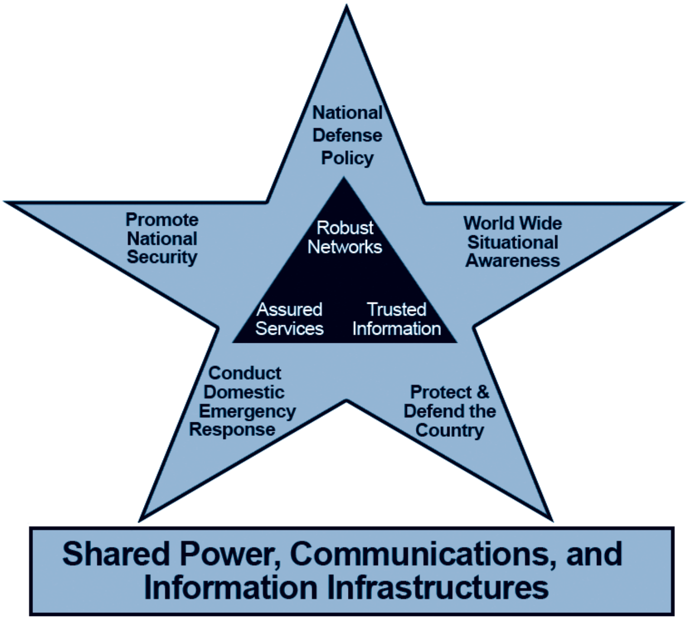

National Defense Policy
Promote National Security
World Wide Situational Awareness
Robust Networks
Assured Services
Trusted Information
Conduct Domestic Emergency Response
Protect & Defend the Country
Shared Power, Communications, and Information Infrastructures

Figure 1 DoD's Primary Mission-Essential Functions

In this effort, we have recommended three key initiatives within the DoD. One is recognition that this is not just a technologist issue; this issue concerns the operator as well as the user.

In DoD, it concerns both the warfighter (J3) and the technologist (J6). That is why it is very important to improve our ability to plan, simulate, and execute exercises under serious cyber degradation. We have to take the gloves off when it comes to planning and training if cyberspace is truly a warfighting domain.

"Cyberspace resilience is much more than networks. . . it is the flexibility, adaptability, and trustworthiness among the human, the physical, and the information domain."

We have to then enable cyber situational awareness, improve diversity planning, integrate policies and plans for resiliency, and take a holistic risk management approach, examining how we measure and manage risk, balancing the technology and operations. The opportunities to achieve this are through improving our models and simulations, understanding complex cascade effects as well as single points of vulnerability, and enhancing defenses against the top-tier adversaries. We must also improve risk management compliance and enforcement while recognizing the shared responsibility with the information, communications, and technology (IC&T) industry. We all share a common critical information infrastructure amongst government, private sector, and international entities. The common defense and approach to resiliency is incredibly important.

MORE THAN NETWORKS

Cyberspace resilience is much more than the creation of diverse networks—resiliency is more than just redundancy. It is the survivability, flexibility, adaptability, and trustworthiness among the human, the physical, and the information domain. It spans our people, processes, and technologies (Figure 2). Cyberspace resilience is the ability to operate through cyber conflict and recover quickly to a trusted environment.

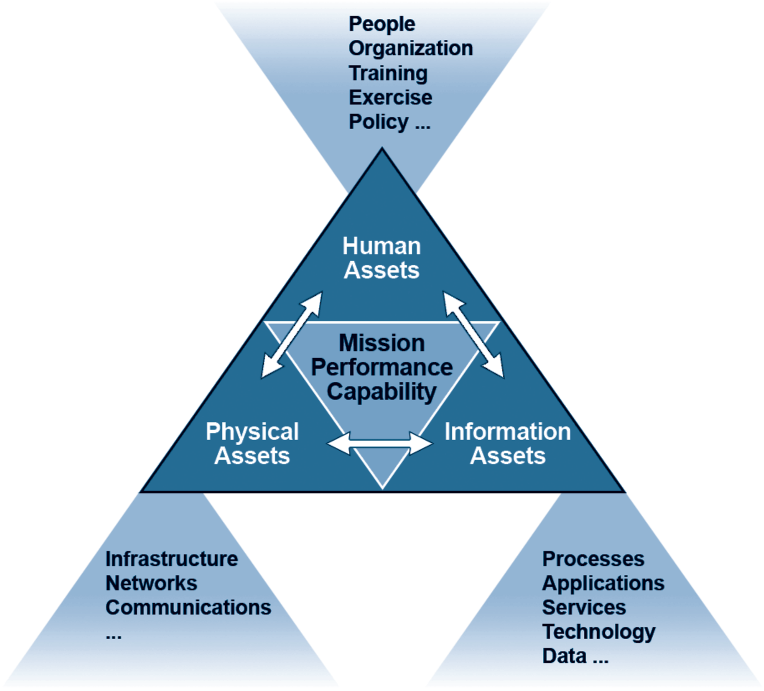


Figure 2 Nexus of Human, Physical, and Information Assets

2.4 QUESTIONS AND ANSWERS HIGHLIGHTS

Transcripts

Q: Mr. Wolf, does the U.S. government have the competent human capital to deal with conceptual and technological challenges that are facing us?

Dan Wolf – That is a good question. I think in the wake of the collapse of the ".com" boom, many of the students who were in computer science and other similar fields have gone elsewhere recently. In terms of a new workforce, I think we have a challenge ahead of us to convince the new students that there is an opportunity in cyber.

Inside the government, I believe there is a lot of "old think." If I go back a few years ago and think about the work that we were doing, we were trying to protect the perimeter. That was a good approach at that time. I think what we learned is that people get through the perimeter. Now, you need to start looking at the entire enterprise and start instrumentation in the entire enterprise. That is a change in thought process. Also, you need to find people who are looking at things differently. In the cyber initiative, a number of activities address leap-ahead technology: new ideas, new thoughts, and new ways of looking at things.

We need to challenge "old think," whether it is the government employees or the contractors, the commercial world or the academic world, and start looking at things differently. In my dealings with a number of companies, I am somewhat surprised at how many are still thinking in terms of perimeter defense. That is not where we really need to be in the present timeframe.

One of the points I made in my presentation was that we needed to react to some of these threats in computer time: under a second. That means there will not be people in the loop. You need to think through those processes in terms of how you are going to react. What is the level of significance of some activity? How do you implement that in an automated way? We have some challenges in terms of the people. Many people out there are doing good work, but I think we need to change some of the thought processes and look at new ideas in terms of how you deal with these problems.

Q: Could you comment on the relationship—relationship being defined as the linkages and causality—between cyber security and technology protection? Are there linkages? Can we trace causes/effects between technology protection—although I am not sure whether that applies to certain supply chain protection and inherent IT protection of that nature—and cyber security?

Anthony Bargar – I think it all starts around how you define cyberspace. Within the DoD, I am asked to define the global information grid. You have to look at it holistically. It is kind of like the force in Star Wars; it is everything that surrounds us. Technology protection, from cause and effects, is quite different yet very related components. You really have to look at the people, processes, and technology.

Robert Gourley – I talked about cyberspace resilience as being a component of cyber security, but I view technology protection as a subset or component of cyberspace security. Maybe the other panelists have a different opinion. I am not sure of the full nuance of that question, but it did make me think of a supply chain type question where, of course, cyber security is extremely important. Consensus Audit Guidelines (CAGs), which I mentioned earlier, are a great way to measure the protection of your information technology. However, CAGs have nothing to do with protection of your supply chain. If your supply chain is not protected, you run the risk of getting hardware into your system that does not behave the way you believe it is supposed to and perhaps hardware or software that have been maliciously tampered with.

This is a complex question that I do not have the right answer to, but I do know that it is a big piece of the comprehensive national cyber initiative. It is also a big piece of the White House study, so it is a known issue. I just have not heard, in my limited exposure, a solution that I think is going to be comprehensive and work well. What does that mean? It means that we will always have to deal with systems that have some threat of having been maliciously tampered with. We have to have a defense-in-depth mechanism that lets us adjust and operate in that environment.

Dan Wolf – Given that you are dealing with supply chain that you do not necessarily control, you might have a system in place that has the sensors that are monitoring what is going on so that, if some anomaly occurs at any given time, it sets off a yellow flag, whether it is software or hardware. We will continue to use equipment that is from sources that are suspicious.

It may be unique in that we have to use it. If you do, then you have to put either a wrapper around it or some sort of sensors into your grid to look at activity. When something unusual happens, that sets off an alarm that somebody then looks at. Again, it goes back to resiliency and operating in a degraded mode. In some ways, you are suspicious of anything that is going on inside your network, and you should to be looking at it holistically.

Q: *There has been a lot of debate over the ability of the Department of Homeland Security (DHS) to effectuate its cyber security duties for the federal government and for private industry coordination. Is there an agency or department that is better suited for the job? What are the possible ramifications, if any?*

Robert Gourley – To me, the right answer comes right out of the GAO reports. Read the GAO report—*National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*—the 10 March issue written by Dr. David Powner, Director of Information Technology for GAO, who spells out the view of many reasoned professionals about the right way ahead for the nation. He does not spell out exactly what has to occur, but he does issue a lot of well-informed, well-reasoned opinions on the ability of DHS to lead. In the opinions of these GAO reports, most definitely DHS has some work to do, but it cannot instantaneously step up to all of its responsibilities. DHS has a role, and there are ways it can address that. Also, the White

House 60-day study, to be issued 29 May, will define what the roles of DHS and the rest of the federal enterprises will be.

Dan Wolf – James Locher talked about creating teams to do things. I am not sure there is any one agency, one organization, that can do this. I believe it has got to be a team effort, many players from many agencies.

Anthony Bargar – Considering teams, one possible construct is for teams that are based around the elements of national power. Now, there are many different constructs to think about (e.g., the midlife approach with military intelligence diplomacy, law enforcement, information, finance, and economics). When I started to think about the different constructs for national power, one thing that is common is information being an enabler for everything. I think it is important for a construct to have that organization that is securing the information or providing that cyberspace security to span all of those organizations or teams.

Q: Can any of the panelists identify an organization today that is operating in accordance with the precepts of resiliency so that organization would be ready to perform its essential functions even after a strong cyber attack?

Anthony Bargar – I have just a quick comment—and perhaps it does not address the cyber attack—but it is a model that I think we need to build our information environment to. When I started this project for mission assurance for DoD, I did a Google search on the term "mission assurance," as anybody would do who is starting to research an issue. One of the items at the top of the list is the National Aeronautics and Space Administration (NASA) Office of Safety and Mission Assurance, which has a very interesting view of mission assurance: it is very much from an engineering perspective. I believe we need to look at our information environment and build it to degrade and understand the failure modes and effects. I do not think we have the answer yet in a complex cyber environment—and as dependent as we are on information—to be able to build our cyber capabilities to be "cyber-survivable" against an advanced, persistent threat. It is a big challenge. Perhaps some lessons can be learned from looking at NASA's engineering approach for mission assurance and applying that to the greater information environment.

Robert Gourley – I have seen a lot of very poor examples that maybe we should not mention, but one superb example is our nation's nuclear command and control capability. We probably do not want to get into too much detail here, but it is resilient and survivable, and it provides a good segue for me to state a second opinion: we need something like that for cyber recovery, something that goes beyond the resiliency that Anthony and others are developing in the Global Information Grid (GIG) to be resilience for the entire enterprise. For example, let's say there is some massive attack on our Supervisory Control and Data Acquisition (SCADA) systems that control our fuel distribution, and at the same time, there is an attack on our power grid and our communications infrastructure, and there is a massive worm staking out a lot of our PCs. How do we reboot all of that? We need to be able to communicate with Microsoft, with Sun Microsystems, with IBM, with all of Silicon Valley, and we need to link them into the cyber response centers (e.g., the Carnegie Mellon Community Emergency Response Team (CERT), the U.S. CERT, and the NSA. How do we do that if we are using the same network that is under attack? That is something we need to think through when it comes to resiliency. Maybe we need a totally different network, a totally different communications path, to all of these organizations.

Q: *In follow-up to that question, is any thought being given to defining what critical infrastructure and systems should be closed computer systems (in other words, non-hackable)? For example, systems is anyone considering systems that are completely off the net or that use technologies that are not cyber controlled?*

Dan Wolf – In the National Infrastructure Protection Plan (NIPP) DHS reissued for 2009, there is direction to each of the sectors reflected in the critical infrastructure to come up with a report addressing vulnerabilities, threats, and recovery [*National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf]. The plan lays out a 10-step process in which DHS is asking the various infrastructures—the critical infrastructures, the elements—to conduct analyses; so, there is a mechanism now by which various sectors can identify elements of their systems that should be more isolated in the future.

Anthony Bargar – There is a significant challenge—you could look at it as an opportunity—to improve in this area of defining what critical infrastructure assets need to be isolated. It is evident in the breakout of the critical infrastructures in the National Infrastructure Protection Plan: cyber assets are pervasive throughout them. Sometimes, each one of those sectors has stovepipe solutions that address understanding what the key cyber aspects are for each specific sector's tasks. We need a holistic approach to examine these cyber aspects uniformly—common lexicons, for example.

Dan Wolf – In the NIPP's Sector-Specific Plans (SSPs), this is the first year where they actually put emphasis on cyber security. They specifically directed each of the sectors to consider cyber security because they had not previously thought about how the information systems go across all of the sectors and how dependent they are.

Anthony Bargar – Another challenge I have faced in the mission assurance effort in DoD is to draw that line between sectors. The phenomenon of net-centricity is pervasive: we use cyber enterprise services for almost everything, but they are multipurpose; we do not have one capability that provides support to one mission. The challenge is to draw that thread throughout the layers from our operational success all the way down to the critical infrastructures they support, and to be able to define the needs for resiliency or the engineering requirements for that thread throughout cyberspace. That is a significant challenge that we need to examine. I will be speaking on a similar effort at the Conference on the Committee for National Security Systems. The National Security Systems construct needs to be examined again, particularly how we work together to secure these systems.

Q: *What are the key cyber warfare/defense/security questions that DoD must grapple with in the next Quadrennial Defense Review*

(QDR)? It starts with mission assurance generally, but are there specifics that you think merit a QDR statement?

Anthony Bargar – I have been pushing hard for resiliency and mission assurance, so I hope that we are able to add it to the QDR. We were successful in getting it into the guidance the Secretary of Defense provides for the development of the Force for 2010 through 2015, and I believe it will drive a big push in the QDR. I do believe a big section is needed on mission assurance or cyber mission assurance. However, the concept of mission assurance does not apply to only the cyber arena; it is really a larger homeland defense issue. We have an organization called Assistant Secretary of Defense for Homeland Defense and America's Security Affairs [ASD(HD&ASA)] run by the Under Secretary of Defense for Policy, for which cyberspace is one component of an overall mission assurance construct.

Robert Gourley – I think that was a great question. I have one that I think OSD needs to tackle in the QDR: How do you pick competent, qualified leaders who can make operational decisions in cyberspace? Right now, the methodology seems to be "Pick a four-star—all four-stars are smart—and put that four-star in charge because all smart four-stars will be able to make the right decision." That is the model we have had for the last 10 years. It is a very good model—it really is—because four-stars are incredibly smart; but does it work for cyber security?

For me, an issue the QDR needs to address is how does the department pick the best, most competent, most qualified leaders, to be decision makers in the cyber realm? I think it is time to reexamine the process and optimize it. What background do we want those four-stars to have so they can make real operational decisions? Maybe their background should include 20 years of operational computer network decisions and intelligence type collection and processing and dissemination and infusion—so that they can really be in charge of cyberspace, instead of just picking someone who maybe was a pilot, maybe a ship driver, maybe a submarine driver and incredibly smart, but maybe with not enough experience in this domain.

Q: Another part of that issue is who is going to follow that four-star's orders? That is a topic the USSTRATCOM Cyberspace Symposium will address in Omaha, Nebraska 7–8 April. Who will be the cyber core of the future? I was at a meeting a few months ago in which someone made the point that the Internet is only 5,000 days old. Check the math; I will just take that at face value. That means we are in the biplane era, if you use aviation as an analogy. Speaking to the CAG point you made, is it time to address enforceable guidelines or standards in the Internet? Keeping in mind that cyberspace is public, private, and international—it is a global issue—is it time to address some sort of infrastructure improvement to address vulnerabilities that have emerged because the Internet is growing organically, haphazardly, in many different ways over time?

Robert Gourley – I think that is another perfect question, so let me start with a metaphor from science fiction: Star Trek, the Movie, the Wrath of Khan (1982). The opening scene begins in the midst of a scenario that came from Gene Rodenberry called the Kobayashi Maru, which was used to test how candidates for Starfleet command react to unwinnable situations. In Star Trek science fiction lore, Captain Kirk was the only one who passed this test in the Starfleet academy; every other candidate for captain failed because it is impossible to solve. Kirk passed. To make a long story short, the way Kirk passed was to hack into the scenario and redesign it.

I think of that when I think of the major problems we have on the Internet today. We can pass. This is a human-designed thing, human engineered, human built. It is not too late to change it. That is a very good point about this being the biplane era of Internet development. We need to redesign it; just as Kirk redesigned the Kobayashi Maru in Star Trek, we need to redesign the Internet. Of course, that is just a metaphor. What is really going on? Two big initiatives at MIT and Stanford are looking at the total redesign of the fabric of the Internet, which will give us more ability to do things like attribution and assured delivery of all traffic and enhanced protection of the data in transit and data in rest. I think both of these efforts at MIT and Stanford are worthy because they are not looking at throwing away all of the old stuff. They are looking at leap-aheads that bring the legacy with it. So, I think we do have to redesign, and there are initiatives underway to do that.

Q: *Here is a set of related questions: Should most cyber attacks against the U.S. critical entities involve an active response (e.g., active defense, legal means)? If not, what would be the consequences to the attacker? Parallel to that, considering the focus on interagency efforts in this symposium and the international scope of the problem, what are we doing with the State Department or others to develop resources by states to respond to cyber attacks? What defines a cyber attack on a nation's security, and how can the responses be made more effective to deter or deny an attack or hold the attackers responsible and accountable? If an attack occurs, what are our options? Who should lead that from an interagency standpoint?*

Anthony Bargar – As the DoD Co-Chair to the National Cyber Response Coordination Group, I will start by stating the official position: We have a process that has existed since 2003, a Concept of Operations (CONOPS) to come together as an interagency body during a cyber event of national significance. This was built under DHS, under the national response framework and there is currently a draft cyber annex to the national response framework that is being developed to flesh all these things out. We currently operate under the draft. Of course, this is all being reexamined with the White House cyber initiative.

We need to come together—in the U.S. government, and from an international and an interagency policy perspective—to examine closely some of the levers that we have as a nation to respond and advise the Secretary of DHS on how to respond to cyber attacks. Considering the first question (should we pursue an active response?), I think attribution is the real long pole in the tent here. Depending on what you mean by active response, we will be judged in the world of public opinion on how we respond.

If active response means blocking ports and dynamically stopping the bleeding, so to speak, I think that is the type of activity we can look forward to now. However, without positive attribution—which requires the changes to the Internet that Mr.

Gourley mentioned—I think we have got a long way to go before we can take further action.

In response to the other question about what the State Department is doing with states to develop resources to respond to cyber attacks, I would offer that the State Department is a big contributor to the national response coordination group that we mentioned before.

Dan Wolf – In my presentation (Cybersecurity: Attacks on the Critical Infrastructure, Chapter 1), I mentioned Project Solarium, which Eisenhower had initiated at a cabinet meeting in 1953. The task was to examine all possible nuclear scenarios and what the reaction should be by the U.S. government. Eisenhower tasked strategic advisers (Vice Admiral Richard Conolly, Air Force Major General James McCormack, and George Kennangave) to assemble teams of specialists from the State Department, the military services, and other national security agencies and gave them six weeks to examine three different strategies.

I think we need to do that kind of thing in terms of cyberspace because in many cases, we cannot wait beyond computer time—meaning, again, that we have only a few seconds to respond. There should be many predefined things that we can do. Having said that, I go back to my chart that shows the progression from the .mil and .gov domains and the critical infrastructure (Figure 1). Clearly, in the .mil domain, because of Titles 10 and 50 of the United States Code, which outline the authorities of the U.S. military, because of the authorities they establish, we can react. When you get beyond that, into the .com and .org domains, then you get into the issue—a significant issue—of attribution. You also get into the issue in terms of what authorities they operate under. If you look at the various Information Sharing and Analysis Centers (ISACs) and how much information they provide to the government about attacks that are going on in, for example, the financial sector or the power sector or the transportation sector, they are not necessarily forthcoming with a lot of details. So, if DoD or the military is going to be the instrument to stop or react to incidences, how do they get that information in a timely fashion?

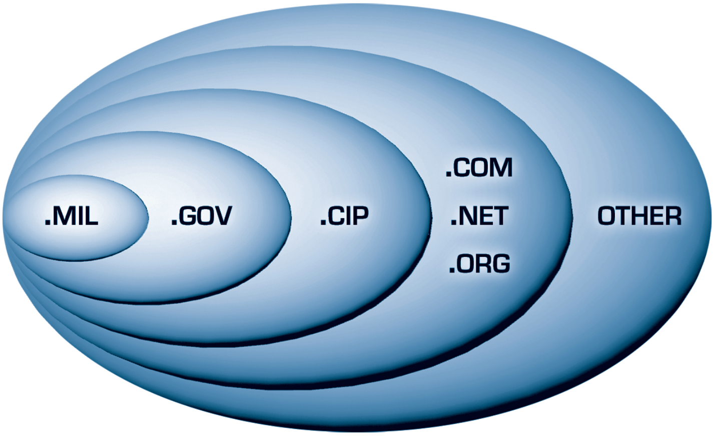


Figure 1 Dimensions in Cyberspace: Authorities, Ownership, Privacy, Liability

I think we have some interesting challenges here. There is also the issue of liability, which I believe I also had mentioned earlier: you can go after the wrong computer or the wrong network if you do not have the correct attribution; it all relies on attribution. The financial sector, the power sector, etc., are passing information to the government, and they are concerned about the government revealing that to others through the Freedom of Information Act (FOIA); if that happens, does that affect their stockholders?

These pose some interesting challenges that go back to the need for legislation and some other measures that need to be in place before we can respond to cyber attacks more effectively. The bottom line is, I think we do have to say that there is a penalty for bad behavior on the Internet.

Thomas McNamara – I think too there is a danger in active responses and their unintended consequences. As in the Estonia case, somebody moved a statue and look what it created. There are several other open-source cases—examples of someone making a statement that is found offensive by people in other nations, and they use the cyberspace to counter-attack. So, when we take an active response to some cyber attack, I think we have to count on collateral damage, unintended consequences and the escalation that it might bring to us in response. We have to be very careful of that.

Dan Wolf – In the Estonia example, there were a million computers that were used as part of the denial of service. You cannot react to those million computers. You really need to go back to who was controlling those computers.

Robert Gourley – This raises one other thought I wanted to mention. The State Department, in my experience, has some exceptionally smart people on these issues of international law and cyber crime and proposed cyber treaties and all these other dimensions, but they are very thin. During the Cold War, if there were questions about what were the U.S. strategies regarding containment, you could go to any ambassador in the Foreign Service and they would be able to articulate that in detail and know what their position and role in that is. I wonder if it is the same in the cyber dimension, or if there is one small cadre at the State Department that is wise on this and then the rest of the Foreign Service Department could use some enhanced learning. If that is the case, maybe it is something that deserves further thought by all of us on how do we help the State Department think through this type issue.

Q: *In 2006, government agencies and departments were mandated to evolve to Internet Protocol Version 6 (IPv6). U.S. industry seemed unprepared to really support the intent of the mandate. Since then, DoD has heard little more on the subject. In your opinion, does IPv6 have an important role in expanding our nation's capabilities and aiding cyber security? Should we be concerned by the progress in Asia in using IPv6 and accepting it?*

Robert Gourley – I think there are real issues there. At the time the mandate to adopt IPv6 was issued in 2006, I was helping run a large federal enterprise. I had this memorandum that said by June 2008, I must be totally IPv6. I had no intention of complying with that memo. Neither did any of my other counterparts in the federal enterprise. It is one of these things about who wrote this direct military order? What was the mission need for me to go to IPv6? I was not running out of IP addresses on the Joint

Worldwide Intelligence Communications System (JWICS), and none of my counterparts were running out of IP addresses. What was the mission value of it?

I understand there could be some benefit in the operational military if you had IPv6 over a battlefield and you can better link sensors directly to sensors, for example. There are some security benefits if you are on an open, unclassified network, but for our closed networks, why do it? So, that is a situation in which we rapidly renegotiated with our bosses, asking what did you really mean? Shouldn't we just be IPv6 capable? If so, let's just buy equipment that can run IPv6. We did not switch over in 2008.

What about for big Internet? I would love to see the power and benefits of IPv6 when it comes to security, attribution, throughput, direct connection, and enhanced collaboration. I would love to see that throughout the Internet, but it is just so hard to make that total switchover, and there are security dimensions we have not thought through (e.g., fire walls and intrusion detection devices). There is not a commercially available firewall that works on IPv6—i.e., commercially available for use in a household or small business. The only thing you can do for a firewall or Intrusion Detection System (IDS) in IPv6 that I know of is buy a high-end piece of industrial grade equipment like CloudShield and program that to do your firewall in IPv6. So, the network is not ready in the U.S. for IPv6. Now, in Asia it is everywhere; they have made that leap, and they are seeing benefits from it. So we do have to deal with that. I just do not see it happening in the near term, not in the U.S.

Dan Wolf – I would question whether or not the U.S. wants to stay in the lead in these various areas of technology and wants to be influencing the standards. At this point, as you said, in Asia IPv6 is widely adopted; they are making inputs into the standards. If we really want to protect cyberspace, I think we need to be there working those issues also.

Q: *What are the pros and cons of using telecommuting, both in government and commercial industry, as a tactic for increasing resiliency?*

Robert Gourley – I will expand that a bit—maybe not to directly address it—but talk a bit about telepresence technology, which provides collaborative meeting capability. The most famous provider of telepresence is Cisco, although there are others that do that (e.g.,Tandberg, Polycom). The technology provides not just video collaboration or video teleconferencing (VTC), but really is an experience like being there: telepresence. That is a way to rapidly enhance our communication and coordination. I think there is a role for more of that in the cyber response to link together all of our cyber response centers in a way that is not just a telephone and not just some clunky old VTC, but real telepresence—that will allow us to assess and work these major cyber issues. I think there is a role for that.

Anthony Bargar – I believe in the principles of telecommuting because it addresses the other elements of the human domain that I spoke of being resilient, but I would also offer that a component of the telecommuting challenge or an approach to it would be the concept of virtualization. Virtualization allows you to be anywhere anytime. Although there are some security challenges with how to do that, I believe it will make us more resilient if we approach it with that concept.

Dan Wolf – I am a strong supporter of telecommuting and all the other things that you mentioned. I think it is a way of tapping into resources, human resources, that may not be available say in this particular area. As we talked earlier, I think the people who have expertise in this area are not plentiful. Yet, in other areas of the country, the people have some of the talent. Telecommuting is a great advantage. We should do more of it.

Q: *How vulnerable is the world to this type of threat, specifically in terms of manual monitoring and controlling the state of remote equipment? In other words, how prominent are these vulnerabilities outside of Europe and North America? We saw some data earlier about the amount of penetration the Internet has in the U.S. Obviously, there are less developed countries in the world that perhaps do not have the exposure we have, are as technologically advanced. Although, Estonia is certainly a case that has shown otherwise.*

Anthony Bargar – I would offer that even if a country is not as technologically advanced, it still depends on products and services and the global economy that drives the shipment of goods. I think that there is a complexity to this level of reliance on the common critical infrastructure, information infrastructure, that we have not addressed. Perhaps those cascade effects are not just technology cascade effects that will just address technology or technological nations, but also spill over to others as well.

Q: *That was actually my question. I am asking it for a specific reason. I am doing a Red Team project on an exercise looking at Africa 10 years in the future. One focus is on weapons of mass destruction (WMD), another on nuclear, but I think the red team needs to consider infrastructure issues such as water control and electricity. However, I have not figured out how vulnerable these types of infrastructures are in other parts of the world.*

Anthony Bargar – In places such as Europe, you can make a case study of the gas distribution system. In the U.S., sometimes we just do not think about getting our critical infrastructures and critical energy sources from other nations. I think it would be informative to look at not only the political instability from what is happening with the Ukraine and Russia and the rest of Europe, but also look at the technology challenges to that.

Q: *I am focusing on areas outside the U.S. and Europe, at places like Africa and parts of Asia. You mentioned that China has 22 percent of the population that is engaged in the Internet. Do we know how dependent critical infrastructures are on computer technology?*

Thomas McNamara – I have seen data recently that the market in Africa for the Internet is increasingly rapidly, and there are many political ramifications to that. Of course, companies, the private sector that wants to invest particularly in wireless is where a lot of the growth is happening. If you look at the demographics of cell phone use, it is growing leaps and bounds in Africa. Private industry is trying to provide more third-generation wireless access, but they are concerned about political stability of the regimes and whether or not they make an investment in a country that in five years might be nationalized or have losses due to terrorist risks, etc.

I think the access to the Internet is going to be compelling for those people who do not have news or do not have access and they want it today. The danger that poses is: Does that open up new avenues for us from the cyber security standpoint, new avenues, new populations, that could express their dissatisfaction with the U.S. through that medium.

Robert Gourley – An unclassified resource you can look at is called telegeography.com, which provides good background situational awareness on the telecommunications infrastructure of the entire globe. To get to the real essence of this kind of information, if you really want to dive into it, I think you need to find some classified sources, either at NSA or the Defense Intelligence Agency (DIA) and start asking some hard questions there.

Dan Wolf – I would say that there are probably half a dozen countries in the world that are not quite equivalent to the U.S., but are as dependent upon cyber security for their critical infrastructures; and there are probably another dozen with particular segments—passport control, for example—where they may be very dependent upon networking. Then there are probably 18 to 24 countries in which very small pieces of their infrastructure are computerized. I recommend that you to talk to NSA about some of the classified studies it has conducted.

The other point I would make is about the definition of cyberspace. I have a very broad definition of cyberspace; it is not just Transmission Control Protocol - Internet Protocol (TCP/IP). I realize that it is a very broad definition that might be a catchall, but I would include things like the telephone system, the Common Channel Signaling System No. 7 (SS7) linkset. Some countries, for example, use SS7 to pass various kinds of information, so you should look at that also.

Q: *How does the panel believe that virtual worlds, such as Second Life, relate to cyber security and unrestricted warfare issues? At a recent conference, one of the presenters talked about using Second Life* *as a means to avoid international record keeping of international funds transfers, and that they could make a transaction in Second Life in the U.S. with dollars, and somebody on the other side of that transaction would be in Denmark or Germany, and that transaction never had any traceability through the international financial records of transferring. They were talking about Second Life as being an environment that would foster international crime, money-laundering types of activities.*

Anthony Bargar – I just know that the Second Life environment is a big challenge for looking at counterintelligence issues, and insider trading, and other people's behavior in cyberspace. How does that affect uncovering that type of activity? It is a mask, an easy mask. If we could create an environment and just put all the world's problems in Second Life and just keep the real life pretty normal, that would be a good goal.

Q: *What is being done to ensure manual overrides to SCADA within the U.S., which parallels an earlier question about defining critical infrastructure in a way that we have closed computer systems that do not allow the access as a protection means.*

Dan Wolf – In the last few years, the national labs have done a lot with the SCADA system. I mentioned Sandia at my presentation; Sandia has a center for SCADA security and has done a lot of analysis on various SCADA systems and made recommendations in terms of how to improve the security, the reliability, etc. and those are being implemented. Returning to the Sector-Specific Plans in the NIPP, you can see some of that starting to creep into SSPs in terms of upgrading and improving the security of SCADA systems.

In addition to Sandia, a number of academic institutions are doing research in SCADA. Some of those go along with the NSA, DoD, and DHS information assurance centers of academic excellence. Some universities are putting research effort into SCADA security, so there are some good things that are happening now. If I go back four or five years ago, I do not think there was as much attention being paid to SCADA. Because of some of the incidents that have happened—and I only cited a couple of them—much more attention is being paid to SCADA security. So there is progress being made there.

Q: *Regarding the response side, how do we respond to this? What are we going to do to the culprits when we catch them? We often hear about how a serious attack, especially on SCADA type systems, could put us in the Dark Ages for weeks or months. Are we this vulnerable to resetting our systems and getting us back on our feet? Is there a defined policy that the U.S. would take for retaliation? With the improvement I think over the past few years, are we still looking at nightmare scenarios with SCADA systems? Or will the improvements likely make us more resilient so that our down time and severity of loss would be shorter?*

Robert Gourley – I would argue against the thesis that we are better, more resilient, today than we were five years ago, because there has been a rapid proliferation of SCADA, and not everybody is aware of the threat. In fact, I have seen evidence that our electronic regulatory bodies, the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC), are addressing it by putting on blinders and pretending there is no problem. It is not quite that bad, but they are not as aware and aggressive at fixing these problems as I think they should be. So, I think this is still a very valid concern: there is a threat to our systems. The good news is that the major players that could commit cyber war against us have reasons not to do that. So there is reason for hope. There is some way of deterring. I do not think our national security and national survival should be based on simple hope. We do need to protect our systems, but those actors that could conduct massive cyber war against us are deterred somewhat.

Anthony Bargar – I share the same opinion as Mr. Gourley. In fact, as time goes on, we are more and more dependent on technology and more comfortable in our technology issues so to speak. Yet, our approach to resilience is not keeping step. I would also offer that it is true that all of our nations, the nations of the world, are dependent upon each other's economies to succeed. We all share this information infrastructure, which our economies and financial systems depend on. The wild card really is that terrorist actor, the transnational, or even the criminal who is after it for financial gain or for its terror value. So I think that is a very big concern. I subscribe to the "look at the doomsday scenario" approach.

Dan Wolf – I was not trying to say that things are perfect at all. A lot of work still needs to be done. I think there needs to be a lot more effort in terms of informing and educating people and organizations on what the threat really is—because again, I think some people do not understand how serious this is. The example I had about the nuclear power plant, the fact that they had a connection in terms of the open Internet, I would hope that has been corrected. Not only do you need to do better in terms of educating the private sector, but I believe the government also needs to hold their feet to the fire. It goes back to that issue of 85 percent of the infrastructure being in the hands of the private sector. What do we do in terms of holding their feet to the fire? How do we enforce or require or penalize or whatever if they do not implement proper security procedures that you know will fix some of the problems? In some cases, that might be creating a closed network or maybe putting in new hardware or software or educating or training.

Q: *Two questions combined: The discussion we have had has primarily been focused on defense and assurance. Are offensive capabilities and preventive operations applicable concepts when examining this issue? In thinking more specifically about an application for an offensive concept, is working with organizations such as the National Counterterrorism Center (NCTC) or counterterrorism community to combat terrorists by preempting their use of the Internet—or preempting their use of particular sites to spread hate doctrine against the U.S.—would those options be worthwhile in the strategy to deal with cyber security?*

Anthony Bargar – I would just like to say that I focus on resiliency in the defensive side. So that is really all I can comment on in this forum.

Dan Wolf – Actually, I will make a comment on that question. I think what is needed is a measured response. I remember some of the early documents at DoD that talked about active defense, things like shutting down ports, for example, or turning off services. But then you have to start talking about how far you can go out in the Net before that is something more than just active defense. I think you have got to have a measured response. Then, attribution is certainly an issue, because you really do need to make sure you know who is doing what you think they are doing, who is conducting the attack.

Chapter 3

Roundtable 2

Responding to Resource Attacks

3.1 MODERATOR'S SUMMARY

Lesa McComas

Access to resources, including agricultural, land, minerals, timber, and energy sources, has driven conflicts since earliest recorded history for unfettered access to resources is the lifeblood of national wealth and power. This suggests that aggression to obtain and defend those resources, or to deny them to an adversary, is a biologically adaptive behavior. Some historians argue that such competition is at the root of all human conflict.

Throughout history, the interdiction of enemy supplies through blockade, capture, or destruction has been an effective strategy in warfare. America's own continental Navy was formed to intercept the movement of British arms and supplies as well as to reduce British profits from commercial trade. German U-boats conducted highly effective, unrestricted submarine warfare campaigns to interdict Allied supply lines in World Wars I and II, and the Allies'

Ms. Lesa McComas is the Supervisor of the Asymmetric Warfare Analysis section within the National Security Analysis Department at JHU/APL. She supports several DoD clients in efforts including scenario and CONOPS development as well as technology assessments. Prior to joining The Johns Hopkins University Applied Physics Laboratory, she served as a Navy Surface Warfare Officer and later worked as a Technical Trainer and Training Manager at Concurrent Technologies Corporation and as a Project Manager at Aberdeen Proving Ground for Computer Sciences Corporation. Ms. McComas has a B.A. in Biology from Franklin & Marshall College and an M.S. in Operations Research from the Naval Postgraduate School with an emphasis in Human Factors Engineering. In 1998, she co-authored Naval Officer's Guide (11th ed.), published by Naval Institute Press, and is currently at work on the 12th edition.

extensive bombing of German oil facilities was arguably the most significant factor causing the collapse of Nazi Germany.

The very notion of "enemy" has become increasingly blurred as globalization has spurred the expansion of a complex, interconnected web of economic and diplomatic adversaries, rivals, and shifting alliances. The preemptive nature of unrestricted warfare potentially redraws the once bright line between denying an enemy the means to make war on you and denying a potential adversary the means to compete with you.

> *"Warfare must always include attack on resources as well as attack on life. If the enemy can be cut off from his supplies he must yield."*
>
> *— Rear Admiral William L. Rodgers USN, The American Journal of International Law, October 1929*

Further, this increased interconnectedness, coupled with recent technological advances, has provided terrorists, pirates, and even corporations with the means of motivation to enter the field of combat and inflict the kind of punishment that was once the sole province of states with military capacity. Such nonstate actors have fewer assets of their own to protect against retaliation and fewer qualms about inflicting civilian hardships and casualties.

Although there is considerable international maneuvering among the world's nations, including the U.S., China, and Russia, to ensure access to their own future energy needs, such actions currently remain largely in the competition category. China cannot afford to clash directly with the West over energy. Russia's leadership recently acknowledged mistakes in that country's dealings with other nations on energy issues, possibly signaling recognition that in anything short of a hot war scenario, such tactics can result in unintended and undesirable consequences.

That said, the nature of global energy competition is projected to become increasingly intense over the coming years. China is currently the number two consumer of oil behind the U.S. and, before the recent economic downturn, was poised to overtake the U.S. in 2010. Russia has been seeking means to expand its own oil and gas reserves in the Arctic by laying claim to vastly larger territory than is currently recognized under international law—a claim that includes an estimated 13 percent of the world's remaining undiscovered oil and 30 percent of its undiscovered natural gas.

Although competition is clearly not the same thing as conflict, the likely increased intensity of this competition will help to create an environment in which states' hunger for energy places them in an adversarial posture. Although, "No Blood for Oil" presents an appealing antiwar sentiment, the economic devastation to the U.S. that would be caused by an interruption of our access to foreign oil is undeniable. The Carter Doctrine, proclaimed in the 1980 State of the Union Address, warned the Soviet Union against attempts to limit the free movement of Middle East oil.

However, state actors are no longer the only, or even the largest, threat to such access. As previously mentioned and as previous attacks have shown, kinetic attacks on resources are no longer the purview of state actors alone. Terrorists and pirates are capable of inflicting significant damage to further their own ideological ends, influence markets and nations, and finance their operations. Osama bin Laden has called upon terrorists to strike supply routes and oil lines and to assassinate company owners who provide the enemy with supplies.

Resources can also be attacked by subtler, nonkinetic means. The role corporations can play in these attacks was highlighted this winter by Gazprom's role in cutting off natural gas supplies to much of Eastern Europe. In the U.S., Enron and other corporations ruthlessly manipulated electricity markets, resulting in widespread blackouts in California in 2000 and 2001.

The U.S. is fortunate in that we are self-sustaining in many resources, including agricultural products. However, by one estimate, the U.S. now relies on imports for more than 50 percent of at least 45 key mineral commodities, double the number from 1996. Also, we remain critically dependent on foreign sources of energy. According to the U.S. Department of Energy, the strategic oil reserve now stands at a 62-day supply, down from a peak of 118 days in 1985.

Dependence on long pipelines and complex distribution infrastructures makes modern industrialized nations remarkably vulnerable to interruptions of supply. U.S. domestic manufacturing is increasingly reliant on resources such as oil and minerals that can only be obtained in the quantities required from foreign sources, necessitating an elaborate transportation network as well as diplomatic obligations or foreign entanglements—with all the baggage that phrase implies—to help ensure uninterrupted access to those resources.

Susceptibility to resource attacks is not confined to those resources that need to be imported from foreign sources. Public health experts believe that contamination of food and water supplies would be the easiest method for terrorists to distribute biological or chemical warfare agents. A 2003 Rand study suggested that factors including concentrated and intensive farming practices and insufficient security and surveillance make the U.S. food supply especially vulnerable to attack.

The nation's electrical grid is also at risk, judging from the results of recent natural disasters and our own systemic failures. In August 2003, the largest blackout in North American history left large swaths of the U.S. without power for four days. In addition to destruction of oil and natural gas production wells and import facilities brought by hurricane Katrina, damage to the regional electricity generation and distribution infrastructure had a far-reaching impact and forced the local electrical utility into bankruptcy.

The concept of unrestricted warfare with its emphasis on non-military means of attacking one's adversaries provides a possible framework for understanding the broad range of resource targets susceptible to attack and the conditions under which such attacks might be possible. In this roundtable, our panelists will explore the potential adversaries, tactics, vulnerabilities, and defensive actions associated with resource attacks.

Jan van Tol is a Senior Fellow at the Center for Strategic and Budgetary Assessments. Prior to his retirement from the Navy in 2007, Captain van Tol served as Special Adviser in the Office of the Vice President. At sea, he commanded three warships, the last of which, USS *Essex*, was a major participant in post-tsunami relief efforts in Sumatra, Indonesia. Captain van Tol's analytic work has focused mainly on long-range strategic planning, military innovation, and war gaming.

Celina Realuyo, President of CBR Global Advisers, an international strategic consulting firm, is also Assistant Professor of Counterterrorism at the National Defense University where she teaches national security policy and counterterrorism policy. She has served as the Director of Counterterrorism and Finance programs for the State Department and has managed a foreign assistance program aimed at safeguarding financial systems against terrorist financing.

3.2 RESPONDING TO RESOURCE ATTACKS: PROTECTING CRITICAL INFRASTRUCTURE

Celina Realuyo

INTRODUCTION

Just a moment ago, I saw some people when they were out in the foyer, probably checking on the status of their 401Ks, comparing today's results to the euphoria of yesterday's stock market gains. When we think about a tax on national resources and critical infrastructure, it is amazing that over the past 20 years, the U.S. has become so vulnerable to what happens in very remote parts of the world.

GLOBAL RISKS

First of all, if we look at the negative impacts of globalization in our world, we are almost victims. Let us take a look first at the core global risks that we are dealing with in 2009 (courtesy of the 2009 World Economic Forum Global Risk Network Report):

Ms. Celina Realuyo is President of CBR Global Advisors and has almost two decades of extensive expertise in national security affairs, enterprise and geopolitical risk management, international banking, counterterrorism, etc. As Assistant Professor of Counterterrorism at the National Defense University, she educates U.S. and foreign military and civilian leaders on national security and counterterrorism strategies. In Washington, Ms. Realuyo served in the State Department Operations Center and as Special Assistant to the Secretary of State. Ms. Realuyo holds an M.B.A. from Harvard University, a M.A. in International Relations from Johns Hopkins University School of Advanced International Studies, and a B.S. in Foreign Service from Georgetown University.

- **Economic:** asset price collapse, food price volatility, oil shock, U.S. $ collapse/economic crisis, Chinese hard landing, fiscal crises, retrenchment from globalization
- **Geopolitical:** terrorism, war, collapse of NPT, transnational crime, corruption, global governance gap
- **Environmental:** natural disasters, climate change, loss of fresh water, air pollution, biodiversity loss
- **Societal:** pandemics, infectious and chronic diseases, demographics, migration
- **Technology:** critical information infrastructure, web, global communications breakdown, data fraud/loss

Every January in Davos, Switzerland, the great leaders in business, academia, and the world at large, those most in favor of globalization, meet for what has been touted as the summit of the rich and famous. We must admit that over the past 25 years, we have been the beneficiaries of globalization. However, with all of those benefits have come tremendous risks. It is pretty interesting to see this is the first year that the world economic forum has actually placed economic risks in front of geopolitical ones, which is a very significant change compared to prior years, especially considering the national security audience attending this symposium.

What is also a little bit ironic is that the Head of AIG's risk units has always chaired the group of international chief risk officers that meet at Davos. I have to give him credit for being right in predicting that retrenchment from globalization was going to be a top issue and a top threat. Unfortunately, it has actually transpired and come upon us. It is interesting to see the categories and organizational structure that these experts use to address several of the questions concerning the different spaces in which we could be attacked and whether they will be through biological pandemics or through information technology.

It is quite fitting to take a look at the global context that we live in and more importantly the risks that our war fighters and national security leaders are really grappling with: situations very different from what we have been dealing with over the past 50 years in the post-Cold War environment.

"We must admit that over the past 25 years, we have been the beneficiaries of globalization. However, with all of those benefits have come tremendous risks."

PROTECTING OUR CRITICAL INFRASTRUCTURES

Because the U.S. is the driver of the world economy and integrated in so many fashions, both in the private sector as well as in government and our research and development, we have seen that a lot of these key sectors, and more importantly our key resources, are overly reliant on external sources. Professor Klare elucidated the fact that we are so dependent on supply chains that we need to start rethinking how to protect our critical infrastructure, particularly at a time of extreme economic duress. Examples of these vulnerable, and attractive, supply chain targets are:

- Food and water
- Energy (oil, gas, coal, nuclear, and electricity)
- Manufacturing chemicals and pharmaceuticals
- Transportation and shipping (air, land, rail, and sea)
- Information technology and the worldwide web
- Financial and communications systems

Eighty five percent of our critical infrastructure is in the hands of private sector players. As private sector players try to meet the demands of their shareholders, and more importantly their consumers, to be able to stay in operations, safety and security thinking about how to protect supply chains becomes focused on cost cutting. Consequently, they become the victims.

I teach a course called "Terrorism and Crime" as well as another on globalization. It is truly an honor to be on a panel with Professor Klare, whose materials I use for my students. We look a lot at the vulnerabilities of supply chains and more importantly why these types of vectors are quite attractive for criminal and terrorist groups. Unfortunately, over the past couple of years, we have seen an unholy alliance between the two types of non-state actors, and we cannot even really be aware of who or where the attack is coming from.

Attacks on critical infrastructure or supply chains can be divided into two different categories. First, there are inadvertent attacks. These attacks focus on hazards, whether it is a natural disaster, an accident, human negligence, or an IT or electrical outage. In many emerging markets, they still suffer frequent brown outs due to unreliable energy sources, which could actually even happen here in the U.S. if we do not try to focus on the projects of creating a smart grid for the future.

More importantly, I focus a lot of time in my course looking at deliberate attacks. The bigger question as to how other rivals, whether China or Russia, may view and use these seams or gaps in our security to harm us. Also, you see many other organizations, whether they are criminal or terrorist groups, taking advantage of these perceived vulnerabilities, whether it is in supply chains or different types of critical infrastructure.

Most of us are in the business of practicing and preparing for crisis or response management, so we all think in terms of the following five emergency response phases:

1. **Extreme Event**: Catastrophic/extreme event occurs (e.g., terrorist attack or hurricane).

2. **Respond Immediately**: First response to event by emergency services.

3. **Rescue/Recover**: Rescue personnel; search for, secure, and recover assets.

4. **Restore/Rebuild**: Restore services/rebuild installations affected by extreme event.

5. **Redundancy/Resilience**: Establish redundancies in staff, operations, information technology, and data to mitigate future risks.

If you really think about how you can never be 100 percent sure that you have protected your critical infrastructure or key resource, you cannot just focus on the prevention part but more importantly the response and the resilience part. I predict my colleague from the Council on Foreign Relations, Steve Flynn, will be speaking a lot about resilience.

It is quite interesting to see how different sectors of our economy and our society look at and understand these issues at an academic or theoretical level. You would be surprised how many Fortune 500 companies have not really thought through the response resiliency and how to respond after a cyber attack or even a fire in their facility.

When I think of natural resources, I think about our people as a vital natural resource. A country's greatest contribution to society is its people. People bring critical skills and play critical roles in maintaining the operation of our national security infrastructure and economic activities as well as fulfilling our basic needs. It is this combination of skills, roles, and people that form our human capital (Figure 1).

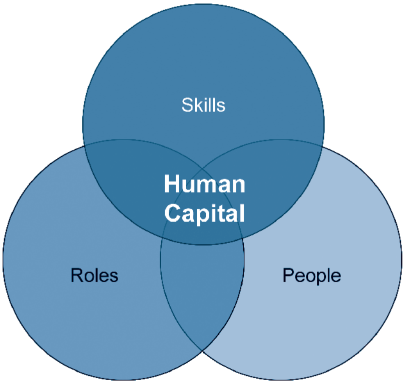


Figure 1 Human Capital

It is really the basics that sustain our human capital. I have had the privilege of traveling to about 70 countries around the world. It has always been amazing to me, whenever I come back to the U.S., how we can truly rely on having four basic needs: food, water, shelter, and security. There is never an instance that we go to the bathroom and turn on the tap, unless you had a contractor who did not really do the job right, that you do not expect clean water. Many places in the world have people living on less than $1 a day, and they have to walk for miles to gain access to food and water. More importantly, because we actually live with the luxury of these basic needs, we do not think as much about the resilience or response to potential deprivation.

As I mentioned, we are really beneficiaries of globalization. I challenge any of you to go to Wal-Mart or Target—you choose which one—pick up 10 items, and try to find at least three that are only made in the U.S. It is quite difficult because we have been able to access a wider variety of cheaper products. We have also been subjected to a lot of questions on how our supply chain has been infiltrated and about the types of dangerous products that are coming into our system.

It is a significant paradox that we have one of the most developed and productive agricultural industries in the world from which many of our other trading partners import and copy our best practices yet we still have a vulnerable food supply system.

INTERAGENCY PERSPECTIVE

In terms of the interagency, there are agencies that are responsible for our safety: the Food and Drug Administration (FDA), the Center for Disease Analysis, and more importantly Health and Human Services. We focus quite a bit on the interagency, particularly regarding national security. We all know a lot of how I would call the military side of the house is structured but not so much on human services or the health side.

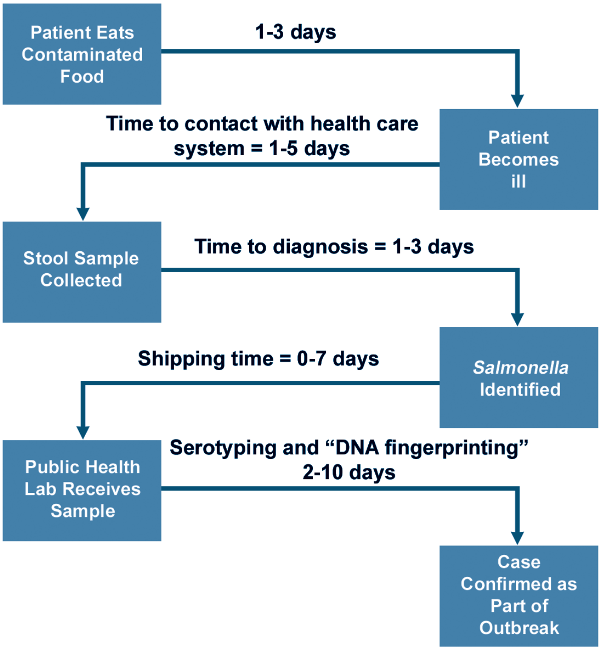
It is really quite interesting how much time, energy, money, and resources we spend and devote to the issue of maritime security. Curiously, we have not devoted the same time to translate the best practices that we should apply for other types of supply chain management such as the issue of food safety in the U.S.

I am sure many of you are familiar with the fact that last year there was a red tomatoes scare. It actually was an accident. There was a huge response by large suppliers and sellers of raw tomatoes, including huge chains (i.e., McDonald's, Wal-Mart, and Young Brands, which owns Burger King and Pizza Hut). They decided that it was more important to protect their consumers than to risk putting raw tomatoes into the food chain.

This scare had a huge impact on tomato growers. We also saw huge questions and gaps in the system that was supposed to protect us from salmonella contamination. Figure 2 shows the timeline for reporting cases of food contamination. After a couple of months of backtracking through the FDA as well as their interagency partners, they discovered the problem was not red tomatoes but jalapeno peppers from Mexico. By the end of the summer, there were visibly detrimental effects on those in the agricultural industry of the tomato growers. As you all know, there are certain seasons that particular plants and crops flourish, and this entire industry had been mistakenly identified as the cause of the contamination as opposed to the jalapeno peppers.

In assessing this example, there is a lot of room for improvement in terms of our food safety preparedness and reaction. There is an FDA food protection plan that has very basic core elements considering the prevention of, intervention during, and response to a food crisis. Recently, because of reports on the salmonella outbreak last year, that there is an increased call for more human resources and staffing at agencies such as the FDA and a greater awareness at the federal, state, and local level of how to take contamination and other food safety issues much more seriously.

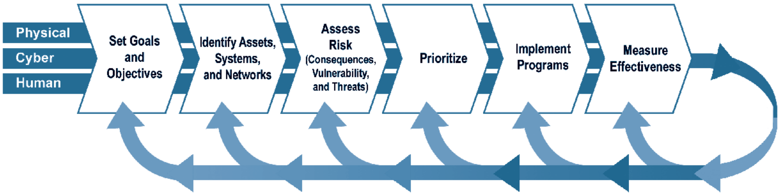
This is, obviously, an inadvertent attack on the food system. Imagine, though, if we actually had a non-state actor think about the vulnerabilities in our food and supply chain and want to do us harm on a large scale, thinking of Lisa McComas' introductory remarks.


Patient Eats Contaminated Food
1-3 days
Patient Becomes ill
Time to contact with health care system = 1-5 days
Stool Sample Collected
Time to diagnosis = 1-3 days
Salmonella Identified
Shipping time = 0-7 days
Public Health Lab Receives Sample
Serotyping and "DNA fingerprinting" 2-10 days
Case Confirmed as Part of Outbreak

Source: U.S. Centers for Disease Control and Prevention

Figure 2 Timeline for Reporting Cases

The question then becomes: why should not or would not we want to translate all of these games and best practices that we use in the military mindset to other areas of critical infrastructure protection? The Department of Homeland Security (DHS) has been in charge of coordinating the upgrade and redesign of the National Infrastructure Protection Plan (NIPP), shown in Figure 3. Because it addresses so many different sectors and industries and overall interagency effectiveness, there has to be a way that to look at this risk-based analysis and find ways to truly protect and maintain the integrity of our supply chains and critical infrastructure, not only within the scope of a weapon of mass destruction infiltrating the port of Norfolk.


Physical
Cyber
Human
Set Goals and Objectives
Identify Assets, Systems, and Networks
Assess Risk (Consequences, Vulnerability, and Threats)
Prioritize
Implement Programs
Measure Effectiveness

Source: U.S. Department of Homeland Security

Figure 3 National Infrastructure Protection Plan

The DHS has evolved and now better understands its mandate and limitations in taking a sector-by-sector approach. Their core priorities are to:

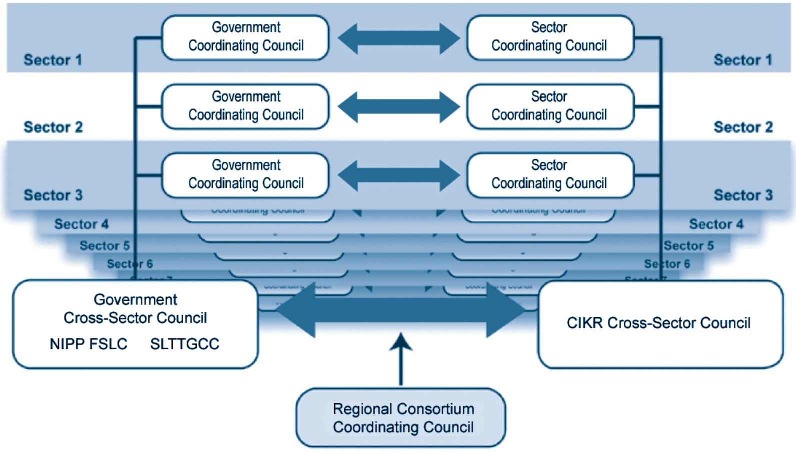
- Protect our nation from dangerous people and goods.
- Protect critical infrastructure.
- Build a nimble, effective emergency management system as well as a culture of preparedness.
- Strengthen and unify DHS operations and management.

"It is a significant paradox that we have one of the most developed and productive agricultural industries in the world from which many of our other trading partners import and copy our best practices yet we still have a vulnerable food supply system."

The NIPP's sector partnership model (Figure 4) depicts how we can draw from a lot of expertise within industries to learn what can and cannot be done to put new regulations and new safety measures in place without impeding the viability and profitability of the private sector, which as I mentioned owns 85 percent of the critical infrastructure.

To conclude with some food for thought, we should consider overselves all as guardians of our homeland safety and its people. We have to bring together government, academic, and private sector minds to protect our homeland in an inter-disciplinary and inter-sector collaboration to foster the full capabilities of the interagency.

This is a question and the dare that I pose to my colleagues at the FDA: instead of trying to reinvent the wheel, why cannot we simply draw on great examples and proven best practices in securing supply chains in different industries to protect our people from food contamination, accidental or otherwise.


Sector 1
Government Coordinating Council
Sector Coordinating Council
Sector 1
Sector 2
Government Coordinating Council
Sector Coordinating Council
Sector 2
Sector 3
Government Coordinating Council
Sector Coordinating Council
Sector 3
Sector 4
Sector 4
Sector 5
Sector 5
Sector 6
Sector 6
Government Cross-Sector Council
NIPP FSLC
SLTTGCC
CIKR Cross-Sector Council
Regional Consortium Coordinating Council

Source: U.S. Department of Homeland Security

Figure 4 NIPP Sector Partnership Model

3.3 QUESTIONS AND ANSWERS HIGHLIGHTS

Transcripts

Q&A

Q: How would we use an interagency team approach to energy resource security, including rules, tools, and processes to allow DoD, DoE, State Department, DHS, etc. to have major roles to contribute?

Ms. Celina Realuyo – Having actually been a victim—or more importantly, a beneficiary—of interagency collaboration, having tasked these types of things out, I think the biggest question is to figure out who is actually in charge. In his Keynote Address (Chapter 1), Jim Locher mentioned that the idea of setting up specific "task teams" is a novel concept that they hope to be putting into place in the next couple of months. I suspect it might be on energy security, although he did not disclose what it was going to be about, and I am not privy to that.

The question, then, is does that leadership come from the White House? Whether that is embodied in someone at the NSC level or elsewhere, it is important to have the right people at the table. Many of us have been tasked to represent our agencies at many of these very painful Policy Coordination Committee (PCC) meetings that last for hours. There was seldom a well-defined agenda or very efficient use of time or clear parameters of authority the attendees were able to bring to the meeting, particularly to respond to a certain crisis.

Another thing I have observed over the past couple of years, particularly in the post-911 context, is the need to prepare and practice. Often that is a question of gaming; many of my colleagues unfortunately do not take exercises and games as seriously as perhaps they should—because maybe they have never been in a crisis.

I had unfortunately the sad duty of being on-call at the White House Situation Room during the Oklahoma City bombings 19 April 1995. That was one of those examples of a rude awakening situation in which we actually had to draw on the interagency. As you may remember, it was one of the first times in the mid-1990s we actually used the Corporate Information Management Vision System (CIVIS) with all of the cabinet members via videoconferencing where technology was our friend. We had not truly tested the system at that level. Thankfully, it worked. But it was sad that it was a tragedy that brought upon that interagency collaboration.

The spirit is there, I think, with the new administration coming in, and particularly as energy is a top priority for the Obama administration. The question, then, is how to delineate the roles and then more importantly be able to move forward with action plans that respond—whether it is the crisis de jour or a broader approach to this idea of energy security or energy independence.

CAPT Jan van Tol – I would just like to reiterate what Celina said: The key to this is exercising and practicing these things at the highest levels. In the context of the Undersea Energy Infrastructure (UEI) problem, one of the things that surprised us the most is how little awareness of the vulnerabilities was present at senior levels of government.

Q: *I have a short question for Jan van Tol about the role of Mexico in the UEI game. The attack was in the Gulf of Mexico but never mentioned Mexico. Was Mexico also attacked or not? What engagement, if any, did we have in Mexico to help fill in? What was the role of Mexico in the game important for anyone interested in international relations?*

CAPT Jan van Tol – I would have loved to have Mexico be part of the Red coalition, but the sponsor directed us to keep them neutral—presumably because of possible political sensitivities should the story of the wargame get out to the press. Keep in mind what we were trying to do in the game is look at the tactical-level problems of defense of UEI, not at specific national interests in the region. Obviously for the U.S., the Gulf of Mexico is the place of greatest interest. We needed to have a geography to explore the undersea tactical issues. In other words, it was not a game about political military issues. Remember, too, that the wargaming here is only to surface issues. It is not at all to make predictions about the future.

Q: *Professor Klare gave a very clear and cogent speech on the prospect of conflict over resources. My problem with the speech is that it could have been given 50 years ago. It could have been given 25 years ago. In fact, it was given during the Korean War boom of 1951 in spirit, if not in detail, and it was given again during the commodities boom of 1973. And yet, as I think of the bloodiest wars over the last 50 or 60 years—Korea, Vietnam, the Soviet invasion of Afghanistan, the Iran/Iraq war—none of them in my judgment were fundamentally resource wars. So my question to Dr. Klare is, what is going to make the next 20 years different from the last 60? I do not mean that we should not pay attention to resource conflicts. My suggestion rather is that they are ever-present. We should pay attention to them, but why are they going to be more prominent in the future than they have been in the past?*

Dr. Michael Klare – Thank you very much for that question. I would enjoy discussing that at much greater length than I think anybody would want to have me speak on it today. It is a wonderful kind of conversation that my students love to have with me. Some of the answer to that was implicit in my presentation, some of it explicit, and some I cut for reasons of time.

I think there are dramatic differences between the current and future period than were true 25 or 50 years ago. One is I did say there is an unprecedented increase in demand. I did not talk about the rise of China, but that certainly was in the prepared comments I have. Suddenly we have a rising economic dynamo in China—with India coming along—which has a demand for resources on a scale that has never before been seen, except possibly for the rise of the U.S. over the past 100 years or so, but much more intense, much more compressed. So, there is just the pressure for resource demand increasing enormously along with population growth on an unprecedented scale.

Global warming is going to have an extraordinary impact on the availability of resources for hundreds of millions of people.

That is coupled with what I did talk about, which is that we are facing—unlike 25 and 50 years ago—a dramatic contraction in the availability of certain key materials on which we rely so greatly, especially oil and, in the not too distant future, water. The human population has never faced this kind of resource contraction on this kind of scale before. This is dramatic.

The third factor—which I did mention but because of time only alluded to—and this is the big whammy, and that is global warming. Global warming is going to have an extraordinary impact on the availability of resources for hundreds of millions of people. And it is coming. The effects are visible today, but the impact will accumulate with time, and this is primarily going to be seen in areas in the developing world that are already suffering from water scarcity in particular. Global warming is not going to deprive the world of water uniformly. Some areas—Northern North America, Northern Europe, and Northern Russia—will have increased water supplies, in some cases too much water with intense flooding. But large parts of Africa, parts of Central America and Mexico, parts of Central Asia, Southern Europe, and the Mediterranean Basin, are going to have significantly less water. In parts of Africa, the Intergovernmental Panel on Climate Change (IPCC) projects 250 to 500 million people facing food scarcity, and this is going to create a global security crisis—food security crisis—unlike anything we have ever seen before.

This does change the situation in very dramatic ways. Again, I would love to be able to discuss this at greater length, but these are just some of the ways that the world is changing dramatically with respect to the resource picture.

Q: *From an economic point of view, substitution and income effects will result in using more of energy sources, other than petroleum, for example, and using less energy per unit of output. What might be some expected reactions to rising resource prices? That sounds like two questions, so let us look at the first part of that, some of the effects of using alternate energy sources and squeezing more output out of each unit of energy.*

Dr. Michael Klare – This again is a complicated picture and one that we cannot be absolutely certain how it is going to play out worldwide. This will favor countries like the U.S. and the European countries that are in a position to benefit from the development of new energy sources and where we are quick to put these new technologies to use. I think we are going to see many benefits from that. Many entrepreneurs are going to arise, and I hope that we will see the growth of entire new industries in this country that will develop these new technologies, create jobs, and create economic growth. So that is a good thing. It will also encourage conservation. Of course, some of these new sources of energy will be more expensive. So, it will encourage conservation in the use of resources.

But there are negative sides to this because not everybody will be able to afford these new technologies. In places where people do not have the money to do so, they are going to suffer all kinds of negative consequences. One problem that the World Bank has been looking at a great deal is the growing use of crop land to produce biofuels for transportation, thereby depriving the use of that land for food production. It is raising the cost of food—basic food commodities—in many parts of the world, which is a cause of malnutrition and hunger for many people. So, there will be positive and negative consequences.

Ms. Celina Realuyo – For those who are interested, the Department of Energy and the new Secretary of Energy, Dr. Steven Chu, as part of the stimulus plan that all of our tax dollars are paying for, are looking at how to encourage the development of alternative energy sources. The idea is to make it more affordable for average Americans to be able to access alternative energy resources.

However, Dr. Klare is right, in terms of who will and will not benefit from technological advances and access to these types of alternatives. The problem is, those who do not have that access are going to see much economic instability. It is the "food or fuel" debate, and we are even dealing with it here in the U.S. in places like Omaha, Nebraska. Is it better to grow corn for ethanol or to grow corn for the cattle supply—which, of course, effects the dairy supply? It is not just a problem of the Third World or the emerging markets, but also here in the U.S.

We want to get off the dependence on foreign oil, and we are trying to use the government stimulus package to encourage new technology to come online much faster. The question is, to what extent can the private sector absorb new technologies or begin developing them within the timeline that the recovery plan has, which I think is 18 months? Can you actually move to developing commercially applicable solutions within a short timeframe given a capital infusion—which is a good thing, but sometimes is actually a curse if you cannot actually meet the expectations.

Q: *This question relates to Professor Klare's comments during his luncheon address: What are the limitations of the military instruments of power in the emerging resource competition environment?*

Dr. Michael Klare – I did address that in my talk. The question is, what are the sorts of threats and how usable are military instruments in responding to them? If you are trying to protect a pipeline that stretches 500 miles across a very difficult terrain, can you afford to station soldiers every 100 feet to defend that pipeline, which is what it takes in some places? That is probably not a very effective use of military manpower. The same is true of protecting the sea lanes. Can we have a Navy large enough to protect all of the sea lanes that are at risk? I don't think so.

On the other hand, there are some very vulnerable areas, such as the Gulf of Guinea and the area off the Coast of Somalia, that are at great risk where cooperative naval activities in multinational naval operations might be very effective. So I do not think there is a single answer. I think it is a matter of where a military response might be appropriate, but I think the answer to that is probably "rarely."

CAPT Jan van Tol – I would partially agree, partially disagree. It depends an awful lot on what is the specific nature of the threat? There are some types of physical attacks to which military response or military protection might be entirely relevant. There are other ones where the military may be forced to choose among many competing needs to provide protection. A lot of our military effort obviously is spent protecting energy flows and to some extent indirectly infrastructure in the Persian Gulf.

When we price our military forces, we price energy. We do not include the price of military forces and deployments that are required to protect those. If there was some mechanism for doing so, then perhaps an alternative may end up being far less expensive than employing military forces.

Dr. Michael Klare – I know that this program is cosponsored by the Paul Nitze School of Advanced International Studies (SAIS). I have not met anyone who is from there, but maybe there are people here. I think this is as much a foreign policy question as a military question. Because I think we get into trouble as much by our choice of allies and the fact that we have forged "special relationships," in quotation marks, with particular foreign governments for historic reasons. For example, there is the "special relationship" forged between the U.S. government and the House of Saud, originally on 14 February 1945, when President Franklin Roosevelt met King Abdul Aziz aboard the USS *Quincy* and forged the relationship that basically guides U.S./Saudi relations together. Whereby, the U.S. made a promise to protect the House of Saud indefinitely in return for privileged access to Saudi oil. That implies a pledge to protect the Saudi regime—the Saudi family—against internal as well as external attack. This has all kinds of implications for U.S. military purposes.

The question is not whether the military is doing the right thing or the wrong thing under certain circumstances, but whether that is in 2009 a correct foreign policy position to maintain, whether that original agreement is still in America's best foreign policy interest. I would like to have a debate about that today. I do not believe it is still in our best interest to maintain that original agreement. Some of you may think it is a good idea. We could have a good discussion about it, but the problem is not what military actions are being conducted on a day-to-day basis in accordance with that agreement, but whether that agreement is a good idea or not. Thank you.

Q: To what extent does common interest in stable oil supplies force the U.S. and China to passively or actively support each other in opposing nonstate actors such as terrorist organizations?

Ms. Celina Realuyo – Having been a diplomat, I would look at it through a different lens: You really must try to find with your adversaries or your rivals—and this works very well in business as well—a place for common ground, for you to see where you actually have those common interests. Particularly in the case in which you must look at not just the U.S. and China, but you must bring India into the picture as well—which is a large consumer with pent-up demand for oil and gas resources—you have to try to figure out how to cohabitate, if you want to use that word, in different parts of the world. Whenever you travel now to Africa or to South America, it is very rare that you will be on a plane and you do not see a Chinese official businessman or woman on the same flight. They have a very interesting way of are looking at a very long and protracted timeline in the relationship, both in diplomatic and economic ties, particularly in places such as South America.

We have been there for many decades, but sometimes some people argue—and I actually was originally a student of Latin American studies—we have forgotten about this hemisphere. As we now retrench and discover that many things are happening just south of our border, anybody who has watched the news the past couple of days would have to conclude that this is an area where two nation states can actually think of not just being rivals, but actually being collaborators. Whether that means now looking at sharing all of this new technology for carbon sequestration or not, I would say the right way to look at alternative energies is by sharing as opposed to this rivalry. That is something that I think is moving forward.

I have done business with the Chinese. Trust, but verify. But there are amazing places that they are now allowed to go, and they have been leapfrogging much of the technology and spaces such as energy. We should actually be more open minded to learn from that and seriously think about how to leapfrog in our own country as well—because much of that technology and the brain cells were actually incubated here in the U.S.

Dr. Michael Klare – I believe that this is an area where we should make this a high priority: Rather than view the U.S. and China as competitors that are destined to engage in resource wars over energy, which is where many people see the way things are headed, I think we should head that off at the pass and see the U.S. and China as potential cooperators in the path towards developing energy alternatives and cooperating. This is one area where I think there is much potential. There was already some agreement on this.

After 9/11, the U.S. and China agreed to cooperate in fighting Uighur separatists in Xinjiang Province. Uighur terrorist groups were added to the State Department's list of terrorist organizations. The Movement for the Emancipation of the Niger Delta (MEND), the organization that I mentioned, threatened China's activities in Nigeria. China's facilities have come under attack. Oil facilities and personnel have come under attack in Sudan and in the Ogaden region of Ethiopia; they are at risk from the same kind of behaviors that I discussed in my talk. I think there is a common basis for cooperation in working together to prevent these kinds of attacks. This could be a basis for cooperation.

CAPT Jan van Tol – You would think that certainly there would be plenty of space for cooperation between the U.S. and China in ensuring the free flow of energy and other trades at sea. And you would think that the Chinese would appreciate the free good that in essence the U.S. Navy tends to provide in terms of maintaining freedom in the navigational regime. Yet, we see increasing competition in the naval realm from the Chinese—not too much yet, but the trends are quite clear.

Q: *The speakers keep referring to technological changes and changes to environmentally friendly technology so the U.S. is less dependent on foreign oil. What they fail to mention or address is the time period required to make these required changes in the next 10 to 15 years. What are the short-term recommendations to fix these problems? In other* *words, if it is going to take 10 to 15 years before we have these alternate energy sources, what do we do in the meantime?*

Dr. Michael Klare – Absolutely. The questioner is absolutely right in saying that. That was the intent of my presentation: to say that if we are going to remain dependent on imported energy in the meantime, we must try to move away from an automatic reliance on military means to protect that and to rely as much as possible on market forces. I believe that we should sever as much as possible the military aspects of our ties with the foreign providers of our energy so that we are not associated with foreign dictators and therefore incur the wrath of populations that despise us because of those ties. Just buy oil from whoever wants to sell it to us while we work as hard as we can to diminish our reliance on foreign oil providers.

Ms. Celina Realuyo – As a person who has worked in venture capital and private equity, and looking at the space myself on a personal level as well as professional level, there are actually technologies out there that are coming on line. One very interesting project—and it was the first project out the door that was infused by a $535 million loan guarantee from the Department of Energy on 20 March—was for construction of the Solyndra, Inc. solar panel manufacturing plant in California.

That is an example where now the private sector needs to step up, working with a new team on energy to figure out how to use the stimulus plan to leverage new technologies, but more importantly to get those dollars to technologies now to move them closer to that commercialization point than they have been in the past. Although we do not really know how well this technology works, for the first time, we actually have government and the private sector really in partnership with a timeline to put our tax dollars to work in the most efficient fashion.

Chapter 4

ROUNDTABLE 3

Responding to Economics and Financial Attacks

4.1 MODERATOR'S SUMMARY

Ted Smyth

INTRODUCTION

I would like to set the stage for discussion of the economic and financial world in which we live and provide you with the context for the briefing that will follow from Jim Rickards as well as briefings from our other panel members. Unless you have literally been marooned on a desert island for the past 12 months, you fully appreciate the fact that we live in a rather gloomy economic and financial world. In the space of a year, our economic and financial world has changed somewhat dramatically. Although the world remains as interconnected as ever through telecommunications, the arts, culture, and the Internet, the once steady advance of economic globalization that changed the lives of millions is facing at least a strong pull back through financial retrenchment and potentially resurgent economic nationalism.

Mr. Ted A. Smyth (USMC, ret.) is a Fellow within the National Security Analysis Department and a Fellow and former President of the Military Operations Research Society. Since joining The Johns Hopkins University Applied Physics Laboratory, he has served as the Director, Campaign Analysis Team of the Surface Combatant 21 Cost and Operational Effectiveness Analysis, as the Director, Land Attack Warfare Studies, and as Supervisor of the Effects Based Operations Group of the National Security Analysis Department. He is a former Marine Corps Colonel with 30 years of active service commanding units at the company/battery, battalion, and regimental level. He recently led a The Johns Hopkins University Applied Physics Laboratory Analysis of Alternatives on the Joint Effects Targeting System and an Economic Analysis Study.

Some nations that once invested heavily beyond their borders are now sitting on the sidelines as the global economy flounders. Those who had invested so heavily in the likes of Citibank and Merrill Lynch have been burned and are in all probability going to be much more cautious—if not reluctant—to invest in the future. In fact, some economists have gone so far as to suggest, and I quote, "the collapse of economic and financial globalization is absolutely possible."

Compounding this economic and financial environment is the fact that we live in a dangerous, unstable world, a world that has witnessed an expansion of potential threats and new forms of warfare, intelligence gathering, and advancing technologies.

> *"The longer it takes for the recovery to begin the greater the likelihood of serious damage to U.S. strategic interests."*
>
> *— Annual Threat Assessment, Director of National Intelligence*

Our multipolar world now requires us to consider a wide range of security issues that include combating terrorism; the possibility of pandemics; the proliferation of weapons of mass destruction; insurgencies; and conventional warfare missions that include homeland security, regional conflicts, postwar stability and reconstruction, and cyber and resource attacks. Of interest to some attending this symposium, and very much related, is our ability to respond to such diverse challenges and, specifically, to understand what the implications of this economic and financial downturn might be on those companies and corporations that are focused on our national defense. Gordon R. Sullivan, President of the Association of the U.S. Army in September 2008 listed some of the potential impacts to defense contractors if the credit crisis is not resolved soon:

- Failure of contractors to meet cost and schedule requirements (increased cost and risk on programs to DoD)

- Decreased competition (increased costs for DoD) as the number of capable companies is reduced

- Deterrence of new small business start ups (less competition, more risk, higher cost)
- Risk aversion in large companies, which may result in decreased spending on technology development
- Decrease in acquisition and merger activity (decreased efficiency of the overall defense sector)

Now, into this mix, we must add the potential of active economic and financial threats. Well-documented cases already exist, in which some organizations have chosen a variety of means to support actions against nation states. Methods to fund the threat include the use of nongovernmental organizations (NGOs), state support, wealthy individual donors, trade-based donations, and cash smuggling. In Roundtable 1, Dan Wolf described the attacks directed against Estonia and the Estonian banking system [Cybersecurity: Attacks on the Critical Infrastructure]. Whether such warfare will mirror the Estonia case or will take the form as evidenced by Hezbollah, which involved the movement of financial support via seemingly legitimate NGOs in support of terrorist activities, remains to be seen.

> *"The global economic crisis is the most serious security peril facing the United States."*
>
> *— Dennis Blair, Director of National Intelligence, 13 February 2009*

Importantly—and quite frankly very fortunately—key government leaders have recently recognized that economic and finance-related issues and actions are now prime concerns as they relate to our national security. Perhaps in recognition of this peril is the Obama administration's recent appointment of a gentleman by the name of Michael Froman, perhaps known to some in this room, to a dual position. Mr. Froman is appointed as the Deputy Assistant to the President but also the Deputy National Security Advisor for International Economic Affairs, a position to be held jointly at the National Security Council (NSC) as well as the National Economic Council.

ECONOMIC AND FINANCIAL THREATS

Now, let us consider specific economic and financial threats to gain a clearer understanding of the nature of these threats and their potential implications for our national security. The second phase of our investigation into economic and finance attacks well be a discussion on how to create imperative for interagency action and options for enhancing appropriate capabilities.

Are we prepared to counter economic and financial attacks? To counter them effectively, the U.S. Government needs a planning process to enable a comprehensive national approach, and that must result in a comprehensive national doctrine. This premise is clearly consistent with what we heard from our keynote speaker, Mr. Locher. Although we are trying to remedy some of these deficiencies, we are not there yet. However, the good news is that as of February, for the first time in recent memory, the intelligence report that the President receives on a daily basis now includes reference to economic and financial issues, the effects of the financial crisis and its cascading effects on the stability of countries throughout the world, and the potential implications of those issues on U.S. national security.

THE PANEL

This roundtable includes a superb group of speakers: a well-respected authority on this subject and Senior Managing Director of Omnis, Inc. (Mr. James Rickards), a Senior Research Fellow at the Kennedy School of Government at Harvard University (Dr. William Overholt), a Senior Professor of China Studies at The Johns Hopkins University School of Advanced International Studies (Professor Pieter Bottelier), and the Maurits Boas Professor of International Economics also at Harvard University (Professor Richard A. Cooper). The panelists will have the opportunity to respond to Jim Rickard's paper and presentation and propose interagency actions and options that will allow us to address some of these economic and financial threats.

4.2 OVERARCHING ECONOMIC THREAT

Pieter Bottelier

GENERAL COMMENTS

One of the great merits of Jim Rickard's report on economic and financial attacks is that it forces you to think about things that you do not normally think about, concepts such as weaponized money. His report can serve as a useful manual for discussion or instruction on issues that are unquestionably very important. I will start with three general comments, make some observations on some of the scenarios in Mr. Rickard's report, and then end with some conclusions.

It is ironic that we are here together to discuss the possibility of some foreign financial or economic attack on the U.S. Presently, we are in a mighty crisis, which we have provoked ourselves. To reiterate what Dr. Overholt mentioned in his address to this roundtable, no adversary could have done to the U.S. what we have done to ourselves in neglecting proper regulation and

Professor Pieter Bottelier is an economist and China scholar and has served as a Senior Adjunct Professor at The Johns Hopkins University School of Advanced International Studies since 1999. He has also served as a Senior Advisor on China and an Adjunct Lecturer at Harvard University's Kennedy School of Government in 2001-03 and at Georgetown University in 2004. He is the author of many articles on China's economy. Previously, he was Chief Economist and Marketing Director of the (then) Zambian State-owned copper company (Lusaka), 1968-70. Professor Bottelier has earned degrees from the University of Amsterdam and MIT. He was a Harkness Fellow of the Commonwealth Fund in New York and a Research Associate at the Brookings Institution from 1963-64.

supervision of the U.S. financial sector during the past seven or eight years.

It is sobering to realize that the enormous losses that we have inflicted upon ourselves and the rest of the world are the result of gross mismanagement of our financial system. While I recognize that foreigners or adversaries of a non-state nature could try to inflict significant damage on this country by causing disruptions of the financial system, I do not think anybody could do as thorough a job as we have done ourselves.

Having said that, I believe Jim Rickard's report is a valuable addition to the discussion of our vulnerabilities to financial attack. I cannot claim expertise in financial markets as much as he does. I have never run or advised a hedge fund. I initially had some trouble understanding credit default swaps; I had never heard of them before the crisis broke. Although I am not an insider in the financial world, I am quite convinced that this report provides an excellent basis for discussion on these subjects.

The third general comment is that I have also been convinced that non-conventional threats to U.S. security in the form of monetary, financial, and economic attacks are a serious matter. We have not really seen much of it—that I am aware of—but I think it behooves us to think these issues through because one day those threats might become serious. We are naturally more inclined to think of security threats in terms of military issues, access to raw materials, and other related concerns. I think some of the scenarios in Jim's report are potentially very real, and as such, I commend his work.

ANALYSIS OF SCENARIOS

One of the scenarios Jim explores in the earlier part of the report is the possibility of an organized, coordinated hedge fund attack on the U.S. by a group, either a state or a non-state actor, that puts together maybe $10 billion leverage in the U.S. capital markets to cover a huge fund with which they can purchase assets and then release them in a way that disrupts markets and decreases asset values.

When I was reading that, I wondered, “Is that plausible or not? Which state actor could possibly be motivated to organize such a thing?” I could not really think of one. The actors that would have enough money, knowledge, and expertise to carry out such an action would be Canada, the European countries, China, or maybe Russia, but we must ask: what could be their motivation and how could they benefit from an economic crisis in the U.S.—assuming they can actually provoke one, which I doubt. The possibility that a non-state actor—al Qaeda, for example—would come up with such a scheme seems even more remote.

Although I found the idea interesting and thought provoking, I did not come away with the impression that this was a real threat. Europeans would never do it. They would have absolutely zero motivation. I cannot think of any reason why the Chinese would wish to try, except perhaps in the unlikely case of war over Taiwan, but even then, it sounds implausible to me. I do not think the Russians could organize themselves to do it. Who is left? Brazil?

On many of the other scenarios, I had different reactions. I think that the risks to companies of strategic importance to the U.S. are perhaps more serious than I had first realized. I can see that through various mechanisms, ill-intentioned foreign parties, states, or agents on behalf of state or non-state adversaries, could indeed acquire a minority interest in disguised forms and begin to influence or gain access to privileged information in a way that escapes attention. I was rather impressed by that section of the report that deals with equity positions in U.S. companies that can be disguised in ways that are hard to detect. I think we should study that carefully. Whether the current instruments with which we deal, enumerated in the back of the report, or the various legal instruments we have are adequate to deal with these risks, I do not know. I am inclined to think not.

On sovereign wealth funds, which are the focus of many of the comments in Jim’s report, I see a potential threat but, realistically, nothing serious. Russia’s pile of money is dwindling as a result of lower energy prices and efforts by the Russian Central Bank to support the exchange rate through the sale of reserves, so I do not see Russia in a position to inflict serious intentional damage on U.S. companies or financial systems through the use of its sovereign wealth funds or proxies for them. The largest sovereign wealth funds are actually held by countries in the Gulf and Norway, which are allies of the U.S. Norway has a huge fund, and I think Jim correctly identifies that as one of the most transparent operations of its kind.

China is a bit of a question mark because its leaders are very new to this. The initial $200 billion they put in that fund is often seen to be a potential threat to foreigners, although I am personally inclined to discount that threat. I just came back from China on Sunday. While there, I met with some of the senior managers overseeing their sovereign wealth fund. They are having a hard time. Their first investments (in the Blackstone Group, Morgan Stanley, the Belgian Dutch Bank, Fortis, and Barclays) were all bummers: They lost 80 percent of their money. To deal with the suspicion that the Chinese state might use that fund to gain access to corporations surreptitiously, they are trying to emulate the Norwegian example by subcontracting the investment of these funds through a number of independent agents, who would then compete amongst themselves to get the best return for the parent company.

The significance of what I see in Jim's report is that the Chinese cannot win. If they do not follow the Norwegian example, they will be subject to the suspicion that they themselves directly used that fund for political purposes. If they subcontract investment decisions to independent agents acting in their own name, there is a new suspicion, namely that these agents would gain positions in companies without divulging that they are actually owned indirectly by the Chinese state.

I am inclined to think that we should not be so afraid of these sovereign wealth funds; they have a very useful role to play in our damaged global financial system. They can contribute to the recapitalization of our banks and non-financial corporations with long-term capital that is not leveraged in the same way as hedge funds. I am altogether in a more positive frame of mind on sovereign wealth funds. I see them as mostly benign and potentially very helpful to us in the current crisis.

Jim plausibly argues that there are all sorts of devious contractual arrangements, wolf pack attacks, and derivative contracts that can be used as weapons to strategically gain access or control over important companies or commodity markets. I agree. We should understand these things. If there are such risks, we should carefully examine whether our regulatory supervisory system adequately protects us against these risks.

Another scenario he discusses at some length is the possibility of market and price manipulation through the spreading of rumors, announcements, and so-called head fakes. These could undermine open market processes and I think can be harmful. However, I doubt very much that they could cause disturbances and damage on a scale that could cause national security risks. Nonetheless, these are risks that we should consider.

Concerning the macro-oriented scenarios that Jim developed—scenarios that discuss undermining the U.S. currency as an international reserve currency—I think they are useful. The first scenario is the Russian gold reserve dollar. I have not really thought that through, but it is an intriguing idea: one country with a lot of oil and gas to export and little else could create a gold-based currency with which it could require its customers to pay.

However, we have to think this through a little further. For example, what would happen to oil prices if this pricing mechanism would unintentionally trigger a recession in the industrialized world? In conventional dollar terms, the price is likely to go up sharply. The demand for oil would then shrink. What would be the consequences of that, particularly if the Organization of Petroleum Exporting Countries (OPEC) were then to undercut the Russian pricing scheme by offering different rules and discounts?

Another question I have not thought through but wonder about is: what will happen to the ruble? Jim suggests that it would remain the domestic currency for Russia, but how long can we maintain a watertight separation between the new international currency, aimed at sharp depreciation of the U.S. dollar, and the ruble? I think that after awhile, that system would be in danger of collapsing because it would lead to all sorts of unintended domestic economic and social consequences in Russia.

In any event, it is interesting. We should think about it. I am not convinced that this is a real option for the Russians. I am certainly not convinced the Chinese would join the Russians for two reasons: (a) the Chinese are smart enough to see the possible pitfalls of such a scheme and (b) they never fully trust the Russians. They would not go along with the Russians simply to pester the Americans.

The possibility that China might drive a wider gap between short and long-term interest rates in the U.S. by (1) selling an initial $100 billion worth of Treasury holdings and then announcing that they would sell more if the situation would warrant it and/or (2) shortening the maturity structure of the Treasury holdings to steepen the yield curve significantly could become troublesome for the U.S. economy. However, China would pay a price for that. They would significantly reduce the returns on their investments. Why would they do it? The Chinese want to build their own economy as quickly and as strongly as possible; a prosperous U.S. economy is much more helpful to them than a damaged one. The Chinese are a stakeholder in America's prosperity, as we are in theirs. It is hard to imagine circumstances that would fundamentally change this equation.

THE OVERARCHING THREAT

Whereas we should have security people worry about these potential scenarios, the biggest threat to U.S. security is the U.S. itself. Economic mismanagement in the U.S. has triggered the largest crisis in the last 80 years. It has spilled over into the global economy, unintentionally causing enormous wealth losses, almost equal to global GDP by the latest accounts.

What is the answer? I think the best security protection for the U.S. in the economic/financial arena is to have good domestic supervision and regulation of the financial system. A second precaution is economic policies aimed at ensuring a strong, real economy and high employment. I think we have to reform the health care and education systems. We have to rebuild infrastructure and aim at much higher levels of energy efficiency. Japan and Europe are well ahead of the U.S. in terms of energy efficiency. Our dependence on imported energy and the associated vulnerability is much greater than it should be and can be with sound economic policies.

I believe that Jim wrote an interesting and important report, but it does not, in my opinion, profile what I see as the biggest security risk: poor oversight of our financial system.

4.3 RESPONDING TO ECONOMIC AND FINANCIAL ATTACKS

Richard Cooper

GENERAL COMMENTS

Jim Rickards' report concerning economic and financial attacks is a long and very rich paper. I found a very useful summary late in the paper of existing U.S. laws, institutions, and instruments to deal with some of the threats that he discusses in the core of the paper, as well as a much briefer, but nonetheless useful, summary of instruments available to the European Union. He provides a quick rundown of what could be done instrumentally and legally to deal with threats to the U.S.

In contrast, I found his long introduction on economic models and financial markets simply a distraction. I found it a confusing mixture. The essential point, which I think is correct, is that modern financial markets are large, complex, nonlinear, dynamic, and stochastic systems. Economic models are very useful for pedagogy and for understanding some features of these systems;

Dr. Richard N. Cooper is the Maurits C. Boas Professor of International Economics at Harvard University and Chairman of the Advisory Committee of the Institute for International Economics. He was the Chairman of the National Intelligence Council (1995-97), Chairman of the Federal Reserve Bank of Boston (1990-92), and Under Secretary of State for Economic Affairs (1997-81). His many books about international economic policy include Economic Policy in an Interdependent World and Boom, Crisis, and Adjustment: Macroeconomic Management in Developing Countries, as well as hundreds of articles. He received his B.A. from Oberlin College, his M.Sc. from the London School of Economics, and his Ph.D. from Harvard University.

unfortunately, the economic models have been applied within the risk management sections of banks, insurance companies, and rating agencies, but they are totally inadequate to deal with the nature of real markets in all of their complexity. That is a point worth making, but it also has a bearing on the possible threats to our system.

ANALYSIS OF SCENARIOS

The Rickards report has a section on the national security implications of the current recession. Some of you know that the House Armed Services Committee held hearings on this particular issue two weeks ago, where I was one of the panelists discussing what the possible implications are of the current recession. Those discussions are available elsewhere, so I will not comment further on them. [1] Instead, I am going to focus on the three sections of the paper that detail possible manipulation by foreign entities, either governments or possibly nongovernment entities or adversaries, against U.S. interests. I will focus on deliberate manipulation.

The first such manipulated activity involves what could be called swarm tactics by one foreign entity operating through many channels or several foreign entities operating in collaboration, designed to disrupt U.S. financial markets and cause financial and/or economic chaos. The Rickards paper provides a very useful discussion concerning how any foreign entity so motivated could conceal its activities ahead of time in today's financial markets; this issue also was broached in Dan Wolf's discussion of cyber attacks [Cybersecurity: Attacks on the Critical Infrastructure]. We could not necessarily—at least initially—attribute such actions to a particular source; this assertion is a very useful contribution to this topic. It is certainly possible that such an action could take place.

To reiterate Rickards' essential point, financial markets are dynamic, large, complex, nonlinear, and stochastic systems. They are hard to predict, not only by analysts in the U.S. but also by any foreign adversary who wanted to disrupt them. The probability of disrupting them through a single action or set of concerted actions is negligibly small. It would be a coincidence if it were to occur. It could occur, but it would just be a coincidence.

" . . . financial markets are dynamic, large, complex, nonlinear, and stochastic systems. They are hard to predict, not only by analysts in the U.S. but also by any foreign adversary who wanted to disrupt them."

Consequently, any strongly motivated adversary would have to try several different methods many times to achieve a successful disruption of markets. This trial-and-error methodology makes the action, in principle, detectable. It is like code breaking. If you have a single message in code and the coder is good, you have negligible chance of breaking the code, but if there are repeated messages in the same code, a competent cryptographer is likely to break it. This is one area where I think there is some scope for interagency interaction. I just want to note, as Rickards does in his paper, that market manipulation of U.S. markets is illegal and actionable by the Securities and Exchange Commission (SEC).

Another section of the Rickards report relates to covert acquisition of a controlling interest in companies that have technologies or other information that might be useful for a foreign adversary. Again, I think the Rickards paper has done a good job of indicating how this could be done. With current markets, it would be easy with some forethought and effort to acquire a controlling interest in an American company through diverse channels.

What Rickards does not explain is how, having achieved such a controlling interest, the adversary could then take adverse action against the U.S. Additional steps are necessary beyond simply achieving controlling interest (e.g., controlling enough voting shares). I can identify three possible channels.

One, after achieving a controlling interest, the foreign adversary could change the Chief Executive Officer (CEO) and other board members. However, hostile proxy fights in the U.S. attract a lot of attention. This would no longer be a covert action. If the U.S. government is paying attention and has some idea of what it wants to look for, then such an action would clearly be detectable. Again, this is another area for interagency cooperation.

It would be harder to detect if the acquirer persuaded the CEO and the board that the agent should actually have a board seat, thereby not starting a noticeable proxy fight. This second scenario, of course, requires the cooperation of the CEO and the existing board and gives away the concealment. As Rickards reminds us, under our laws, if you acquire more than five percent of a publicly traded U.S. corporation, by law you must declare your acquisition and what your interest is. Are you just a portfolio investor, or are you planning to acquire more shares and so forth? It is a giveaway, and it is illegal if it is not declared.

The third possibility would be threats to the CEO or the Chief Financial Officer (CFO) through, for example, sales of stock in which the officer owns a lot of options. The officer can be financially damaged if he does not turn over information that is desired by the adversary so that, in effect, the CEO or some other senior officer is recruited by the foreign adversary as a spy. That is the only way to describe it. That is always possible. Even without stock ownership, it is possible, although owning some stock may make the possibility of extortion somewhat greater.

This scenario threatens the security of U.S. companies generally, particularly those dealing with highly sensitive defense work. It is not a new problem, although financial leverage may add a new dimension to the capabilities of a foreign adversary. Again, it would violate several U.S. laws. This is certainly another area for interagency cooperation and raises the question, who is responsible in the U.S. government for dealing with industrial espionage?

The third section of the Rickards paper that deals with manipulative action by foreign entities, especially governments, concerns a somewhat creative proposal for issuing a gold-backed currency with the objective of undermining the U.S. dollar. Russia is used as an example. However, Rickards indicates that although Russia is the most obvious country, it is not the only country that could do it.

I have to say I do not understand this proposal at a fundamental level, or I find it completely farfetched. The key idea is that Russia would create a gold-backed ruble, managed from either London or Zurich, and insist that its oil and gas sales should be paid in this new currency. The original paper valued the gold ruble or the gold behind the gold ruble at $4,000 an ounce, roughly four times the existing price, although the revision dropped the initial price to around $1,000 an ounce. The assumption is that the price would quickly rise much higher than $1,000 an ounce.

This action allegedly would undermine the U.S. dollar as an international currency and, through U.S. inflation, would also undermine it as a domestic currency. Fundamentally, I do not understand the dynamic that links the action proposed. Russia could issue a gold currency at any time with the supposed result. Rather than go into it in detail, I just want to list a number of questions—Pieter Bottelier has already touched on a few of them—that require sound answers for me to concede that this is a reasonable option. Even so, I think that my own list of questions taken together cannot be answered in a way that is persuasive.

First, as Rickards points out in his paper, it would not take a government to carry this out. Anyone with enough capital could issue a gold-backed currency. If it is going to be as lucrative as Jim suggests, the equilibrium price of gold must be around $4,000 an ounce. That is more than four times the existing price. This is an economist type question: Why has someone not done it? It looks like a $20 bill lying on the sidewalk. Why has someone not picked it up?

Presumably the answer is that Russia would be more persuasive. First, it has a pile of dollars that it could use to buy the gold. Although, as Pieter Bottelier said, that pile is diminishing rapidly as we speak. Second, Russia, unlike a private party, could insist that at least its oil and gas had to be paid in this new currency. Russia's trustworthiness is very low worldwide, hence the role of London or Zurich in ensuring success, which is part of Rickards' proposal.

My first question is: Why would either Britain or Switzerland cooperate with Russia in a scheme whose objective is to undermine U.S. currency? The second question, as Pieter Bottelier touched on, is: What would Russia do with its existing ruble? Concretely, will the Russian public and private oil producers and the mostly private gold producers be paid in the gold ruble or with existing rubles? The Russians would have to make that decision, and either way, it does not go well. If they did not pay the gold and oil producers in the new currency, it would create a credibility problem in the rest of the world. If they did, it would create deep complications for the Russian economy.

Third, how would other oil exporters—Mexico, Saudi Arabia, and Canada or Norway, both members of the North Atlantic Treaty Organization (NATO)—respond? If Venezuela were the only country to sign on, why would the scheme take off?

Fourth, there is actually a lot of gold in the world. Some of it is in the ground. However, at $4,000 an ounce—even at $1,000 an ounce, which is roughly where we are now—much more of that gold is going to be mined and processed. Mining companies are sifting through the tailings of the mines of the 19th Century because at today's prices it is profitable to extract the gold and silver that remains. Therefore, the potential increase in new gold supply is very large.

Central banks around the world hold a huge amount of gold. The International Monetary Fund, but also many central banks, particularly European central banks, began to sell their gold when prices were much lower than they are now, around $300 an ounce, roughly a decade ago in quite substantial amounts. Switzerland, Britain, Belgium, Portugal, and a number of other countries started to sell their gold.

The African gold producers complained and persuaded the Europeans to pull back from their gold sales on the grounds that central bank gold sales would depress the price of their newly mined gold from their poor countries. With a perfectly elastic demand for gold because of this new currency, though, that argument goes away. Why would not the central banks just sell their gold to Russia at the new price, essentially swamping Russia's ability to take this gold? How would the other governments of the world respond in terms of their own gold?

Fifth, how would foreigners actually hold this new currency? Assuming Russia succeeded in getting it established, how would they hold it? Most institutions want to hold marketable instruments. We have dollar bills, Euros, and British pounds in our billfold. Where are the marketable instruments? Who would pay interest on this? Now, with a high confidence in the ability of financial markets to innovate, we could say such instruments could be devised and marketed. Maybe institutions would issue such things, maybe not. It is a big question mark.

Finally, if the U.S. dollar were depreciated as much as Jim Rickards expects, U.S. goods would become super competitive in world markets. U.S. asset prices would rise sharply with foreign demand because productive U.S. assets would be really cheap. It is not clear that either of these developments would be devastating to the U.S. economy.

Then, there is a more technical point that is unclear: whether Rickards' scenario would yield a real or only a nominal rise in the value of the gold ruble. What happens to world prices other than Russian oil and gas prices, which by assumption are linked to this? This gets into the general equilibrium effects and is a more technical discussion than we can address here.

My ultimate point is that there are so many important questions with very uncertain outcomes, the scheme cannot be taken seriously. These concerns will surely detour any sensible Russian from actually putting forward the proposal. Therefore, I am very skeptical about this proposal.

Finally, Rickards mentions in passing that the U.S. should, as a preventive move, go back to the gold standard. That is an entirely different subject. If you remember, we actually conducted an official study of that course of action in 1980–82. There was a bill signed by President Carter but concluded under Ronald Reagan. Many people looked at that issue; there were a lot of hearings, papers, and so forth. The general conclusion was that the gold standard in the late 20th Century, and now by inference in the 21st Century, for the U.S. would be a disaster.

I want to say one further comment about the yield curve, which Rickards mentioned in his oil remarks. I agree with Pieter Bottelier that I do not see the Chinese motivation for converting their holdings of U.S. Treasury bills to short-term only, which would increase the yield curve. However, let us suppose they did. Anything they do, we can undo with fiscal and monetary management. Particularly these days, we have, as was mentioned, a large amount of new debt to be floated every month. Decisions have to be made by the Treasury about where to float the new debt, at the short, medium, or long term.

Anything the Chinese do, the U.S. Treasury, with minor adjustments, can undo on the yield curve. If the Treasury does not do it, the Fed could do it now that they are buying bonds again. In my opinion, the technicians in the People's Bank of China would discourage the Chinese from even thinking about it. Why do it if you only create a fuss and some irritation in Washington and accomplish nothing for it?

> *"Jim Rickards' paper has pointed out some possibilities for concealed foreign action, none of which could be devastating to the U.S. but nonetheless would be undesirable. It is very useful to point them out. We should know about them. We should arm ourselves with knowledge of what is happening and what could happen."*

INTERAGENCY COLLABORATION NEEDS

Let me conclude by discussing the interagency implications, which I have already foreshadowed. I think, along with Pieter Bottelier, Jim Rickards' paper has pointed out some possibilities for concealed foreign action, none of which could be devastating to the U.S. but nonetheless would be undesirable. It is very useful to point them out. We should know about them. We should arm ourselves with knowledge of what is happening and what could happen. This involves some classic intelligence, particularly communications intelligence, working with U.S. government agencies and legal authorities that are not used to working with the intelligence community.

In particular, some in the SEC and in the Department of Justice (DoJ) need to be cleared for National Security Agency (NSA) briefings. Some in the Treasury Department already are cleared for NSA intelligence. More importantly, we need to think about the targeting strategies. Who decides how our intelligence assets are targeted? Already, there is some tension when we are using our limited intelligence resources to address national objectives and military objectives. This would add further to already existing tension.

There are priority issues. There is an allocation issue. Having decided the priorities at a senior level, then there is the actual targeting issue: How do you get information on the targets? In terms of the objectives of this symposium, I would put these down as new assignments for the intelligence community with the objects in the first instance being selected sovereign wealth funds and selected state-owned enterprises, because they are the ones who will be the initiators on behalf of their governments. The Treasury, DoJ, Federal Bureau Investigation (FBI), and SEC would be a new set of customers.

This raises not only process questions of priorities and targeting but also issues concerning the ethics of employees in the intelligence community. The Treasury has always been very stingy with financial information within the U.S. government. I know that because I worked in the State Department on several occasions. That stinginess is partly due to unhelpful, unsatisfactory bureaucratic reasons, but it is partly for real reasons (e.g., having prior information about financial transactions can create huge opportunities to make money).

We must have very clear rules and some monitoring to enforce the rules on the employees who are involved in collecting information on actual and potential financial transactions. I do not know what the rules for NSA are on such matters. I do know the rules for the Federal Reserve. Federal Reserve employees are essentially precluded from holding most assets. Anyone collecting intelligence becomes a potential insider in SEC terms. Of course, inside trading in the U.S. is illegal. There are some very practical issues that arise, but these are all soluble.

Finally, I will mention one issue that is not discussed in Rickards' paper but which relates to the previous session: critical materials. With the unexpected invasion of South Korea by North Korea in 1950, materials prices shot up. There were those in Washington who thought—because Stalin was still in charge of the Soviet Union—that this was just the first shot of World War III and we were demobilized.

We were also short of some key materials based on our experience in World War II. Consequently, we built up a huge stockpile. As I recall, there were 109 items in the list of critical materials. It included tungsten, tin, feathers, and industrial diamonds. There was a long list of critical materials that the U.S. government purchased on the assumption that we might need them.

Our interest in those materials receded enormously. We still, of course, have a big stockpile of oil, which was done in a different program. We are not going to fight World War III, which we assume will not occur. It is certainly not going to be on the model of World War II. Therefore, many of these materials are not necessary.

However, a useful interagency activity would be—I do not know what the right timeframe is but maybe once a decade if we have not done it recently, and as far as I am aware we have not—for a group of knowledgeable DoD people, with the aid of other agencies (i.e., U.S. Department of Agriculture (USDA), DoE, etc.), to convene and ask, “In the next five years, what are the really critical materials that could be in jeopardy because of our dependence on foreign suppliers?” I think it would be useful to have a review, at not too frequent but regular intervals, of vulnerabilities relating to critical materials.

REFERENCE

1. Richard N. Cooper, "Global Recession and U.S. National Security," Testimony Before the House Armed Services Committee, 11 March 2009: http://armedservices.house.gov/pdfs/FC031109/Cooper_Testimony031109.pdf.

4.4 PUTTING ECONOMICS BACK AT THE CENTER OF NATIONAL STRATEGY ATTACKS

William Overholt

INTRODUCTION

An imperative for our national security policy, which has become well publicized but I think not fully digested, is getting economics back to the core of national strategy and national security strategy. If you look at our successes and problems as a nation, they revolve very heavily around economics.

Why are we number one in the world? We are number one because of our economy, which started out a couple hundred years ago as every European economist's example of a very poor, primitive, lawless, and divided place but subsequently became the biggest and most advanced economy. One by one, our big competitors—Britain, Germany, and the Soviet Union, fell away.

How did we win the Cold War? We had a strategy that, in Europe, revolved around the Marshall Plan, rebuilding the

Dr. William H. Overholt holds a research position at Harvard's Kennedy School and is Principal of AsiaStat LLC, a consulting firm. Previously, he held the Asia Policy Distinguished Research Chair at RAND's California headquarters and was Director of that Center. Dr. Overholt is the author of six books, including Asia, America, and the Transformation of Geopolitics. He has been a consultant on strategic planning and foreign affairs numerous international corporations, served as a political adviser to several of Asia's major political figures, and conducted consulting projects for the, Korea's National Defense College, the Philippine Ministry of Agragrian Reform, and Thailand's Ministry of Universities. Dr. Overholt received his B.A. from Harvard and his Master of Philosophy and Ph.D. from Yale.

economies and institutional structure of Europe—protected by the military. In Asia, we had the Japanese economic miracle succeeded by the Asian economic miracle—protected by the military. Had we not had the economic and institutional success, all our military power would have been for naught. The military's vital role was to protect the core economic and institutional strategy in order to give it time to work. It did work. Conversely, the Soviet Union had a completely ineffectual, self-defeating economic strategy that eventually led to its total collapse despite a formidable military machine.

THE RISE OF THE PACIFIC BASIN

The core of my professional interest has been the rise of the Pacific Basin. I wrote a paper for the Pentagon in 1972 discussing how it was not so much the Vietnam War or Association of Southeast Asian Nations (ASEAN) or Asia Pacific Network of Science and Technology Centres (ASPAC) or Maphilindo that would save Asia from communism. It was a great economic takeoff, which I alleged—to much ridicule at the time—was in the process of happening. That rise has not only saved Asia from the spread of communism but also has fundamentally altered the way geopolitics works, and we have not yet absorbed that.

I think in the last eight or nine years, we forgot about the central role of economics until our senior military commanders in Iraq, followed by Secretary of Defense Robert M. Gates, reminded us. I think we never absorbed the real lesson of the Pacific Basin, which was an historic shift. Japan was suddenly taken seriously as a major power, virtually without a military, because they learned to grow—for a while—at 10 percent a year. Nobody in history had ever done that. Britain took over half the world when they learned to grow two percent a year. We did better on a little more than that.

When Japan learned to grow 10 percent a year and other countries learned from that, it changed the way the world of rising powers works. In particular, it put economics rather than traditional territorial and military aggrandizement at the core of Asian national strategies. The second rising power in Asia was

South Korea. In the 1950s under President Syngman RheeSouth, Koreans put all their money into the military. They fell farther behind North Korea, which at the time seemed politically more stable, militarily more powerful, and economically more successful. Then, General Park Chung-hee abandoned that failing strategy; he drastically cut the military budget and bet everything on economic development. Today, as a result of Park's economically-focused strategy, the South Korean economy is between 20 and 30 times the size of the North Korean economy. It is clear which strategy won. The point here Is not that military power Is unimportant; to the contrary, it is absolutely essential but it is essential In the role of protecting a strategy founded on the acquisition of economic superiority.

South Korea's success was followed by the rise of Thailand and Indonesia. Indonesia claimed all of Southeast Asia under Sukarno, and it was headed toward becoming a failed state. Then, under Suharto, they gave up virtually all their territorial claims on other countries and focused on economics, and they became the rising power and the leader of ASEAN and Southeast Asia. Thailand's case was less dramatic than Indonesia's, but half a century of rapid economic growth changed Thailand from a hapless, backward country radically inferior to Vietnam into the deputy leader of ASEAN, far more respected than Vietnam. Subsequently, Vietnam has moved to an economics-focused strategy and is rapidly increasing its regional stature.

In the late 1970s China, under Deng Xiaoping, looked around and asked, "How come everybody else is doing so much better than we are?" Shortly thereafter, they simply copied the South Korean strategy: They radically reduced the military's share of the economy—from around 16 percent to around three percent. They gave up most of their territorial claims. They settled 12 of their 14 boundary disputes to the satisfaction of the other parties. They gave up trying to change other countries' politics, instead focusing everything on economics.

As a result of all this, every country in Northeast and Southeast Asia understood that the world had changed. Once you could grow seven–nine percent consistently, you could become a big power very quickly, but only if you put your resources into economic development at considerable expense to any territorial and military ambitions you might have for the time being. I do not think we have digested that. Most of the time our scholars and strategists are still looking at Bismarck's Germany and 1930s Japan.

We have also been slow to digest the collapse of Japan as a partner and as a leader of Asia as they have mismanaged their economy from the 1980s onward. The 2000 Armitage Report claimed that we were focusing too much attention on China and that we needed to revert to a posture of making Japan the sun and the moon of our policy in Asia.

Following that recommendation of reversion to Cold War priorities, we replaced the key assistant secretaries and the Asia Director at the National Security Council (NSC) and so on, many of whom were China experts, with Japan specialists. Subsequently, we found ourselves dealing with North Korea. We sat down with the Chinese and came up with the least bad strategy and pursued it over the opposition of Japan. Likewise, for a wide variety of other key Asian issues—the war on terrorism, regional crime, regional drugs, regional free trade, regional freedom of investment, and agricultural free trade we found that China was our principal partner. Take genetically modified crops, a key U.S. agricultural interest. We are number one in the world in genetically modified crops; China is number two. The adversaries were Japan, India, and Europe, who just want to keep genetically modified seeds out of their countries. The economics determines who is going to be important, who is going to be our partner, and who can get things done. China's success and economic priorities make it a stabilizing factor and a crucial partner. Japan's economic decline entails diplomatic decline. While many of our respected strategists are yearning for a return to Cold War verities, including a focus on Japan, and, based on obsolete models, obsessing about the risks of the rise of China, they are missing the great dilemmas created for us by the inexorable decline of Japan. They are missing the opportunities, including forward movement on Taiwan, stabilization of the Korean Peninsula, addressing global warming, and joint efforts to recover from the global financial crisis, that can arise from embracing partnership with China.

A crucial example is the war on terrorism. If we are going to contain Islamic fundamentalist terrorism, the key is to spur the development of Africa. In 1965, Islamic terrorism and fundamentalism concentrated in Indonesia, which had more Islamic fundamentalists, political figures, and movements than the rest of the world combined. It has simply faded since Indonesia's economy started developing rapidly. Notice that some of the Islamic fundamentalism revived after the 1998 crisis but has since been contained. The key to containing the global Islamic terrorism problem is to achieve in sub-Saharan Africa what we achieved long ago in Indonesia.

Until recently sub-Saharan Africa was experiencing negligible or negative per capita economic growth. The extraordinary suffering entailed by that bleak economic trend made the continent the perfect breeding ground for a spread of Islamic and other forms of fundamentalist violence that could have been expected to dwarf the terrorism problem that we face today. But in the last few years a remarkable turnaround has occurred. Prior to the current, hopefully transient, global economic crisis, sub-Saharan African economic growth rose to around six percent. For the first time polls showed a majority of people in these countries saying that their lives would be better in the future than now and that their children's lives would be better than their own. What has made the difference between Africa having negative rates of growth and six percent until this crisis set in? Chinese demand.

"If we are going to contain Islamic fundamentalist terrorism, the key is to spur the development of Africa."

That African growth and the associated change of people's expectations is the key to our success at what President George W. Bush thought was the core national strategic issue. The positive Chinese economic relationship to Africa is key to our prospects for success in stabilizing the continent. However, if you look at our national security literature about China in Africa you see nothing but disparagement and fear. Much of that literature treats China as if it were the old Soviet Union, seeking to change African politics and to acquire African military bases. But China is not seeking to rebuild African polities in its own image, and as a matter of principle it abstains from seeking military bases. We rarely see the real connection between Chinese involvement in Africa and our national interests because we do not see the economics.

We have a long way to go in getting economics back to the core. As we do that, I think there are some risks that we do not face. Contrary to a paper that has been prepared for this conference, our macro economy cannot be successfully attacked and manipulated from abroad. You cannot collapse the U.S. currency and manipulate the stock market by an initiative from abroad. You cannot lever up small investments into something that will have a huge macro effect on the U.S. economy.

You can bring the U.S. economy down if we collapse into protectionism. You can destroy the U.S. currency if we debase it. You can wreck our financial markets if we encourage excess liquidity and lack of regulation. These things cannot be manipulated from abroad. The markets are too big and too deep. Of course, there are real economic risks: classic industrial espionage, water and food contamination, cyber attacks, and power grid disabling that previous speakers have talked about.

"I think cyber warfare is the 21st Century equivalent of nuclear war."

I would underline what was said about cyber warfare. I think cyber warfare is the 21st Century equivalent of nuclear war. We need a macro strategic debate similar to what we had about nuclear war, for instance considering options like massive retaliation, tit for tat, and so forth. We need the cyber-equivalent of Herman Kahn's book, On Thermonuclear War, as an overarching guide to how we handled all these individual tactical issues being addressed at this symposium.

Supply chain security is a big issue. Wal-Mart and a Hong Kong company called Li & Fung are the best people who know how to manage supply chain security. We have a great deal to learn from them. We also need to learn how resilient supply chains actually are from history in general. In the Korean War, we needed tungsten for our tanks. We had an embargo on trade with China. China had the tungsten. China needed money. Somehow, the tungsten got out of China into the hands of Union Carbide. The Chinese made the money they needed, and we got the tungsten we needed to make tanks to shoot Chinese in Korea. The resilience of these supply chains is remarkable. We need to Improve our understanding of both their resilience and their vulnerability.

RESOURCE VULNERABILITY

I would like to separate two things. One is the vulnerability of our logistics in a war, which Captain Jan van Tol talked about in Roundtable 2.

The other is war over resources. I think the first is very important. Everything Captain van Tol said was extremely important. Given the shortness of time, let me just make some flat assertions about the second, potential war over resources: First, the range of resources over which serious powers fight is drastically reduced in the modern world. Serious powers used to go to war over cobalt and copper and almost anything. They do not anymore. Basically, oil is the only issue. The world is not running out of resources, Malthusian theory to the contrary. It became popular in the early 1970s to discuss the depletion of resources. I used to visit the War College and debate the people from the Club of Rome, a global think tank that had published a report in 1972, The Limits to Growth. It was an entertaining intellectual exercise, but the World3 model the Club of Rome presented, simulating the limits to growth, was flawed. The flawed assumptions of that report, that we are running out resources, that economic progress inexorably depletes resources and worsens pollution, have been thoroughly refuted time after time, but they keep reviving both in economic literature and now in the national security literature.

Every decade for well over a century we have heard forecasts that we are running out of oil. We are not running out of oil. We have a problem that cheap, convenient oil is located in one unstable part of the world. At something well short of $100 a barrel, tar sands, oil shale—all kinds of energy—just flood the world with energy. The problem recently has been that the big oil companies have refused to invest on the basis of anything more than $40 a barrel of oil because they knew the price would collapse, and they know there are so many other kinds of energy available.

"The range of resources over which serious powers fight is drastically reduced in the modern world."

The frequency of resource conflicts over which serious powers go to war, I would argue, has decreased drastically. The kinds of conflict that we allow countries, including ourselves, to engage in over resources have narrowed. A century ago, the Belgians could slaughter huge numbers of people over resources in the Congo. We fought over things like copper and cobalt. In 1980–85, I was involved in some rather rough operations to secure Angolan oil and chrome from Zimbabwe. We do not do those things anymore; it is socially unacceptable.

The Chinese do not even think about sending a platoon to guard one of their oil operations in Africa. They will be careful. They will reluctantly, under international pressure, send a group of military engineers to Sudan to try to keep the peace in certain areas. They do not even think about the possibility of sending a platoon when it could be very useful in protecting their business interests. It is just not in the culture; it is not acceptable. More broadly, resource conflicts are not becoming more prominent. We have drastically reduced the range of resource issues for which we conceptualize military recourse as an option, and the Chinese hardly ever conceptualize resource security strategy in military terms. (Some territorial waters and seabed issues are an exception to this rule.)

THE RISKS OF BEING OVER-DEFENSIVE

Although we need to worry more about economics, we are at serious risk of overreaction in a number of areas, such as export controls. Some are necessary; we obviously need to stop small nuclear bombs from being exported to North Korea. However, many export controls damage U.S. competitiveness and subsidize the threat we are trying to avert.

Let me just give you an example and follow it through. In 1985, I moved to Hong Kong. In New York, I had an IBM XT computer, first generation. I wrote to IBM and asked, "Can I use this with Hong Kong 50 cycle, 220 current?" They said, "Yes, but it will cost you much more than the value of the computer to get your export license from DoD and Commerce. Throw it away and buy a new one."

So I went to Hong Kong. The market was flooded with knock-off AT computers from China, ten times better than what I was banned from taking with me from New York. Virtually every American, and there were a lot, and many others moving to China, dumped their IBMs, and bought Chinese knock-off models. We created a huge subsidy for Chinese companies to make computers through our export controls. Lenovo, the most successful of those Chinese companies that we were subsidizing through our export controls, later bought IBM Think. There was then a nationalist reaction here not to allow the Chinese company to take over IBM Think on national security grounds. However, there were no national security grounds. Most of these things are made in China anyway. If we had stopped Lenovo's purchase, IBM would have been stuck with a money-losing division and unable to move up into the incredibly successful services business they are in today. As long as they had that Think division, they were linked to Microsoft and could not go into competition with it.

To take another example we ban the export to China of U.S. companies' software that was produced for them by researchers in China. Think about that: Our big companies cannot export to

China software that was developed for them in China. Therefore, the Europeans and the Japanese just go in and take the whole market.

I keynoted one conference where the key people who enforce the export control from around the country were prominent. Afterwards, one of the most senior attendees came up to me and said, “I have got to enforce these laws. As long as I am here, I am going to enforce them. As soon as I have my full pension, I am going to spend the rest of my life trying to change the policies that I can see are damaging our country so much.”

“We do not understand our own strength or our own resilience . . .”

We need laws about foreign takeovers and we need some export controls, but we should be very careful about going too far. One of the greatest contributions of some unit of the government would be to pay some objective academics or think tank to create a model that shows us when we are actually achieving our goals with export and investment controls and when we are shooting ourselves in the foot. We are shooting ourselves in the foot terribly by having scared the Chinese off from investing in financial firms and major firms. Citibank was rescued in the previous financial crisis by a Saudi investor. We benefited from that. This time around, it could be rescued by a Chinese investor, but it will not be because we panicked and scared them off. We do not understand our own strength or our own resilience, so we are afraid of things that we do not need to be afraid of.

CONCLUSION

We need to put economics at the core of our strategic thinking. Doing that will transform our perspective on everything from the risks posed by rising powers to the value of traditional alliances to the effects on our interests of Chinese involvement in Africa. It will change the way we allocate our national security resources. It will make us more sensitive to the risks of mismanaging our own economy. At the same time, when we consider defensive actions to protect our economy we need to understand our own economic strength and have confidence in it.

4.5 QUESTIONS AND ANSWERS HIGHLIGHTS

Transcripts

Q: As we understand it, approximately 50 countries have implemented varying degrees of protectionism since the economic crisis began. Two questions: What impact do such measures have on the economic recovery? Do these protectionist measures enable or lessen the potential for economic and financial attacks? Anyone want to take a crack at the protectionist issue?

Richard Cooper – Bill Overholt mentioned protectionism in his remarks as carrying an extremely dangerous potential, and I share that view entirely. If you want a historical analogy, it is 1930, and the Smoot-Hawley Tariff Act passed by the U.S. (actually Australia moved before the U.S. did) was then and is today a much bigger country. One thousand and fourteen economists sent a letter to President Hoover urging him to veto this piece of legislation. He rejected that advice. I believe the single biggest mistake, outside of war, any President ever made was when President Hoover signed the Smoot-Hawley Tariff Act.

Almost immediately—not immediately but after a lag—a number of countries retaliated against the U.S., and Britain, which had been the free trade bastion since the 1860s, moved to imperial free trade. They imposed first temporary and then permanent duties on all nine goods originating outside the British Empire. Then, for the rest of the 1930s, international trade just seized up. I like to think we are much wiser today than the folks in the 1930s. However, I do agree with Jim Rickards that once you get into the framework—the negative sum game—then you want to minimize the damage. It is too late to have gains, but you can minimize the damage in each country.

I think this is a serious risk. I hope that if nothing else comes out of the April 2nd meeting, it is an effective pledge by the G20 to avoid protectionist actions. The list of 50 countries that have implemented protectionist measures, of course, includes a number of actually trivial actions. It needs to be said: I do not know if anyone has done a statistical analysis. In any interval of time, like four months, in the world, there are always some protectionist actions. One cannot attribute them wholly to the situation, but it absolutely would be a disaster if it got out of hand.

Q: *Each participant has discussed China and Russia, but alternatively as a help or hindrance to U.S. economic interests. When participants or observers discuss China or Russia, is there an assumption these governments are monolithic? If not, how does that complicate the challenge of discerning their intent?*

William Overholt – Are China and Russia monolithic? It depends on what you are looking at. The useful thing is that like our government, the Chinese government can decide. It usually is pretty clear about what it has decided. The reigning assumption for heuristic purposes and our discussion is that there are always covert things going on. If there is a government other than ours that is very clear in saying what its policies are and following through with them, it is China. The Europeans and the Japanese cannot make decisions, but the Chinese can.

Therefore, in dealing with this crisis, there are really two big economies in the world that make decisions and move things forward: the U.S. and the Chinese. It means secondly though that, like our economy, theirs is mostly a market. When the crisis started, Chinese exports collapsed, but their imports collapsed more. Their trade surplus actually went up initially because they were using up inventories. Some of the journalists said, "Oh, look: the Chinese are manipulating the economy to increase their trade surplus." They cannot do that; it is too complicated. There are tens of thousands of companies that make decisions about exports and imports. The government cannot just decide what will happen. Certainly, there are parts of the Chinese government that can do things covertly. I think that is not a function of the diversification.

I think the more centralized they are, the more they can do things covertly.

The other thing about China is that there still are substantial pieces of China that can do things without the central government being in control of them or even knowing what they are doing. Remember 15 or 20 years ago, we had this big problem with compact discs (CDs) that were being pirated by senior generals along the coast in cooperation with Taiwanese and Hong Kong businessmen. The central government had a great deal of trouble reining them in because these generals were very powerful figures. At the end of the 1990s, they finally decided to tell the military they had to get out of the business. They did that in two years.

There is still some freelancing. When I was in Hong Kong, we had a problem of the luxury cars disappearing. The People's Liberation Army (PLA) first was just trucking them out of Hong Kong—the Mercedes Benzes, the high-end Toyotas, and BMWs. (They did not like Jaguars for some reason.) The Hong Kong government started x-raying all the trucks. Then, the Chinese Navy essentially built cigarette boats that would go 80 km an hour. The cockpit was shaped like a Mercedes. They would run them out at night. The Hong Kong government strung wires at night, which do terrible things to a high-speed cigarette boat. Then the Army taught all the fishermen along the coast . . . they gave them what I call a condom for a Mercedes. You back the Mercedes into this rubber thing and essentially tighten, pull it behind a fishing boat, and float just below the surface. You had a lot of millionaire fishermen.

These huge cranes that move containers at the port—and it is the biggest port in the world—all started disappearing. Nobody could figure out where they were going. Finally, over the objections of the British, the Hong Kong police got in touch with the Guangdong police and found that the Chinese Army had a construction site. They found these cranes useful for construction. They were stealing them. The Guangdong police surrounded the Army camp and made them give back the cranes.

This kind of thing makes it a little hard sometimes to figure out what is actually going on, especially including some of the military folks in China. The good news is each year they get a little more under control than they were the year before.

Jim Rickards – I agree that intentions are hard to discern, but one of my points is: are we even trying? There are some very rich analytical tools that we can apply to global capital markets that hedge funds and other analysts use all the time that the national security community is unfamiliar with. Why should they be? It is not their area of expertise.

In discussing the paper, both Richard Cooper and Pieter Bottelier made the point that they found some of the scenarios intriguing and interesting but low probability events. I actually agree that they are low probability events. They are potentially very high consequence, though. Before 1941, Pearl Harbor was a low probability event. My point is what are we even doing on the counterintelligence side, the analytical side, or the interagency cooperation side? We are going to talk more about interagency tomorrow, but I think there are a whole host of relatively low-cost, very powerful tools that we could bring to bear to detect and find indications and warnings in capital market pricing. Again, it is a separate source. If you subscribe to a financial analysis service like the Bloomberg Professional service and know how to use it, you can find out a lot about what people are doing behind the scenes.

Chapter 5

ROUNDTABLE 4

Responding to Nuclear Terrorism

5.1 MODERATOR'S SUMMARY

Todd Masse

DEFINING THE THREAT

In any discussion of nuclear terrorism, one of the best places to begin is with definitions—because there are varying definitions, not only of nuclear terrorism, but also of weapons of mass destruction. There are at least four different faces of nuclear terrorism:

- A radiological dispersion device
- A radiological release (e.g., domestic or international a terrorist group attacking a civilian nuclear power plant and releasing radiation)
- Terrorist acquisition of an intact nuclear weapon
- Terrorist acquisition of fissile material [e.g., highly enriched uranium (HEU) or plutonium]

There are also varying definitions of weapons of mass destruction, as many attending this symposium know well. The traditional definition is chemical, biological, radiological, nuclear,

Mr. Todd M. Masse is a Senior National Security Analyst with the Strategic Assessments Group of The Johns Hopkins University Applied Physics Laboratory, a non-profit University Affiliated Research Center. Mr. Masse is responsible for conducting strategic research and analysis on threats to U.S. national security. Mr. Masse has extensive experience in intelligence and homeland security matters and was formerly employed in the U.S. Intelligence Community and by the Congressional Research Service. Mr. Masse holds degrees from the University of Massachusetts (Lowell, Massachusetts), the American University (Washington, DC), and the University of Maryland (College Park, Maryland).

and explosive (CBRNE) weapons. However, when we are talking about nuclear terrorism—the terrorism that by and large is etched not only in the psyche of the populace but also in the media—it is a nuclear fission device, which has blast, heat, electromagnetic pulse, and radiation effects.

As we all know, these types of weapons are in a category by themselves due to their physical destructiveness but also their psychological impact. There are basically two different types of nuclear weapons: the gun and the implosion type device. The gun is the relatively less sophisticated of those two types of designs. There is a general consensus that any type of terrorist-improvised nuclear device would be a gun-type device using HEU.

When you look at the scale of the threat (Figure 1), you see the likelihood of the occurrence along the x-axis and the potential impact on the y-axis. What we are really talking about with nuclear terrorism is in the upper left quadrant: the nuclear weapon itself—the fission device. The source of this is the Federal Bureau of Investigation's (FBI's) Weapons of Mass Destruction Directorate (WMDD), and we have the director of WMDD on our panel: Dr. Vahid Majidi, whose analysts are doing good work.

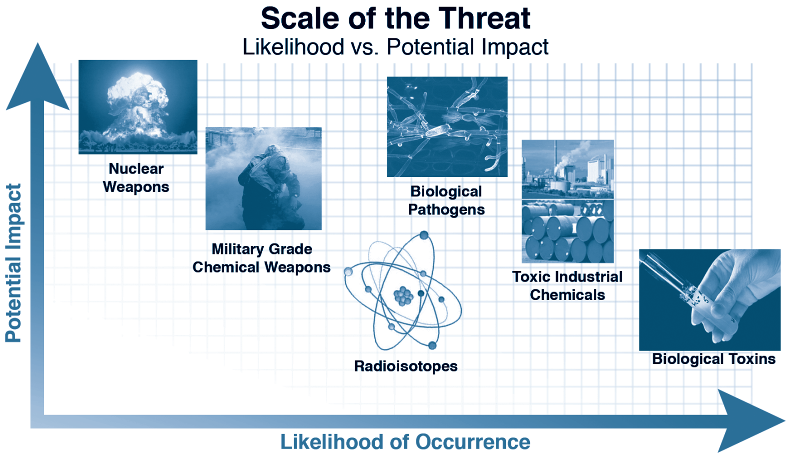


Figure 1 Scale of the Threat

Primary Components of the Threat

What are the three primary components of the nuclear terror[ism] threat? Note that I have "terror" bracketed from "terrorism." Nuclear terror is something that can be self-imposed, something that we inflict upon ourselves based on al Qaeda propaganda that they essentially are now a nuclear power. Nuclear terrorism is the act of nuclear attack, the actual detonation of an improvised nuclear device. The three primary components of the nuclear terrorism threat are supply, demand, and path.

> *"Nuclear terror is something that can be self-imposed, something that we inflict upon ourselves based on al Qaeda propaganda that they essentially are now a nuclear power. Nuclear terrorism is the act of a nuclear attack, the actual detonation of an improvised nuclear device."*

Supply

There are tons of fissile material out there. The international panel on fissile material estimates that anywhere from 1400 to 2000 metric tons of HEU are in circulation for civilian HEU uses in research reactors and approximately 500 metric tons of separated plutonium for military uses. There is an inordinate amount of material out there. We know through the Nunn-Lugar process, which coordinates nuclear reduction efforts going back at least to 1991, that a substantial amount of highly enriched plutonium in the former Soviet Union has been locked down or secured, but there are substantial vulnerabilities remaining today.

Much of the vulnerability has to do with civilian use of HEU, particularly research reactors. Currently, there are approximately 130 research reactors in over 40 countries around the world that have enough HEU to make more than one nuclear weapon, and the status of the security at these facilities is far different from what you would expect at a military facility.

Dr. Graham Allison at Harvard University's John F. Kennedy School of Government, a thought leader in the analysis of nuclear terrorism, has said: “No loose nukes, no nascent nukes, no nuclear terrorism.” If there are no loose nuclear weapons—and fissile material as well—and no nascent nukes (i.e., no new nuclear nation states), there will be no nuclear terrorism. Although I think it is a compelling statement and a truism, as we learned from the discussion of cyber security yesterday, there are very few perfect security regimes out there; it is perhaps unrealistic to think that we are going to have a perfect security regime with respect to all of this material.

There are thoughts that we should have some type of a Fort Knox or a Gold Standard for fissile material. The problem with that analogy is that gold is far different from HEU because HEU is engaged in commerce to a far greater extent than gold is.

Figure 2 is from a project I am managing in collaboration with Harvard University; it shows where the material is and how much is out there. HEU and plutonium—the essential ingredients of nuclear weapons—exist in dozens of countries, with security that ranges from excellent to appalling. Programs sponsored by the Energy and Defense departments help remove such materials to secure locations and assist other nations in improving security at facilities that hold nuclear materials. The map pictured in Figure 2 charts progress that was made in fiscal year (FY) 2006.

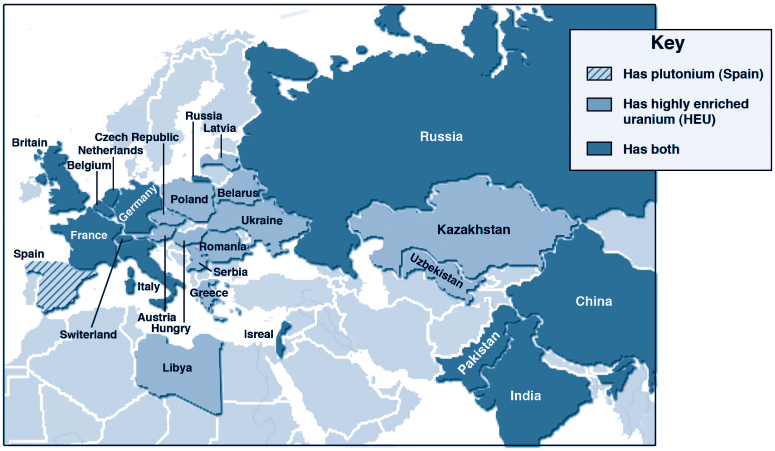


Figure 2 Location of Fissile Material

The dark shading indicates areas that have both plutonium and HEU, and the lighter shading shows areas with HEU alone. The points of highest vulnerability are in some of the research reactors in the U.S. The U.S. government, admittedly, has converted some of these research reactors over time from the use of HEU as a fuel to the use of low enriched uranium. However, many of these facilities, particularly in Russia, are using HEU. Countries that have sufficient quantities require the highest levels of security, based on International Atomic Energy Agency (IAEA) recommendations.

Demand

The second component is demand; terrorist groups have directly expressed desires to use these materials, creating demand. Of course, as Bruce Hoffman mentioned, we should consider al Qaeda as our number one threat and, more specifically, core al Qaeda or central al Qaeda, this being a relatively sophisticated operation, but also terrorist groups such as Aum Shinrikyo in Japan and Chechen terrorist groups in the former Soviet Union (FSU). Of the 33 groups on the State Department's foreign terrorist organization list, many of them have expressed an interest in weapons of mass destruction.

Path

What is the path that a terrorist would follow to a nuclear weapon or fissile material? State sponsorship is first on the list. A rogue state could provide nuclear materials or weapons as a gift, essentially. Pick your favorite bad-guy nuclear weapon country—many like to focus on North Korea—which could provide a gift of an intact nuclear weapon or fissile material to a terrorist organization. A second path could be theft of fissile material or a weapon. Third, and perhaps most likely, is leakage—inadvertent or otherwise—of fissile material or black market purchase by a terrorist group.

Probabilities

When you talk about the probability of an attack—you hear this almost every day or every time a new blue ribbon panel is established—there is a better than 50 percent chance in the next 10 years that this is going to happen in the U.S., or it is 0.27 or 0.56. The problem with that is, no one really knows. It can be a stochastic guessing game in the absence of an accurate, capabilities-based foundation. When we talk about capabilities, it is a question of how well we, the U.S. national security intelligence community, know the capabilities of al Qaeda—or pick any other group in terms of their ability to build a nuclear weapon. The problem with these stochastic models is that they contain many subjective assumptions that can be misleading; the coefficients on these variables can change based on many different aspects of the problem.

"No loose nukes, no nascent nukes, no nuclear terrorism." — Dr. Graham Allison, Harvard University's John F. Kennedy School of Government

The most important question, of course, is whether the risk is increasing or decreasing? As Jim Rickards mentioned yesterday and Professor Hoffman alluded to today, we are in a global recession right now of which we are all painfully aware. Might this be an opportune time for al Qaeda—who has expressed an interest in taking the U.S. to its knees perhaps over a period of time, from an economic perspective—to strike us?

Existential Threat?

I think nuclear terrorism is a serious threat, yet it is not necessarily existential. I do not mean to downplay how catastrophic a nuclear weapon exploding in a major metropolitan area in the U.S. would be. The casualties, the deaths, would be dependent on many factors, not the least of which would be yields, time, the type of nuclear weapon, where it went off, prevailing weather patterns, etc. You would essentially have tens if not hundreds of thousands dead. However, does that necessarily mean that the U.S. would capitulate and fall to its knees? I do not believe so.

Key variables, though, when you are assessing that question is how the populace and the U.S. political leadership would react—or overreact—to such an attack. I think the farther we go down the overreaction road—the more you have a populace cowering in fear, the more you have political leadership that may take rash military actions quickly—the closer you move to that existential threat.

Capability: Can Terrorists Build a Nuclear Weapon?

The billion-dollar—or with inflation, the trillion-dollar—question is, can terrorists build a nuclear weapon? When you look at terrorism threat assessments—and nuclear terrorism threat assessments more narrowly—traditionally you are looking at three factors: opportunity, capability, and intent. Capability can be very difficult to assess.

As Professor Hoffman pointed out very well in his address, "Terrorism from IEDs to WMDs" (Chapter 1), when assessing capability, you are aiming at a moving target; even with al Qaeda, you do not have one al Qaeda, but many different levels of al Qaeda, so it is difficult to assess capability with any high level of accuracy. What you end up with is vulnerability-based analysis or a tendency to look at what is plausible or possible, and that takes on greater importance.

When we look at some of the al Qaeda safe-haven documents that were found in Afghanistan, the super bomb documents that were analyzed by David Albright and others, one of the things they found is that al Qaeda, at that point, had very poor nuclear knowledge. The problem with that is that knowledge is not static, and we know that they are continuing to do research and analysis on this, continuing to try to recruit those individuals who can help them reach their goals.

When we examine networks such as that led by Dr. Abdul Quadeer Khan, Director of Pakistan's Khan Research Laboratories, and efforts to procure nuclear materials or weapons, we know that essentially what we encounter is a nuclear whack-a-mole game: In the case of the activities of Dr. A. Q. Khan, and some of the individuals that were involved in these far-fetched procurement and sales efforts to provide information and nuclear-weapons components to Libya, Iran, and North Korea, some were arrested;

many of them were not. If they were arrested, as was Dr. Khan, they were put under house arrest. These individuals show up continually. They surface in other areas and live to play another game. Dr. A. Q. Khan himself—the father of the Pakistani nuclear weapon—was recently released from house arrest in Pakistan; if you think we have heard the last of Dr. A. Q. Khan, I have some collateralized debt obligations I would like to sell you.

Countries arguably are just as dangerous from a nuclear proliferation perspective. However, as far as we are aware, no country has ever knowingly transferred fissile material or a nuclear device intact to a nonstate actor.

Historically, groups that have tried to develop nuclear weapons include Aum Shinrikyo, a group that had a net worth of a billion dollars and had recruited many of the top scientists and engineers from various Japanese schools. The Czechian groups in the FSU had access to the Russian mafia and others. Both were well resourced, both well connected, but unable to develop nuclear weapons.

EXPERT CONSENSUS?

Is there an expert consensus on terrorists' capability to build nuclear weapons? Not necessarily. The following two quotes portray dueling physicists: a Nobel Laureate physicist, Dr. Luis Alvarez, and Dr. Stephen Younger, former Director of Los Alamos Nuclear Laboratory (LANL) Research and Development and former Director of the Defense Threat Reduction Agency (DTRA).

> *"With modern, weapons-grade uranium, the background neutron rate is so low that terrorists, if they had such material, would have a good chance of setting off a high-yield explosion simply by dropping one half of the material onto the other half. Most people seem unaware that if separated U235 is at hand, it's a trivial job to set off a nuclear explosion, whereas if only plutonium is available, making it explode is the most difficult technical job I know . . . Given a supply of U235, however, even a high school kid could make a bomb in short order."*
>
> *— Nobel Laureate Physicist Dr. Luis W. Alvarez*

> *"It would be wrong to assume that nuclear weapons are now easy to make, that once the secret was out anyone could read the instruction book and make one with materials found around the house. I am constantly amazed when self-declared 'nuclear weapons experts,' many of whom have never seen a real nuclear weapon, hold forth on how easy it is to make a functioning nuclear explosive."*
>
> *— Dr. Stephen M. Younger, Formal Director LANL Nuclear R&D, former head of DTRA*

Dr. Alvarez says that if terrorists had such material—and he is talking about weapons grade, which is material with isotopic composition better than 85 percent U235—they would have a good chance of setting off a high-yield explosion simply by dropping one half of the material onto the other half. Even a high school kid can make a bomb in short order.

At the other end of the spectrum, Dr. Younger says, "I am constantly amazed when self-declared nuclear weapons experts, many of whom have never seen a real nuclear weapon, hold forth on how easy it is to make a functioning nuclear explosive." The core of the difference here is implicit versus explicit knowledge. You can search the Internet and get plans for how to do this, but the important element of this is the implicit knowledge—finding someone who has actually done this for a living—and that is the group of individuals and scientists that al Qaeda is trying to recruit.

CAN TERRORISTS BE DEFERRED?

In the traditional sense—by punishment? Not necessarily. This is the issue of not having a return address. If a missile comes over the transom, we know what the return address is on that; we know whom to attack. However, when an improvised nuclear device comes in a cargo hold on a private jet or sails up the Potomac on a private yacht, we do not necessarily know where that came from.

Deterrence by denial, on the other hand, may be able to deny terrorists their goals; e.g., if al Qaeda wants to take us to our knees economically, one of the deterrence measures you can consider is societal resiliency that Dr. Flynn discussed in his address, "Resiliency in the Face of Unrestricted Warfare Attacks" (Chapter 1)—if we can prove to the terrorists that a nuclear weapon going off in this country is not going to take us to our knees from an economic perspective, we might give them some pause.

Another deterrence measure that we can engender with our policies and actions is to increase the terrorists' perception of potential failure. If they become convinced their efforts will fail here—and they do not want to fail, particularly in a complex initiative like a nuclear attack because they would view that as a failure in the eyes of God, which they want to avoid at all costs—we may be able to deter them.

Self-restraint or self-deterrence is another aspect that may be working to mitigate the threat. Many recantation books have been written by terrorist operatives, some of whom were affiliated with al Qaeda. Admittedly, some of these books were written while these operatives were in Egyptian jails, but nevertheless they question the indiscriminate use of discriminate force, and it has catalyzed a substantial debate the Jihadist enterprise over the use of nuclear weapons. The outcome of that debate we do not know, but it is a factor at work.

Expanded deterrence is another way to prevent nuclear terrorism; i.e., prevent the bad-guy nuclear countries (e.g., North Korea, Pakistan, and others) from providing fissile material or a nuclear weapon to a group. Critically important to that effort are nuclear forensics and attribution. That is, if we want to prevent North Korea from selling fissile material and nuclear weapons to a terrorist group, we have to convince them that we, the international community, the IAEA, and the U.S. have databases that can identify either their fissile material or their debris in the aftermath of an explosion and be able to attribute that to North Korea and perhaps even track it back to the reactor from which the fissile material came. That type of attribution ability—and importantly the perception on the part of the North Korean leadership that the international community has that ability—may cause them some pause because they may believe that they will be retaliated against significantly.

Finally, the doctrine of negligence is essentially the argument that we should have a declaratory policy that if any nation state that has nuclear weapons or fissile material is negligent in their protection of that material, they will be held accountable. "Held accountable" does not necessarily mean in a military sense; it could also mean in terms of financial reparations. By and large, it has military repercussions. The problem with this is credibility and the issue of allies. It may be credible to threaten North Korea with massive retaliation, but it is not necessarily credible with respect to Russia.

STRATEGY TO COMBAT NUCLEAR TERRORISM

We have a multilayered system of systems with independent layers (Figure 3). As you go out from the core, it becomes increasingly dangerous. The core, the first layer, is really protection of that fissile material at its weapon source—i.e., nonproliferation. Here we are talking about the nonproliferation treaty, the Nunn-Lugar cooperative reduction efforts, the global threat reduction initiative, and the global initiative to combat nuclear terrorism. There are many well-founded programs at this level, as there should be.

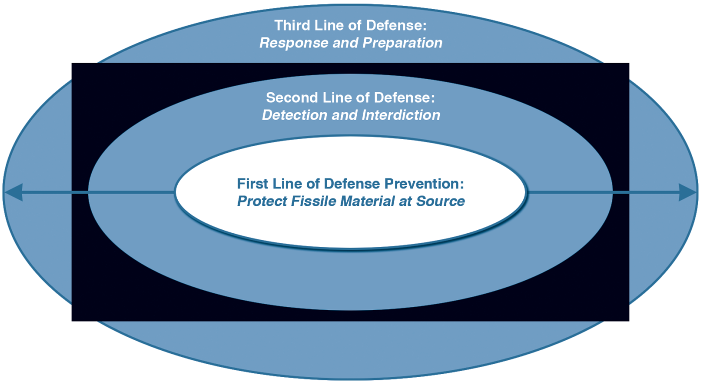

Third Line of Defense:
Response and Preparation
Second Line of Defense:
Detection and Interdiction
First Line of Defense Prevention:
Protect Fissile Material at Source

Figure 3 Multilayered System of Systems

The second layer is the detection and interdiction of fissile material or a nuclear weapon in transit. This is the "horse is out of the barn" scenario, and we have initiated work in this area.

The third layer, response and preparation, is the preparedness to defeat nuclear terrorism by responding to a nuclear device being detonated in the U.S.

"I think nuclear terrorism is a serious threat, yet it is not necessarily existential. I do not mean to downplay how catastrophic a nuclear weapon exploding in a major metropolitan area in the U.S. would be . . . However, does that necessarily mean that the U.S. would capitulate and fall to its knees? I do not believe so."

The interagency challenges associated with implementation constitute the core of the issues presented at this symposium. We have numerous agencies, dozens of programs, nuclear security programs on the one hand, counterterrorism programs on the other, but who is integrating all this? What are the mechanisms for integration?

Today, we are fortunate enough to have several panelists that can answer all of these questions, and speak more specifically to their areas of expertise: Mr. Brian Jenkins from RAND will discuss the components behind a nuclear terrorism; Dr. J. Scott Cameron from the National Counterterrorism Center will share his thoughts on the mechanisms for integration; Dr. Jonathan Medalia from the Congressional Research Service, will discuss detection technologies; and Admiral Harvey E. Johnson, former Deputy Administrator with the Federal Emergency Management Agency (FEMA), will speak to the concept of response.

5.2 THE IMPACT OF CATACLYSMIC EVENTS

Brian Jenkins

INTRODUCTION

To help remember my major points in simple terms, I reduced them to a mnemonic: $C^2I(T/2)$. The C in this equation represents a cataclysmic event, I is for intelligence, and T divided by two stands for terrorism and terror.

Cataclysmic Events

Why is it so difficult to assess the threat of nuclear terrorism? Because there is no precedent for this in the realm of terrorism, our knowledge of nuclear weapons comes from our experience with their use at the end of World War II—we certainly know the consequences. Todd Masse was correct in saying that a nuclear fission device is in a category all by itself. We talk about terrorist use of weapons of mass destruction, but the 2001 anthrax attack in the U.S. killed only five people—fortunately—and the 1995 sarin gas attack in Tokyo killed only 12 people, although it sent

Mr. Brian Michael Jenkins is a Senior Advisor to the President of the RAND Corporation and Director of the National Transportation Security Center of the Mineta Transportation Institute. Mr. Jenkins is one of the world's leading authorities on terrorism and transportation security, and he has served as Captain of U.S. Army Special Forces in the Dominican Republic and Vietnam. He also served as a member of the White House Commission on Aviation Safety and Security and as an adviser to numerous government agencies. His publications include Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves; Three Years After: Next Steps in the War on Terror; and Countering al Qaeda: An Appreciation of the Situation and Suggestions for Strategy.

thousands to the hospital. It is really hard to fathom even a small nuclear explosion. A nuclear explosion is cataclysmic. Even a relatively modest explosion would be an event 10 times worse—perhaps a 100 times worse—than the 9/11 attacks.

In the equation here, C is squared because it is a cataclysmic event that we think about in the shadow of another cataclysmic event. The events of 9/11 fundamentally altered our perceptions. Nuclear terrorism is not a new idea or a new threat; it has been a concern for a long time. However, certainly in the wake of 9/11, it had a tremendous impact on our calculations as well as on how we conduct threat analysis.

> *"From our knowledge of nuclear weapons—from our experience with their use at the end of World War II—we certainly know the consequences."*

Intelligence

In the equation, I stands for Intelligence, but it could just as easily as "insofar as we know." That phrase is often repeated in the discussion of nuclear threats. We are dealing with an inherently difficult assessment problem—it is always extremely difficult to assess that kind of a threat. We are dealing with a statistically rare, uprecedented event with enormous consequences, and we are still dealing with concerns about inadequate intelligence.

The events of 9/11 are considered to be the result of an intelligence failure. Whether this designation is entirely fair or not, there is a perception that we failed to identify a cataclysmic event for the U.S. If we do not see the attacks as just a perceived failure of intelligence, we still have a lack of confidence in our intelligence. We just do not believe that we know enough in this area. Therefore, when we discuss intelligence about events such as these, we add the caveat "insofar as we know" in front of everything.

As Todd Masse mentioned, Graham Allison's book, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, talks about "Dragonfire" [1]. Shortly after the events of 9/11, a report originating from a source named "Dragonfire" stated that there was a terrorist nuclear weapon in the city of New York, and the Nuclear Emergency Search Team was called out to look for it. The report caused great alarm. It turned out that "Dragonfire" was not a reliable source; it was simply not a reliable report.

Richard Myers, the former Chairman of the Joint Chiefs of Staff, recently published *Eyes on the Horizon: Serving on the Front Lines of National Security* [2]. He says that in an October 2002 National Security Council (NSC) meeting, the President said that they had received information that al Qaeda had a nuclear weapon. Jaws dropped around the table, as General Myers described it; this was obviouslya source of great concern. It would be interesting for someone with the appropriate clearances to go back and unravel that story to see exactly where it originated and how it came about. Of course, as is the case of "Dragonfire," it also turned out to be wrong. We cannot say with certainty that al Qaeda did not—or does not—have a nuclear weapon, but *insofar as we know*, it has no nuclear capability. Nonetheless, this shows the difficulties or lack of confidence—and in some cases, simply wrong information—in intelligence about nuclear terrorism.

"Nuclear terrorism is about the frightening possibility that terrorists will acquire and use a nuclear device. Nuclear terror is about our apprehension of that event."

Terror Versus Terrorism

Now we have arrived at the variable T, which is divided by two to make the distinction between nuclear terrorism and nuclear terror. These are different domains. Nuclear terrorism is about the frightening possibility that terrorists will acquire and use a nuclear device (e.g., cause a nuclear explosion). Nuclear terror is about our apprehension of that event.

Nuclear terrorism is about intelligence, evidence, threat assessments, and estimates of capabilities. Nuclear terror is driven by our imagination. The history of nuclear terrorism can be briefly summarized: There has been none—although many would hasten to add “yet.” Nuclear terror has its own rich, natural history that in fact reaches back even before the first explosion of a nuclear bomb in New Mexico; it is deeply embedded in our public mind and in our policy-making circles.

So when we talk about threat assessment, we have to be careful. Are we being driven by nuclear terror, or are we assessing nuclear terrorism? In fact, I will spin off one of Todd Masse’s remarks: In the eyes of some Americans right now, because of our economic crisis, the U.S. is at a particularly vulnerable moment, and therefore this would be an opportune time for al Qaeda to strike with a nuclear weapon. That may be true, but it leaves out the other part of the observation that assumes al Qaeda has a nuclear weapon and that timing is simply a matter of choice. The fact that this year is an opportune time compared with a less opportune time last year or a less opportune time two years from now is irrelevant to the assessment of al Qaeda’s capabilities. When it has a nuclear weapon—if it ever has a nuclear weapon—it will strike.

Three recent factoids point out how we really must make the careful distinction between nuclear terror and nuclear terrorism:

- According to a 2007 Harris poll, 42 percent of all Americans thought it likely and another 14 percent thought it highly likely that a nuclear bomb would explode in an American city in the next five years. That was 2007. It is now 2009—we have three years to go. Clearly, that assessment is inconsistent with our daily behavior. You cannot seriously believe that a nuclear weapon is going to go off in an American city within five years and still buy a home, reside, and raise your children there.

- In a September 2008 address, then-director of the Central Intelligence Agency (CIA), Michael Hayden, said that although Iran and North Korea have the capability to produce nuclear weapons, al Qaeda was the CIA’s top nuclear concern because it was most likely to use them. This declaration was quite interesting because we know that North Korea has nuclear weapons and we know that Iran has nuclear ambitions as well as a lot of centrifuges and scientists, but the CIA's number one nuclear concern was al Qaeda because, as Hayden said, "The question is not of capability, but intent."

- In November 2008, the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism indicated that the likelihood of terrorists using biological weapons or nuclear weapons in the next five years was 50/50. The Commission went on to give some perfectly sensible, preventive recommendations.

These three items were driven by three different motivations. The first—that a large percentage of Americans believe a nuclear attack is likely in the next five years—is simply driven by fear; the American public is terrified of a terrorist nuclear weapon.

The second item was obviously an assessment of intentions rather than capabilities; al Qaeda is our number one nuclear concern not because we necessarily believe it has a nuclear weapon, but we believe that if they had a nuclear weapon, it would likely use it—the concept of deterrence is very difficult to think about with al Qaeda, at least in the traditional application of that concept.

The third item is driven by the necessity for a call to action. Like all commissions, the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism has no statutory authority. Its members have only power of persuasion; they have 15 minutes of fame, and they have to get people's attention and persuade then to do something within that short time frame. The Commission members involved declared a 50/50 percent likelihood of a nuclear attack as a summons to action.

THE PERCEPTION OF INEVITABILITY

When I wrote my book, *Will Terrorists Go Nuclear*? [3], I polled a number of people that I thought of as legitimate experts. These were people at the weapons labs, physicists at Sandia Laboratory and Los Alamos, intelligence specialists, and terrorism analysts. I asked: "What is the probability of a terrorist nuclear explosion in the next 10 years?" The estimates ranged from one in a million to a virtual certainty. What is even more interesting is that there was no distribution curve; it was flat. There was no consensus conclusion. Another interesting result of my polling, which I did in both Europe and the U.S., was that if you considered the Americans separately from the Europeans, you saw strikingly different answers. For the Europeans alone, the probability was one percent. Some would argue that even the European-selected one-percent likelihood is more than enough for us to take serious precautions.

"Americans have a comic book, two-dimensional understanding that terrorists are villains, which leads us into what I would characterize as 'ka-pow' strategies."

The second question asked in the polls was: "Why has it not occurred yet?" These polls called for simple answers, not essays. The answers fell into two large categories: capabilities and intentions. Most Americans pointed to capabilities. Terrorists, they said, "do not have the capability." The Europeans had a much more complex view and introduced the issue of intentions.

We tend either to view terrorists as mad dogs or to consign them to the realm of evil—no further inquiry necessary. Bruce Hoffman raised this point in his address, "Terrorism – from IEDs to WMDs." I agree. We do not know enough about the enemy. Americans have a comic book, two-dimensional understanding that portrays terrorists as mindless villains, which leads us into what I would characterize as "ka-pow" strategies: not very thoughtful responses.

The Europeans have a bit more experience with terrorists. I am not sure they are necessarily right, but they have a very different picture. They see terrorists as far more complex beings in terms of their recruiting, radicalization, motivation, etc.

I do not believe a nuclear attack is inevitable. I do not believe there is any inexorable progression from terrorist truck bombs to terrorist atomic bombs. Estimates of probability are interesting, but they have no predictive value in themselves, so why do we think in terms of probabilities? Opinion is divided here, too. We would hardly spend billions of dollars to prepare for an event that we thought was a one-in-a-million shot. Probabilities are related to perceptions and well-placed, authoritative calls to action.

"I do not believe a nuclear attack is inevitable. I do not believe there is any inexorable progression from terrorist truck bombs to terrorist atomic bombs."

In calls to action, consequences trump probabilities. No matter what the estimates of probability are, forecasts are a murky area. However, consequences are concrete and quantifiable. If we consider an estimated death toll in the tens of thousands to hundreds of thousands, we would be looking at an event 100 times worse than the unfortunate losses from the attacks of 9/11. The death toll would exceed, in an instant, all of the fatalities suffered by the U.S. during World War II.

Apart from casualties, the direct damages from 9/11 ran to about $50 to $60 billion, and the overall economic impact was in the hundreds of billions of dollars. A nuclear attack would have a financial impact a hundredfold that of 9/11, potentially approaching the nation's entire gross domestic product of about $14 trillion. Of course, destruction at that level presumes a worst-case scenario. A 10-kiloton device detonated in the heart of Manhattan would compare to a nuclear 9/11 or an American Iwo Jima, two very popular terms in threat literature.

"Terrorist scenarios that were dismissed as far-fetched on 10 September became operative presumptions on 12 September."

TERRORIST CAPABILITIES

There is a great deal of debate about terrorist capabilities. Some say that a 10-kiloton device would really be extraordinary for terrorists to achieve; most likely, they might be capable of a kiloton or tens of tons, if they achieved any yield at all. The debate, interestingly enough, is divided between the weapon designers and the weapon builders. Weapon designers—the people who do the math—tend to argue that this is easier than people think. However, the people who actually build the weapons—those you meet at Los Alamos who are missing a finger or something because of a machine accident—say, "No, even when you have the math right, this is really hard to do."

I probably could not tell the difference between a diagram of a hydrogen bomb and a diagram of a soft-drink vending machine, so I have no particular opinion on this. Actually, I probably could: Vending machines take quarters; bombs do not. The point is—thinking of how we are dealing in the shadow of a cataclysm—the events of 9/11 fundamentally altered our perceptions of plausibility. Terrorist scenarios that were dismissed as far-fetched on 10 September became operative presumptions on 12 September. If terrorists could carry out the attacks of 9/11, then how could we dismiss anything? Thinking of all the possibilities has brought about a fundamental shift in how we assess terrorist threats. Traditional threat assessment is based upon some analysis of the adversaries' intentions and capabilities. This technique was pretty straightforward during the Cold War. We could count Soviet tank divisions parked in the Fulda Gap and Soviet missiles and warheads; we knew they were pointed not at Paraguay, but at the U.S. So much for intentions; we knew capabilities. It was a calculation one could make.

In the current era of terrorism, we lack that kind of intelligence about enemy capabilities, as was demonstrated on 9/11. Therefore, the threat assessments shifted to vulnerability-based analysis. You start with a vulnerability, posit a hypothetical terrorist foe, and outline a scenario. Vulnerability-based analysis is perfectly legitimate if we are concerned with assessing consequences. If the terrorists were to do this (fill in the blank), what would be the consequences and how would we respond? Would we be prepared to deal with those consequences?

I give very few public lectures where I am not approached by someone after the lecture saying, "You know, if I were a terrorist, I would...″ It is extraordinary that even ordinary-looking people, e.g., librarians and bankers, can come up with extraordinarily diabolical schemes. There is a little armchair terrorist in all of us.

A vulnerability is not a substitute for threat, but it frequently becomes one. In many vulnerability analyses, you will see something that starts out as a possibility, and as you read through the report, it becomes a probability; you read further, and it becomes inevitable. By the time you are at the end of the report, it is imminent. This trend is a problem that has led to what I call threat advocacy.

The problem with vulnerabilities is that they are virtually infinite. All of us at this symposium could fill volumes with vulnerabilities and diabolical scenarios, but resources are finite. Competition for finite government resources leads to threat advocacies in which champions of particular scenarios assert themselves to capture resources because their threat must be worse than all the others and therefore must deserve greater attention and support.

″There is no terror in a bang, only in the anticipation of it.″ — Alfred Hitchcock

THE AMERICAN PSYCHE

Threat advocates are not fear mongers. The risks are real; action is necessary. However, our noisy democratic system responds to fear. This is a contest that nuclear terrorism easily wins. Alfred Hitchcock once said, ″There is no terror in a bang, only in the anticipation of it.″ Americans are uniquely susceptible to nuclear terror. Part of it is the hangover from the Cold War, and the other part is a fundamental element of the American psyche. Todd Masse used an interesting phrase: “etched into the American psyche.″ How did this happen? What kind of acid etched this into the American psyche? How come we are so susceptible to it? Beneath our characteristic American optimism lies a lot of anxiety. We worry that America will lose its exceptional place in the world, we fear that our military will be challenged by new foes against which we have little defense, and we fear that our borders no longer protect our territory or our culture. We fear subversion from within.

In some respects, we are a very religious country, and there are many Americans who see the threat of nuclear terrorism as consistent with biblical prophecy—a sign of the end plus, a confirmation of faith. Nuclear terrorism figures heavily in the fictional literature of popular religious writers. By the way, if you want to talk about writing a best seller, ask Hal Lindsey and Carole C. Carlson, the authors of the book, *The Late, Great Planet Earth*, published in 1970, which has sold 50 million copies, an extraordinary phenomenon.

Our current news networks have magnified this phenomenon. Because the news organizations today in this country increasingly look for sensational stories to hold their audiences, they contribute to the general sense of alarm. Unfortunately, this is reinforced by a relentless message of fear coming out of Washington—from both political parties, which have participated in the manufacture and dissemination of doom.

"I think the most dramatic development in contemporary terrorism has not been terrorists' acquisition of new weapons—the weapons have changed relatively little in the past quarter century. It has been the Internet and the media skills that al Qaeda is providing to its affiliates and others around the world."

Of course, terrorists are also active participants in this process. That is what terrorism is all about. It is what terrorists are good at. Terrorism is violence that is calculated to create an atmosphere of fear and alarm, which in turn causes people to exaggerate the threat that the terrorists pose and consequently the importance of their cause. They achieve this through violence but also through words and images. Bruce Hoffman correctly pointed out the influence of al Qaeda's media jihad, with its hundreds of Websites and the ability to manipulate a narrative, a message of fear.

I think the most dramatic development in contemporary terrorism has not been terrorists' acquisition of new weapons—the weapons have changed relatively little in the past quarter century. It has been the Internet and the media skills that al Qaeda is providing to its affiliates and others around the world. What is interesting is that even as the operational capabilities of al Qaeda—or at least those of al Qaeda Central—have been somewhat degraded, its media campaign—its global media jihad—aimed at inspiring and instructing its followers has increased in volume and sophistication.

Online jihadis participate both as consumers and as co-producers, which has enabled al Qaeda to become the world's first "virtual terrorist nuclear power." We know that al Qaeda has nuclear ambitions. They have tried to obtain nuclear material, and they have talked about its use—from deterrents to an implied first-strike strategy. Insofar as we know (again that famous phase), they do not possess nuclear weapons. According to certain documents that have been discovered, they do not possess the knowledge to make them, but they have figured out that fomenting nuclear terror does not require possession of nuclear weapons at all.

There have been reports of internal debate within al Qaeda's planning circles about weapons of mass destruction. If they are true, these reports indicate that there were serious planners within al Qaeda who thought that weapons of mass destruction were a distraction, but they went along with the others who wanted to acquire them because the language of weapons of mass destruction could create fear. They concluded that "this is part capability and part illusion, and we are really good at creating illusion so we will hold onto this."

What al Qaeda does have is a very effective propaganda machine. Top leaders give official comments with increasing frequency, and then the second and third tiers of online jihadis—the powerless who fantasize about ultimate power—embellish this fantasy with calls to nuclear terror, nuclear threats, and vivid graphics. It becomes real.

If you look at the graphics on these Websites they are really fascinating. There is one of bin Laden poring over a map table, and if you look very closely, the map is of midtown Manhattan. If you look even closer, there are little orange blobs, which are little mushroom clouds at all of the iconic targets in New York. Another favorite theme in al Qaeda nuclear artwork—they should have an exhibit—is the U.S. Capitol building with the mushroom cloud of a nuclear explosion behind it. Another graphic features a mushroom cloud overlaid with the gaunt, bearded figure of Osama bin Laden himself. It is a kind of art, but its production provides a certain amount of psychological satisfaction. This is video-game stuff to a lot of the online jihadis. Naturally, we also view these graphics, and they contribute to our general alarm.

"Fear is not free. Fear can distort the way we address the threat of nuclear terrorism itself. We may too readily accept as real scenarios that merit debate. Fear tends to warp our judgment, both in our threat assessment and in our reaction."

CONCLUSION

We do have to take the possibility of nuclear terrorism seriously, even if the possibility of nuclear terrorism is a long shot. Nothing that I am saying here should in any way diminish the seriousness of concern, but we have to be careful not to succumb to nuclear terror.

Fear is not free. Fear can distort the way we address the threat of nuclear terrorism itself. We may too readily accept as real scenarios that merit debate. Fear tends to warp our judgment, both in our threat assessment and in our reaction. It is remarkable that we have serious scholars writing that in case of an imminent nuclear threat to the country—or heaven forbid—a nuclear explosion somewhere, the Constitution of the United States must be suspended and martial law must be declared. One wonders why the courts could not still be working, assuming they are outside the area of the nuclear blast.

Nonetheless, such a scenario has become a serious issue in today's thinking. It is extraordinary for me to think that this nation has dealt with civil war, the Cold War, and decades of confrontation with a Soviet superpower armed with tens of thousands of nuclear weapons, and yet it is this warped judgment, warped by nuclear terror, that has caused people to seriously consider the suspension of the Constitution. Again, nothing that I have discussed here should diminish the seriousness of the issue, but I want to underscore the difficulty of coming to a concrete, rational assessment of the threat.

REFERENCES

1. Graham Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, New York: Henry Holt and Company, 2004.
2. Richard Myers, *Eyes on the Horizon: Serving on the Front Lines of National Security*, New York: Simon and Schuster, 2009.
3. Brian Michael Jenkins, *Will Terrorists Go Nuclear*? Prometheus Books, 2008.

5.3 SHARING SCIENCE AND TECHNOLOGY WITHIN THE INTERAGENCY

Jonathan Medalia

INTRODUCTION

There are multiple paths to a terrorist nuclear weapon, and as if to emphasize and confirm the point, a recent edition of *The Washington Post* [1] quoted David Kilcullen, one of the world's leading terrorist experts. He said, "We're now reaching the point where within one to six months we could see the collapse of the Pakistani state." If terrorists were to acquire a bomb, the main and last line of defense would be nuclear detection technologies.

I will explain how detection works, give a few examples of detection technology, and discuss several lessons and thoughts for interagency and other forms of coordination. I should emphasize that this talk represents my personal views and not necessarily those of my employer, the Congressional Research Service.

THE SCIENCE

One must learn a bit of science to understand nuclear detection. Nuclear weapons use fissile material. What is important

Dr. Jonathan Medalia is a Specialist in National Defense at the Congressional Research Service, where he has worked for many years on nuclear weapon policy issues for Congress. These issues include MX, Trident, nuclear testing, nuclear weapon laboratory demographics, the Comprehensive Test Ban Treaty, stockpile stewardship, nuclear and radiological terrorism, and most recently the Robust Nuclear Earth Penetrator, Advanced Concepts Initiative. He received a bachelor's degree from Cornell University and a master's degree and Ph.D. from Stanford University. He received a Doctoral Research Fellowship from the Brookings Institution and a Postdoctoral Fellowship from MIT.

about fissile material is that it can be fissioned or split by neutrons traveling at any speed, fast or slow.

In a large enough piece of fissile material, fission releases neutrons that release more neutrons, resulting in a runaway chain reaction that releases vast amounts of energy. The two main types of fissile material are uranium highly enriched in the isotope 235, which is called highly enriched uranium (HEU), and plutonium, especially isotope 239. Collectively, they are called special nuclear material (SNM).

Nuclear weapons and SNM have various signatures by which they can be detected. As we will see, detection is difficult but not impossible. I will discuss five of these signatures.

Gamma Rays

Gamma rays are high-energy photons emitted when an atomic nucleus decays to a lower energy state. The energies of gammas from a particular isotope may be depicted in a spectrum, which is a plot of energy versus number of counts at each energy level (Figure 1). The bottom axis is the energy and the vertical axis represents the counts. There are different peaks at different energy levels. This spectrum is unique to an isotope; if you can identify the spectrum, you can identify the isotope that caused the spectrum.

However, there are several detection problems. A cargo container may hold items containing nonthreatening radioactive material, and dirt may generate background gamma rays. As a result, spectra of several radioactive isotopes may be commingled so that the threat signature must be distinguished from the others. Another difficulty is that HEU is hard to detect because its main gamma ray—as we see on the far left in Figure 1—is a relatively low energy. If terrorists were to build a bomb, they would prefer to use HEU because, unlike plutonium, it can be used to make a gun-assembly bomb, the simplest design. Plutonium is easier to detect. Yet another problem is that dense material can be used to shield gamma rays.

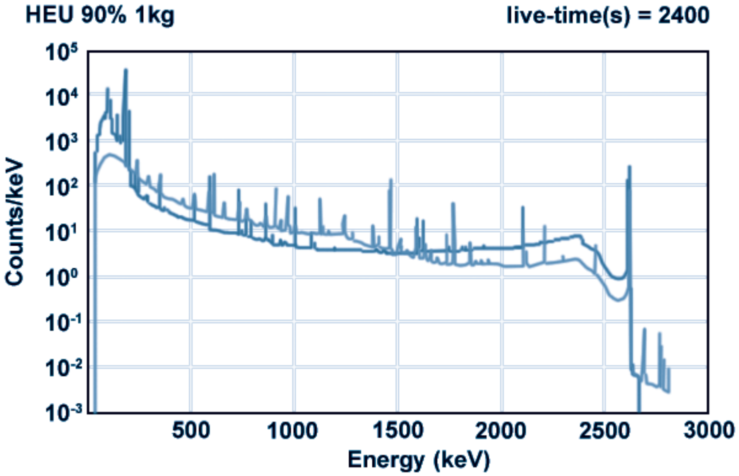


Figure 1 Gamma Ray Spectrum of HEU Taken with Geranium Crystal

Neutrons

Neutrons offer a second signature. Plutonium and uranium to a much lesser extent emit neutrons spontaneously, but few other materials do, so detection of neutrons is suspicious.

Size and Density

Third, a bomb may be detected by its size and density. High-energy photons can be beamed through a cargo container to produce a radiograph, just like a medical x-ray. A nuclear weapon would show up on a radiograph because it is dense, as would lead shielding.

Muons

A fourth signature comes from muons, which are heavy, subatomic particles that are caused when cosmic rays strike the Earth's upper atmosphere. They travel at nearly the speed of light. Their mass and velocity make them very penetrating. When they strike matter, they are deflected in proportion to its density. The high densities of uranium and plutonium would result in a different deflection pattern than plastic.

Flourescence

Fifth, ultraviolet light causes certain materials to emit light in a process called fluorescence. The ultraviolet raises the electrons to a higher energy state, and they emit light when they drop back to a lower energy state. Similarly, when a nucleus is struck by photons of precisely the right energy, it will emit gamma rays in a spectrum unique to that isotope.

This science that I have just discussed forms the basis for technology projects. A detector system has building blocks. Detector material captures photons or neutrons and converts their energy into measurable electrical pulses, algorithms process data, and computers to run the algorithms and provide a usable output, such as a display on a computer monitor.

Technology Under Development

Nanocomposite Scintillator

One technology under development is a nanocomposite scintillator. Many detector materials are plastics or crystals. Certain plastics like polyvinyl toluene (PVT) are rugged and cheap, and they can be made in large sheets. However, they have poor resolution of gamma ray spectra, so they cannot identify the source of radiation. As a result, they are prone to produce nuisance alarms.

Figure 2 is a spectrum taken with a PVT detector. It shows negligible detail. Contrast that with the spectrum from the germanium detector in Figure 1. Certain crystals, like high-purity germanium, have high resolution and can identify a substance emitting gamma rays, but they are small, delicate, and expensive. Los Alamos is currently mixing nanometer-size crystals in a plastic matrix to develop a detector material with the best features of both; the Domestic Nuclear Detection Office (DNDO), the Defense Threat Reduction Agency (DTRA), and Los Alamos jointly fund this project.

GADRAS

The second technology I want to discuss is called Gamma Detector Response and Analysis Software (GADRAS), the gold standard of algorithms for analyzing a spectrum to determine what material(s) generated it. GADRAS originated in 1985 at Sandia and has continually been updated, especially after 9/11. While many spectrum analysis programs examine spectral peaks, GADRAS analyzes the entire spectrum, which is important because most data are outside the peaks, and shielding and multiple radioactive sources may subtract from or add to the spectrum.

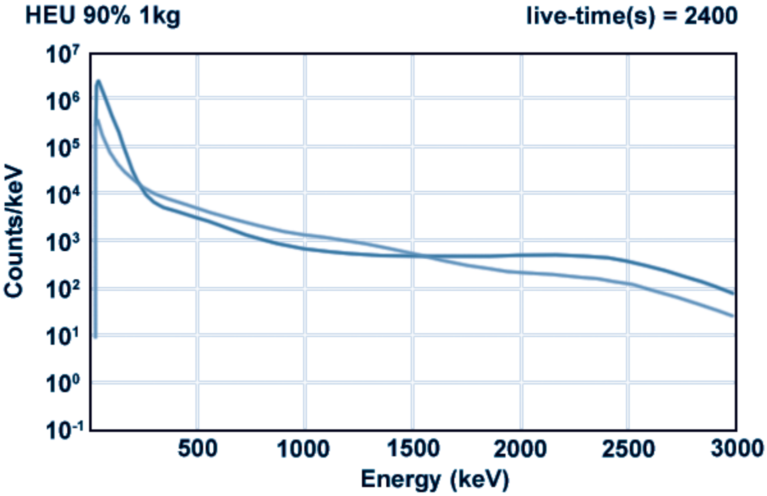


Figure 2 Gamma Ray Spectrum of HEU Taken with PVC

CAARS

A third technology is Cargo Advanced Automated Radiography Systems (CAARS). DNDO started CAARS to develop next-generation radiography equipment for Customs and Border Protection (CBP) to screen cargo at ports of entry. The goal is to detect dense material like uranium, plutonium, or lead. Dense materials are more opaque to high energy x-rays than less dense materials, and both materials have similar opacity to lower energy x-rays. The pixel-by-pixel ratio of the two radiographs of a container taken with x-rays of higher and lower energy permits differentiation between dense and less dense material.

One approach is to use two x-ray generators, one for each energy level. That requires a larger system, which is a problem where available space is at a premium, such as seaports. In another approach, Science Applications International Corporation (SAIC) and Accuracy Corporation developed a single so-called interlaced accelerator that generates x-rays at both energy levels. This accelerator is expected to permit a much smaller system.

Muon Tomography

The fourth technology is muon tomography. Recall that muons are highly penetrating subatomic particles. Los Alamos, through a cooperative research and development (R&D) agreement with Decision Sciences Corporation, has developed an algorithm to calculate the track of individual muons entering and exiting a cargo container. Calculating the deflection of each track is used to determine density of each volume element and locate dense material. This equipment is large but does not generate radiation because it uses naturally-occurring muons, potentially making the equipment of particular value for inspecting cars with passengers inside, such as at border crossings.

Nuclear Resonance Fluorescence

A fifth technology is nuclear resonance fluorescence (NRF). Bombarding an isotope with x-rays of the right energy level can cause the nucleus to emit gamma rays. The gamma rays are emitted in all directions, so by placing a detector behind the object to be detected relative to the x-ray beam, it is possible to detect only those gamma rays that are scattered backwards, minimizing interference from the x-ray beam. Because the gamma spectrum is unique to each isotope, this technique indicates which isotopes are present; for example, it can differentiate between U235, which can be used in a gun-assembly bomb, and U238, which cannot. Note that the gamma spectrum produced by NRF is different than the spectrum emitted through radioactive decay. Passport Systems is developing this system under contract to DNDO.

INTERAGENCY COORDINATION

Coordination might be improved in various ways. Here are two possible forms of international coordination:

1. Foreign governments, corporations, and universities are conducting nuclear detection R&D. Is there a way to coordinate U.S. and foreign R&D and acquisition to reduce overlap with work in the U.S. and take advantage of complementary efforts?

2. Terrorists might be deterred by fear that their attempts to conduct a nuclear strike would fail. Is there a way to coordinate a campaign to communicate to terrorists—indirectly, of course—that the large and growing global portfolio of detection technologies will increase their risk of failure?

Within the U.S., three agencies fund most nuclear detection work: DNDO, a part of the Department of Homeland Security (DHS); DTRA, a part of DoD; and the National Nuclear Security Administration (NNSA), a part of the Department of Energy. Dr. William Hagan, Acting Deputy Director of DNDO, told me that these agencies do coordinate in various ways. They evaluate each other's proposals and participate in each other's program reviews. If a laboratory submits a proposal to NNSA, DNDO and DTRA also know about it, they can decide on a case-by-case basis which agency conducts the work on a project. Sometimes, as we have seen, two or three agencies jointly fund a project. Could coordination be improved?

Improved intra-agency coordination may also be of value. CBP and DNDO are two components of DHS. DNDO funds development of nuclear and other detection technologies that CBP uses to inspect cargo. Some interactions between them have been well coordinated. For example, so-called contextually aware systems for inspecting cargo containers combine data from radiation detectors with data from a container's manifest and other sources to help CBP operators determine which containers merit additional attention. This determination is important to CBP because much of its work involves detecting traditional contraband like guns and drugs.

At the same time, CBP's agents operate the equipment to carry out DNDO's mission of detecting nuclear weapons and materials. Any technology that DNDO can devise to support both missions benefits both agencies.

Other interactions have not been well coordinated. DNDO misunderstood CBP's needs when defining the requirement for CAARS. CBP had a detection facility with an area of 160 by 60 feet, and DNDO thought that was an acceptable size for CAARS. Two of the three CAARS candidates used enclosures that size. However, the CBP system was experimental and much too large for use at seaports, where space is at a premium.

DNDO and CBP have learned from this experience. For example, they established the Joint Integrated Non-Intrusive Inspection Working Group to coordinate work on both CAARS and non-CAARS detection programs. A more general lesson learned is the importance of coordination between technology developers and users.

CONOPS

The success of a detection system requires a concept of operations (CONOPS), one aspect of which is the response if a threat is detected. Think of the detector material as the eyes and ears of a system, the algorithm as its brains, and the CONOPS as its hands. A system needs all three. If a CBP operator detects HEU but cannot use that information, the system is valueless. Thus, it is imperative to develop plans for various scenarios.

What happens if CBP detects something that looks like a terrorist nuclear bomb? Who determines if it is a bomb? Who attempts to defuse it? Who orders an evacuation? CONOPS requires coordination between CBP operators, weapons laboratories, response teams, state and local responders, and many others. Improved coordination or information sharing might also facilitate and increase productivity at the working level.

In preparing my report on nuclear detection, I found that hundreds of detection projects are underway, and work on one project might benefit other projects. However, in speaking with dozens of scientists and engineers, I found that they were often unaware of such work. How can information on these advances be distributed among projects that are funded by different agencies or carried out by competing laboratories, companies, or universities?

Brian Reese, a technical staff member at Los Alamos National Laboratory (LANL), believes that the root of this problem is that there is not a classified forum for disseminating this information outside the intelligence community. He says, "I am reluctant to publish things that skirt a classified topic. There is not even an appropriate forum for publishing For Official Use Only material."

To conclude, the U.S. is working on many nuclear detection projects. Understanding them requires a basic understanding of the science on which they are based, but that science is comprehendable. Improved coordination at various levels should promote more efficient development of nuclear detection capability.

REFERENCE

1. *The Washington Post*, "A Conversation With David Kilcullen," Interview by Carlos Lozada, Sunday, 22 March 2009; Page B02.

5.4 CREATING AN INTERAGENCY "CRITICAL MASS" FOR U.S. WMD TERRORISM ANALYSIS

J. Scott Cameron

INTRODUCTION

> *"There is no clear leadership or bureaucratic architecture defining roles and responsibilities for WMD terrorism. This adversely affects analysis, collection, and threat warning."*
>
> *— 2005 Robb-Silberman Commission (p. 296)*

The threat of WMD terrorism, and especially nuclear terrorism, are among the greatest national security challenges our nation faces. The need for interagency cooperation and in preventing or responding to such an event has never been greater. While there still remain gaps in intelligence and challenges in information sharing, the interagency response to this challenging problem set has improved dramatically in recent years. New organizational alignments, enhanced information sharing, and mission integration has brought greater focus and synergy to our national effort. The positive impact of these changes is most readily apparent in the analytic mission of the Intelligence Community (IC).

In order to better understand some of the progress that has been made in the nation's interagency posture against WMD terrorism, it is instructive to review a few of the conclusions drawn by the 2005 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction – also known as the Robb-Silberman Commission. When comparing the WMD terrorism analytic environment today to the Commission's

Mr. J. Scott Cameron, Ph.D., is the Chief of the Chemical, Biological, Radiological, and Nuclear Counterterrorism Group, U.S. National Counterterrorism Center.

view of interagency interactions in 2005, it is clear that much has changed.

THE EVOLUTION OF WMD TERRORISM ANALYSIS IN THE POST 9/11 ERA

In 2005, the Robb-Silberman Commission described the different yet overlapping roles of two primary analytic voices for WMD terrorism in the IC – one at the National Counterterrorism Center (NCTC), and the other in the Central Intelligence Agency's (CIA) Counterterrorist Center (CTC).

National Counterterrorism Center (NCTC)

> *"Perhaps most significantly in light of the criticisms leveled by the 9/11 Commission, the NCTC is producing analytic products that integrate the comments and concerns of analysts across the Community."*
>
> *— 2005 Robb-Silberman Commission (p. 283)*

The Commission recognized that the NCTC had created an environment where all of the nation's terrorism intelligence could be jointly exploited and analyzed by intelligence professionals of differing backgrounds and cultures from across the IC. This was especially important for Chemical, Biological, Radiological and Nuclear (CBRN) terrorism, the "functional" intelligence discipline of WMD terrorism that requires not only "traditional" intelligence analysts, but also subject matter experts (SME) from various fields of science and engineering.

The NCTC CBRN effort provided a balanced approach to intelligence analysis and its technical foundations, while creating a new, unique organization that reflected the best elements of the IC. The NCTC CBRN group was able to work effectively across the IC by relying on the networks and the "reach-back" of its organizationally-diverse analytic cadre. This process bridged cultural divides and respected the equities, missions and expertise of partners, thus making the production of finished intelligence a more comprehensive and inclusive process. Similarly, the challenge of translating the foreign threat into the domestic mission sphere became a more natural process through the implementation of NCTC's interagency authorities related to the Homeland.

CENTRAL INTELLIGENCE AGENCY'S (CIA) COUNTERTERRORIST CENTER (CTC)

> *"Perhaps most importantly, from an operational perspective it is clear that many of CTC's efforts to disrupt terrorist networks and plots—partially enabled by its in-house analytic cadre—have been extraordinary successes. Put simply, CTC has brought the fight to the terrorists."*
>
> *— 2005 Robb-Silberman Commission (p. 284)*

The Commission recognized the efforts of CIA's Counterterrorist Center (CTC) as an effective, mission-integrated force against WMD terrorism. This was credited in part to the integration of CIA's WMD terrorism analytic cadre with the corresponding elements of CIA responsible for intelligence collection and operations against WMD terrorism. The Commission valued this direct alignment of analysis with operations in that it not only produced better target-focused operational support, but also provided senior policy customers with a more tactical view of what was being done about the problem.

CIA's WMD terrorism analysts were also supported by CIA's broad portfolio of programs in counterproliferation, regional and terrorist organization expertise, and science and technology. These resources provided solid foundations for strategic analysis that could address complex issues in a broader, more global context. In addition to a large infrastructure and rich organizational heritage, CIA analysts were supported by excellent educational resources and training programs that enhanced their foundations of analytic tradecraft.

ONE TEAM, ONE FIGHT?

While the Commission highlighted accomplishments of several agencies as evolutionary steps indicative of progress in intelligence reform, they were also very concerned by some lack of cooperation and coordination among various analytic elements of the IC, most notably two primary WMD terrorism voices in the IC – the CBRN analytic cadres of CIA and NCTC. Going well beyond discussions of "bureaucratic battles", the Commission also observed that senior policymakers at the highest levels were not being served as efficiently and as effectively as possible due to "unproductive competition" between these organizations. At this point, both organizations recognized and began to address some of the significant cultural and organizational barriers that prevented the establishment of an optimized "one team, one fight" approach to WMD counterterrorism that the Commission was looking for.

> *"Ambiguities in the respective roles and authorities of the NCTC and CTC have not been resolved, and the two agencies continue to fight bureaucratic battles to define their place in the war on terror. The result has been unnecessary duplication of effort and the promotion of unproductive competition between the two organizations."*
>
> *— 2005 Robb-Silberman Commission (p. 288)*

SEEKING AN ORGANIZATIONAL SOLUTION

As of 2006, the majority of CBRN terrorism analysts in the IC were working in either CTC or NCTC in two separate organizations which essentially functioned independently of each other but yet had significant overlap in their respective missions. Seeing an opportunity to create a much needed "critical mass" on an issue of tremendous importance to national security, senior leaders of both organizations agreed to pool their analytic resources.

What resulted in 2007 is the jointly-managed NCTC-CIA CBRN Counterterrorism Group (CCTG). The missions of both organizations remained the same – CIA didn't gain a domestic mission, and NCTC didn't take on a direct operational role – but through a new and unique organizational alignment, the analysts of both organizations were now sitting together, working together, and fully supporting the missions of both organizations. To further build on this model of analytic integration and synergy, this combined interagency analytic cadre was imbedded with the CIA Counterterrorist Center, thus optimizing a continuum of analysis, collection and operational support in one location against WMD terrorism targets worldwide.

TODAY…

As it approaches the two year anniversary of its creation, CCTG has been able to use its interagency critical mass and subject matter expertise to evolve national leadership in the strategic and tactical analytic mission for CBRN terrorism directed against the U.S. and its allies. Through its unique organizational composition and integrated missions, CCTG has also been able to lead new and effective partnerships across the policy, intelligence, defense & law enforcement communities. This approach has broadened the scope of analytic viewpoints reflected in the IC's daily production cycles, and has allowed IC partners to better knit their unique assets and strengths into the fabric of an "all elements of national power" strategy against WMD terrorism targets.

Strength in Diversity. CCTG represents an organizationally-diverse critical mass of intelligence professionals with unparalleled access to the nation's most sensitive intelligence on the efforts of terrorists seeking to acquire CBRN capabilities. The net result of this approach has been a measurable increase in the quantity and quality of finished intelligence for the policy customer, the nation's intelligence professionals, and military and law enforcement partners. The uptick in counterterrorism operational tempo worldwide has also been well supported by the integrated missions and diverse organizational culture of CCTG.

Enhanced Functional Capabilities. While focusing its intelligence efforts on terrorist organizations and networks that may be pursuing unconventional warfare capabilities worldwide, CCTG has also focused on building and strengthening the IC's foundations for functional analysis in WMD terrorism. CCTG has recruited high level scientific and engineering expertise from across many disciplines, and has integrated this expertise to improve support for technical aspects of intelligence collection while answering serious questions of "what if?" in the CBRN terrorism realm. This process has also served to better connect the IC to solve hard problems using the more comprehensive technical resources available across the U.S. government, academia, and the private sector.

National Outreach. In addition to classified intelligence products for senior policy audiences and in support of the operator and collector, CCTG, in conjunction with its domestic partners at FBI and DHS, has also developed a large library of unclassified products and training aids in support of the first responder and law enforcement communities. CCTG officers are active in outreach nationally in briefing conferences and educational programs that support the police, fire, and public health professionals who are the nation's first line of defense and response to the threat of CBRN terrorism. These efforts have been recognized by customers as well as members of Congress who have heard positive feedback from constituents across the nation.

New tools. In addition to traditional approaches to the intelligence analysis mission of the IC, CCTG also supports the development of innovations and tools that will allow analysts to more effectively collaborate and while capturing, disseminating and institutionalizing knowledge and experience vital to improving tradecraft. While supporting key working groups for analysts to share information and experiences, CCTG has also been active in developing classified internet-based tools and resources within the IC that mirror the evolving communication and collaboration platforms available to the general public.

Support of Senior Leadership. In response to the creation of CCTG and its integration of analytic resources from across the IC, a number of senior policymakers inquired as to the possibility of creating a parallel effort that integrated the authorities and actions of senior leaders of the IC who had leadership roles in countering the threat of WMD terrorism. As a result, in 2007, the Director of National Intelligence created a "Senior Executive Board" for CBRN terrorism. Chaired by the Director of NCTC, this interagency group meets quarterly to address actions proposed by the IC that support integrated analytic and collection strategies against WMD terrorism in the near and mid-term. This engaged group of senior leaders ensures that potential bureaucratic barriers within the interagency do not prevent critical intelligence needs from being addressed quickly and efficiently. In the last year, this approach has promoted new levels of cooperation and joint action across the interagency in the fight against terrorist acquisition and use of CBRN weapons.

Protecting the Homeland. The Commission also observed in 2005 that domestic intelligence efforts on WMD terrorism were not keeping pace with the IC's foreign intelligence capabilities. Today, new partnerships between IC and law enforcement entities responsible for WMD terrorism analysis and operations have improved their working relationships and are working to further harmonize critical processes that in the past may have impeded joint capabilities to protect the Homeland from CBRN terrorism. New initiatives in this regard are underway, including further integration of CCTG and FBI resources to address the threat of terrorist CBRN activities as they potentially evolve from being a foreign threat into the Homeland.

CONCLUSION

While the IC has done much in recent years to create a more focused critical mass of analytic and functional expertise for WMD terrorism, there is still much work to be done. Analysis can only be as good as the quality and quantity of the intelligence that is gathered. Progress against terrorist CBRN targets requires continued focused interagency attention and strategies in order to field the most effective broad spectrum intelligence collection capabilities possible. Similarly, a broad analytic view of the elements of WMD terrorism is essential to developing a comprehensive strategy to meet these challenges.

The interagency analytic foundations for WMD terrorism have been strengthened, but continued progress in this regard is essential, and is just one element of a comprehensive strategy in the international effort to deny, disrupt and deter terrorist attempts to acquire and implement chemical, biological, radiological or nuclear capabilities.

5.5 THE ELEMENTS OF RESPONSE

Harvey Johnson, Jr.

INTRODUCTION

The question posed by this symposium is the following: Is our nation prepared to respond to a nuclear disaster today? The factual response is that we are not well prepared to respond to a nuclear detonation of virtually any size, neither at the federal level nor in communities around the nation. Yet at the same time, we must acknowledge that the components of an effective response are there for other disasters and would form the basis for a coordinated, if not fully effective, response. Thus, we need to further examine the challenges of an effective response to a nuclear detonation.

At the outset, I want to call attention to Senators Lieberman, Chairman of the Senate Homeland Security Committee, and Collins, Ranking Minority, as these Senators are both keenly aware of the shortfalls in response and recovery to a nuclear disaster.

Harvey E. Johnson, Jr. (USCG, retired Vice Admiral) recently was the Deputy Administrator and Chief Operating Officer of Federal Emergency Management Agency. Mr. Johnson has a wealth of emergency and crisis management experience. Previously, he served as the Executive Director of the Coast Guard's transition into the Department of Homeland Security. He was promoted to Flag rank in 2001. His other major decorations include the Legion of Merit (3), the Meritorious Service Medal (3), the Coast Guard Commendation Medal (2), and the Coast Guard Achievement Medal. Mr. Johnson received a B.S. at the U.S. Coast Guard Academy, an M.S. at the Naval Postgraduate School, and an M.S. in Management as a Sloan Fellow at the Sloan School of Management, the Massachusetts Institute of Technology in 1993.

They are working very hard, through hearings and discussions with the Executive Branch, to elevate and give visibility to these important issues. In part, their aim is to force needed discussion, identify priority issues, clarify roles and responsibilities, and then provide legislative guidance and authorization of funding to the respective federal agencies such that each can work together to improve our national capacity to marshal an effective response to a nuclear event.

In assessing our current capabilities and capacities, you might ask the following questions: "Do we have the right response doctrine?" Do we have sufficient information or knowledge about the effects of radiation and how to respond? The answer is that we do have doctrine, and we have the full measure of knowledge of the effects of nuclear radiation and the necessary countermeasures.

Let us continue: Do we have capable leaders? Do we have the necessary array of response capabilities? Do we focus on the nuclear threat in our exercise programs? Do we gain and share lessons learned? Again, we can respond that we do have capable leaders who are equipped with a broad array of response capabilities—though likely not nearly enough leaders or capabilities to meet a large demand. Yes, we do test our plans and capabilities in exercises at the federal, state, and local levels. We do gather and share lessons learned, even though not all federal, state, and local responders internalize all of the lessons we gain.

Finally, we need to ask whether we fully understand and are prepared for the immediate, the second, the third, and the fourth order effects of such a disaster. In view of the above, do we at all levels take seriously all that we know, including our roles and responsibilities, and perform them all in a forthright manner? Maybe this is the crux of the issue. When we add each of the elements for successful response and recovery—doctrine, leadership, knowledge, capabilities—and contrast them against the overwhelming first, second, and sequential consequences of a catastrophic incident, we become overwhelmed at the prospects. In context of a very large event, the expansive dimensions of the range of requirements and the essentiality of multi-level coordination in near real time are indeed significant and perhaps beyond the capacity of any single local or state capability. Perhaps it is that our planners and responders are already at max capacity with what are considered more likely threats and challenges, or, given the dimensions, we expect the federal government will step in. The reality is that we need to overcome the barriers—whatever they are—and get serious about preparedness, response, and recovery for a nuclear event of significant proportion.

ELEMENTS OF PREPAREDNESS AND RESPONSE

Let us take a look at some of the elements of response. The first element is that we do have a doctrine, our National Response Framework (NRF), which describes how our nation responds to all-hazard disasters. The NRF is built upon scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities across the nation, linking all levels of government, nongovernmental organizations, and the private sector. It is intended to capture specific authorities and best practices for managing incidents that range from the serious, but purely local, to large-scale terrorist attacks or catastrophic natural disasters.

The NRF begins with the premise that all events begin at the local level, and thus, the responsibility for responding to incidents, both natural disasters and manmade, begins at the local level, with individuals and public officials in the county, city, or town affected by the incident. Local leaders and emergency managers are to prepare their communities to manage incidents locally. In the vast majority of incidents, this foundational level of responsibility is able to marshal an effective response. These leaders are not left without support in that a primary role of state government is to supplement and facilitate local efforts before, during, and after incidents. The state provides direct and routing assistance to local jurisdictions through emergency management programs and by coordinating routinely with federal officials. States must be prepared to maintain or accelerate the provision of capabilities and services to local governments when local capabilities fall short of demands. Then, when an incident occurs that exceeds or is anticipated to exceed local or state resources, the federal government can respond to the request of a governor by providing support and services as may be needed. The federal government's response structures are scalable, flexible, and adaptable to the nature and scope of the incident.

These roles and responsibilities are described in the NRF, as are five key principles of doctrine that apply to all levels of government. Taken together, these five principles of operation constitute the national response doctrine:

- **Engaged partnership**: Leaders at all levels must communicate and actively support each level of government by developing shared goals and aligning capabilities so that no level is overwhelmed in times of crisis. Layered, mutually supporting capabilities at the federal, state, tribal, and local levels or planning together in times of calm and responding together effectively in times of need.
- **Tiered response**: Incidents must be managed at the lowest possible jurisdictional level and supported by additional capabilities when needed. It is not necessary, or desirable, that each level be overwhelmed prior to requesting resources from another level. National response protocols recognize this and are structured to provide additional tiered levels of support when there is a need.
- **Scalable, flexible, and adaptable operational capabilities**: As incidents change in size, scope, and complexity, the response must adapt to meet requirements. The number, type, and source of resources must be able to expand rapidly. Execution must be flexible and adapted to fit each individual incident: responders must remain nimble and adaptable.
- **Unity of effort through unified command**: Effective unified command is indispensable to response activities and requires a clear understanding of the roles and responsibilities of each participating organization. Success requires unity of effort, which respects the chain of command of each participating organization while harnessing seamless coordination across jurisdictions in support of common objectives.

- **Readiness to act**: Effective response requires readiness to act with an understanding of risk. A forward-leaning posture is imperative for incidents that have the potential to expand rapidly in size, scope, or complexity.

These guidelines of the NRF and these doctrinal principles will be essential to the marshalling of an effective response to a nuclear detonation. The good news is that the NRF and all of its elements are put into practice for events every day that range from small and locally contained to large hurricanes and other natural disasters. Also, they work effectively.

The NRF is also comprised of a set of Incident Annexes that provide forethought in how the NRF should be applied for certain types of incidents. One such Incident Annex is the Nuclear/Radiological Incident Annex, which details the roles, responsibilities, authorities, capabilities, and assets, as they will be applied in such an incident. This annex is written at the federal level, and describes how DoD, the Department of Homeland Security (DHS), the Environmental Protection Agency (EPA), the National Aeronautics and Space Administration (NASA), and the Nuclear Regulatory Commission (NRC) will provide support to states and communities for incidents involving the release of radioactive materials and the consequences of such an event.

Preparedness

The President has approved the Preparedness Guidelines that establish goals, set priorities, and describe how the nation should prepare and build capabilities essential for the response and recovery from emergencies and disasters. Each member of our society, including our leadership, professional emergency managers, private sector representatives, and nongovernmental organizations, has a role to play in strengthening our nation's response capabilities. Those roles can be described in terms of the preparedness cycle, shown in Figure 1. This figure lays out the process of how to prepare for all disasters: to plan, organize, train, equip, exercise, and gather the lessons learned, only to start the cycle over again to refine our capabilities. Each element of the Preparedness Cycle is defined and described in the NRF and will not be elaborated in this text. The mastery of these key tasks supports unity of effort and thus improves our ability to save lives, protect property and the environment, and meet basic human needs. The cycle represents exercises in the nuclear realm as well by federal departments and agencies identified in the Nuclear/Radiological Incident Annex, as well as by states, communities, nongovernment organizations, and elements of the private sector.

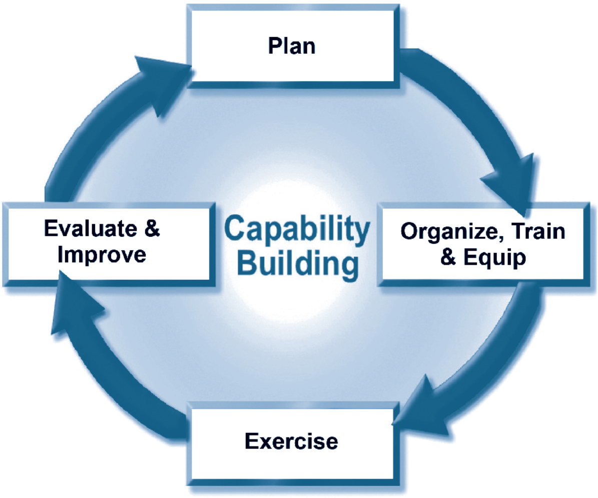


Figure 1 Preparedness Cycle

While the description in the NRF is straightforward, the actual implementation is more complex. The first element is essential to the successful and effective implementation of each of the other elements of the cycle. Yet, as a nation, we do not have a single or common approach to planning. There is no single planning tool that reaches across all nondefense departments and agencies at the federal level. Moreover, there is not a single approach among state and local governments. Significantly, a paradigm shift is in the making that has the potential to transform the manner in which planning occurs at the federal level, the state level, and, more importantly, how those levels interact. Within the last year, at the direction of the President, the Federal Emergency Management Agency (FEMA) has taken the lead in working across the interagency to establish the Incident Planning System (IPS). This system will soon be described in the context of a concept of operations (CONOPS) that will establish how the federal government will plan to address the requirements of a range of potential threat scenarios. The IPS will have a Strategic Guidance Statement to define the threat and outline essential roles, responsibilities, authorities, and high-level objectives. This Strategic Guidance Statement will support the development of a Strategic Plan, and a CONOPS that will be the basis for each department and agency to prepare Operations Plans. Just as significantly, states will begin to plan under the guidelines of Comprehensive Planning Guidance-101, with format, terms of reference, and structure that will more seamlessly integrate with federal IPS plans and supporting documents. We have never had that single plan at the federal level before, but it will lead to operations plans in each of our departments and agencies that will support this particular CONOPS. While it will take time for these new tools to be finalized and implemented, it will lead to improved preparedness across the nation.

With all of that ongoing, and more specific to nuclear detonation, federal departments and agencies issued a new document in January entitled the *Planning Guidance for Response to a Nuclear Detonation*. It is a wonderful, useful, informative, short document that is a great tool for planners at the state and local level to think, act, and prepare for a nuclear response. Every one of our key agencies [i.e., Health and Human Services (HHS), Centers for Disease Control and Prevention (CDC), DoE, EPA, and the National Research Council] have excellent documents that cover the panorama of issues that must be considered, planned for, and developed in a plan for a nuclear detonation.

Key Assumptions

As we begin to plan, one of the first tasks is to identify assumptions. These assumptions will guide the thinking and preparation for an event. In context of a nuclear detonation, critical assumptions would include the following;

- An improvised nuclear device (IND) attack will result in a complex, catastrophic disaster that will stress all of the specialized response capabilities and capacities in every single level of government.

- Initial response will be provided by local capabilities, largely by neighboring response units.
- At least one local community will be severely impacted: not fully capable of functioning in support of post-detonation response operations.
- There will be no significant federal response on scene for 24 hours: full extent of federal assets will not be available for up to 72 hours.
- Lessons from all-hazards planning and response are applicable.
- Some first responders may be reluctant or unable to perform their duties while others will instinctively and unknowingly enter contaminated or hazardous areas.
- There will be mass casualties that will exceed medical capabilities.

These key assumptions point to weaknesses in our current posture toward a nuclear detonation. Most notably, where we will need neighboring and regional communities to band together in mutual support on a significant scale, we do not plan regionally very well. Our communities do assist each other well on a daily basis to fill shortfalls, but the level of support in this scenario is beyond any level typically anticipated. This is a significant challenge.

The practical reality is that while the federal government has the largest share of capabilities needed for such a response, there will be no significant federal response for the first 24 hours, and we will be lucky to get everything in that we need to within the first 72 hours. Subsequently, the state, the local community, and the State National Guard (whose members were not affected by the detonation and first and second order effects) will be on their own for the first 24 to 48 hours. This is a significant challenge.

Fortunately, all of our lessons learned regarding hazards planning work can be applied in a nuclear response. We have our doctrine, and we have a significant level of knowledge that will be beneficial. We have planning guidance as was referred to, and we have the proficiency and professionalism of our first responders. These positives will only remain positive to the extent that states and communities give consideration to how they will be employed in the event of a nuclear detonation.

Capabilities

There is a significant level of capability to detect and monitor a radiation plume and to assess its effects on the health of individuals who may be affected. DoE will lead an immediate deployment of multi-agency organizations, such as the Federal Radiological Monitoring and Assessment Center (FERMAC), and the EPA will provide capabilities to assess the requirements for environment response.

The National Atmospheric Release Advisory Center will track the plume and the fallout and be able to predict and model that information for the first responders (e.g., Incident Management Assist Teams from FEMA), Accident Response Groups (ARGs) from DoE, the Advisory Team for Environmental Food and Health, and the National Medical Radiological Team from HHS among others. When a disaster occurs, leaders will come together in the field to formulate and organize a response.

The Federal Coordinating Officer (FCO) from FEMA, the Principal Federal Official who will represent the Secretary of the Department of Homeland Security, will deploy to the State Emergency Operations Center to coordinate the federal response. There will be a Defense Coordinating Officer who will have a direct link into support from DoD via Northern Command (NORTHCOM). The Senior Federal Law Enforcement Officer is a personal representative of the Attorney General and the Senior Energy Official will represent the Secretary of DoE. In the maritime environment, the Coast Guard will establish an On Scene Commander, and the Secretary of HHS will assign a Senior Health Official.

One of the most effective capabilities will come from within state-led National Guard units. The National Guard has embraced the establishment of Civil Support Teams, of which there are 74 across the nation. Each team has 22 personnel who are trained to swarm towards the direction of the event to provide decontamination assistance, assess the detonation, extent of damage, determine the nature of the threat, and help the first responders. Extrapolated across the nation, the National Guard has the capacity to provide more than 1600 trained soldiers capable of responding to a nuclear detonation. There are trained people who can assist first responders within that state. The Joint National Guardsmen Enhanced Response Force Package is battalion size, and there are 17 in our nation today with experienced National Guardsmen who are trained in exercise to provide support to state and local entities. Each would arrive in the community over time to help the first responders.

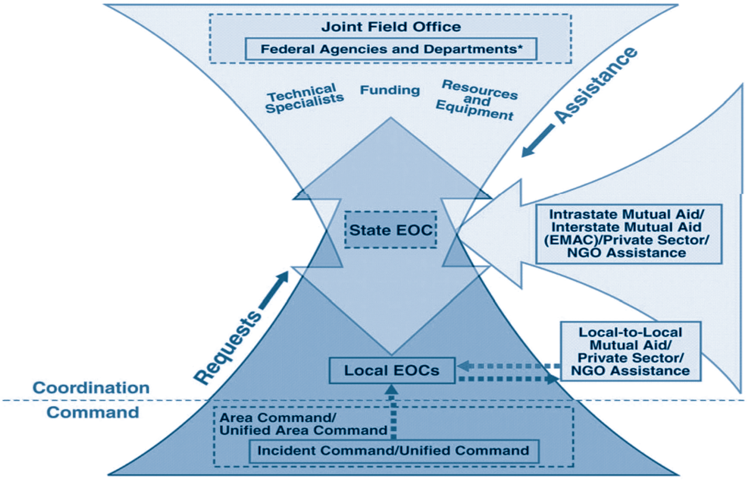

Joint Field Office
Federal Agencies and Departments*
Technical Specialists
Funding
Resources and Equipment
Assistance
State EOC
Intrastate Mutual Aid/ Interstate Mutual Aid (EMAC)/Private Sector/ NGO Assistance
Requests
Local EOCs
Local-to-Local Mutual Aid/ Private Sector/ NGO Assistance
Coordination
Command
Area Command/ Unified Area Command
Incident Command/Unified Command

Figure 2 Integrating Federal Support into State and Local Areas

Additionally, from DoD, the Marine Corps staff a Chemical Biological Incident Response Force (CBIRF). An emerging concept yet to be fully finalized is the development of a Chemical, Biological, Endiologicl, Nuclear, Explosive (CBRNE) Consequence Management Response Team, which will be capable of providing decontamination and security, medical triage and care, and transportation and logistics support. DoD has a number of trained capabilities that will respond, yet there will be a time lapse before they arrive.

All of these individuals will respond in accordance with the NRF, falling immediately into roles and relationships that they follow in all other forms of emergencies and disasters. Through practiciing this process, state and local communities know how to request capabilities, whether mutual aid from community to community; Emergency Mutual Aid Compact (EMAC) from state to state; or requests for federal assistance. These processes, as depicted in Figure 2, link federal, state, tribal, local, nongovernment organizations, and the private sector such that requests for capabilities and the provision of assistance can be organized and placed where needed.

Exercises

Referring again to the Preparedness Cycle (Figure 1), exercises provide opportunities to test plans, validate requirements and improve coordination and integration across jurisdictional and functional lines of responisibility. Exercises identify strengths as well as weaknesses and are essential in building the credibility and confidence. Through the implementation of the National Exercise Program, exercises are better coordinated across jurisdictions and strengthen the national network of capabilities. In the aftermath of the catastrophic events of 9/11 in 2001, there has been a greater federal focus on preparations for response and recovery from a nuclear detonation. The long list of exercises focused on the nuclear threat, specifically within the last three years, includes the following:

- June 2006 – Top Officials 4
- January 2007 – Vigilant Sentry/NUWAX
- April 2007 – Ardent Sentry/Northern Edge
- February 2008 – National Level Exercise [Improvised Nuclear Device (IND) component included)]

- June 2008 – Principal Level Exercise
- 2010 – National Level Exercise

In addition to these federally sponsored exercises, there are likely dozens more at the state and local level. Among these are the more than 30 exercises per year sponsored through the Radiological Emergency Preparedness Program (REPP) for communities surrounding nuclear power plants. FEMA and the NRC recently coordinated to improve REPP exercise scenarios and heighten preparedness for a broader range of potential events to include terrorism as well as the unintentional release of radiation into the environment.

These exercises validate policies, plans, and procedures related to pre- and post detonation; test coordination and communications across federal departments and agencies as well as integration with state capabilities; challenge protocols for the allocation of scarce yet essential capabilities; and examine media relations and public information capabilities.

As the last step in the Preparedness Cycle, it is imperative that all those involved in this extensive exercise program take care, both during and at the conclusion of each exercise, to capture lessons learned that can be reinvested in refining plans, fine tuning requirements, and updating training and education materials. The most recent development of new CBRNE capabilities within DoD and upgraded team capabilities within the DoE and EPA are testament to the translation of lessons learned into new and improved national capabilities.

Risk Communication

A significant level of attention has been devoted to improving the effectiveness of risk communications to individuals and the public at large. In an era where the risk of such an incident has been heightened, our risk communication must be more thoughtful to the realities of human behavior. For example, while shelter-in-place is a preferred inital action, parents are likely to go first to schools and day care facilities in an effort to retrieve their children. Those with special needs require specific direction tailored to their need. Families are more attentive to pets and the need for the care and disposition of pets to be included in public safety messaging. Likewise, technology that has expanded the forms by which notifications can be made opens new opportunities for effective messaging.

MAJOR CHALLENGES

There are a number of significant challenges that confront the emergency management community while preparing for a nuclear event. These include the following:

- **Conduct of realistic integrated regional planning**. A disaster of any significant size will likely affect the broader communities beyond the point of detonation. The plume, variable by wind and weather, may carry radiation to many neighboring communities with different requirements than the detonation community. Yet, most community plans are independently developed, and almost always as the community of detonation. Few communities plan for the second or third order effects of a disaster in a neighboring community. We need to do a better job of regional planning: expecting to help our neighbor and not just focus on the immediate community of impact.

- **There are not enough medical burn facilities**. The nation will not have sufficient burn facilities or medical transportation capabilites needed in the event of a moderate detonation. This likely will not change, thus requiring greater care in triage and in development of temporary medical capabilities that will be required to provide a broad range of immediate and follow-on care.

- **Education of government executives and emergency managers**. The constant turnover of government officials who will be decision makers during a catastrophic disaster, and the need to expand the sizes of thinly staffed emergency managers heighten the need for education on critical topics such as: initial shelter and evacuation plans (informed by plume modeling); establishment of emergency medical care (particularly within the first 24 to

72 hours); decontamination priorities, methodologies and capabilities; response worker safety; and, effective means of devloping and delivering effective communications to the public.

- **Education of the general public**. Despite all of the information and knowledge resident within our many systems regarding preparedness doctrine, incident planning, and medical implications of radiation, the state of public education is woeful. Essential topics include personal and family preparedness, immediate response actions, and the imperative to safely shelter-in-place.
- **Setting realistic expectations**. The setting of realistic expectations for care, response, and survability is a particular challenge. While much of our planning and thought processes lead us to focus on the event of Day One, the most vexing challenges will occur on Days Three, Four, and beyond.

This is a discussion that does not lend itself to a happy ending. While we can claim that should an attack or contamination happen in America, we will find a way to respond through fortitude, determination, inspired leadership, and a national imperative. But clearly, we can—and must—do better. Our nation has an immense need to focus on preparedness, employ the data that we have now (i.e., the doctrine, structure, information, and knowledge), and communicate with our public to educate those who will lead a response.

5.6 QUESTIONS AND ANSWERS HIGHLIGHTS

Transcripts

There was no Q&A Session due to time constraints.

Chapter 6

Roundtable 5

Analysis Support

6.1 MODERATOR'S SUMMARY

John Benedict

INTRODUCTION

This roundtable will examine analysis and support of interagency efforts that are addressing complex, nontraditional national security problems. In this overview, I will give my perspectives on what can and cannot be modeled, cause and effects, goals, metrics, methods, data requirements, and the need for enterprise approaches.

MODELING ILLUSTRATIVE ACTIVITIES

In a complex, operational environment, what are some of the activities that can be modeled? Illustrative counterinsurgency (COIN) Operation Iraqi Freedom (OIF) activities that can be quantified or predicted include raids; direct action missions; fire support; close air support; clear, hold, or retain operations; intelligence, surveillance, and reconnaissance missions; border perimeter security; population resource control measures; counter-

Mr. John R. Benedict is a Fellow in the National Security Studies Office within the National Security Analysis Department at The Johns Hopkins University Applied Physics Laboratory. Prior to this (2004-06), Mr. Benedict served as Head of the Joint Warfare Analysis Branch in the same department, and he was responsible for establishing common analysis processes and developing analytic capabilities required to conduct tactical, mission, operational, and campaign analyses appropriate to its sponsors. Mr. Benedict has had articles published in many journals and was a recipient of the Special Achievement "Bronze Medal" Award from the National Defense Industrial Association in 2002. He has an M.S. in Numerical Science from The Johns Hopkins University and a B.S. in Mathematics from the University of Maryland.

improvised explosive device (ED) tactics; mortar attacks; logistics; re-supply; etc. These activities are largely military problems in a physical domain. However, as Secretary of Defense Gates has told us, ″Success will be less a matter of imposing one's will and more a function of shaping behavior,″ the soft power side. That is where the problem lies.

Illustrative activities cannot always be modeled, quantified, or predicted in the COIN/OIF realm, in my opinion. How do you model, quantify, or predict sectarian violence triggered by al Qaeda blowing up a golden mosque that results in four million displaced Iraqis? How do you predict that the Iraqi government will have a blind eye toward Shia atrocities until a tipping point is reached on a Shia holy day? How do you predict the effects of Intel dominated by informants? How do you predict commanders cutting deals with reconcilable insurgents? How do you predict the effects of pressure on the Maliki government for national reconciliation? How do you predict Sunnis being put on the U.S. military payroll? How do you predict a key breakthrough that was caused by a U.S. Colonel cajoling a key obstructionist female aid in the Iraqi government? How do you predict the extent of and benefits from amnesties, pardons, and detainee release and reintegration programs?

These results occur from relationships forged with Iraqis at every level. They are based on human behavior and socio-cultural factors that cannot easily be modeled and quantified.

Continuing with what things that are difficult, at best, to predict, how do you predict the occurrence of and effects from the following COIN/OIF events; the inflow of foreign fighters; Iranian meddling with the Shia militias; diplomatic pressure on Syria and Iran; special U.S. Intel units to identify extremists; Sunni tribes turning on al Qaeda; U.S. forces collaborating with active insurgents; or even the net effect of negative and positive factors that influence the Iraqi populace reaction to U.S. occupiers? There are a lot of factors there. It is very hard to predict how this all will play out, as is the U.S. populace reaction to protracted COIN operations, with another set of associated negative and positive factors.

Once again these activities largely relate to human behavior and typically entail government interagency problems encompassing social, cultural, information, and cognitive domains that are much more complex than modeling, quantifying, and predicting physical outcomes from military operations.

CAUSE AND EFFECT

Now let us discuss cause and effect for the same COIN/OIF illustrative activities. Let us use an example effect such as a dramatic reduction in violence in Iraq as shown by the number of convoys attacked. One in five convoys was attacked in January 2007, going down over time, until the statistic changed to one in 100 a year and a half later. Potential causes include:

- Sunnis turning on al Qaeda
- Outreach to armed antagonists by local U.S. commanders
- “Sons of Iraqi” volunteers providing security and maintaining cease-fires
- Reversing de-Baathificiation policies (e.g., allowing jobs/pensions for Sunnis)
- More precise counterterrorism operations
- Redistributing U.S./Iraq security forces throughout the populace
- Population control measures to better separate out insurgents
- Clear, hold, retain, and build tactics enabled by increased forces
- Disruption and/or containment of Shia militias

Because we can only speculate on which combinations of these factors are most responsible for the reduced violence in Iraq, how can we hope to make an accurate prediction for this type of complex operational environment, particularly if it is done in the future?

GOALS AND METRICS

Now I will discuss goals and metrics for COIN/OIF. Below are quotes from Albert Einstein and Bing West, from his book *The Strongest Tribe*, that suggest it is very important to establish goals and metrics early in complex endeavors:

> *"Perfection of means and confusion of goals seem to characterize our age."*
>
> *– Albert Einstein*
>
> *"This absence of clear goals and measures would bedevil the [OIF] military effort for years."*
>
> *– Bing West*

Examples of potential OIF goals and metrics include (1) short-term tactical and operational level goals, (2) short-term operational and strategic level goals, and (3) long-term strategic level goals. In the short term, you can try to reduce the number and impact of IEDs, and other attacks by belligerents, which is still very hard to predict because there is both soft power and hard power at work there. Also in the short term, you can try to defeat or neutralize particular groups of insurgents, which is even harder to predict.

The harder long-term goal, in fact off the charts in difficulty, would be defeating the overall insurgency movement and achieving sustainable stability. Accomplishment of short-term, immediate goals is necessary and somewhat easier to predict, but it is not sufficient to determine overall success. The accomplishments that really constitute success have to do with whole-of government approaches, including a lot of soft power actions, not just physical power. These are very hard for us to get our arms around, particularly in future scenarios, much less ongoing operations.

THE ANALYSIS SPECTRUM

The spectrum of analysis informs decision makers. The spectrum begins with events (e.g., a conference, a thought piece, or an article) that are more qualitative than quantitative, much like this symposium; these events are mostly a one-way information dissemination by subject-matter experts (SMEs) that help us to understand a complex and/or emerging problem. There are notable exceptions in some papers, certainly, but largely they provide qualitative professional judgment.

The next step in the analysis spectrum entails seminars and workshops that represent interactions, information exchanges, or possibly even debate among SMEs. SMEs interact in this element to define problems and explore the available solution space.

The third step in the spectrum is what I call the sweet spot: where we are today in most irregular warfare analysis. This includes exercises, role-playing, and war games where SMEs actively participate in the exercise; they take their expertise and apply it to the issues being addressed through the exercise. This portion of the analysis spectrum emphasizes human factors in decision-making. However, you cannot obtain statistically valid results from a war game exercise of this nature.

The final element, and most quantitative, of the spectrum involves models and symulations (M&S) that can provide statistically valid results. This M&S activity has historically supported military work but also, in some cases, interagency problems. The dilemma is that we are not where we need to be today, as many panelists have highlighted, on the soft power side, and we do not have reliable M&S tools ready to provide results to help inform decision makers for complex operational environments. We have models that can do limited predictions for certain applications, but it is challenging today to use a tool that can predict how trends might evolve over only a couple of months, much less for a large-scale problem, that could span a couple of years.

We would like to be in this final phase of the analysis spectrum to inform decision makers with quantitative analysis. We are unfortunately still in the third step, where we are mostly getting insights from SMEs, who can be involved in very different ways. SMEs, in the desired final phase, would provide inputs to the model; then analysts would run the model, and the output. This final phase is less dependent on SME interactions and is more straightforward in terms of analysis. We need to get to this level of analysis if at all possible.

This lack of progression in this final step is difficult for engineers and scientists, who want to see statistically valid results that allow a classic “racking and stacking” of options. We spoiled ourselves over the Cold War years and the post Cold War in military problems because we used to present options that way (i.e., an analysis of alternatives and associated quantitative results) to decision makers to allow them to see the situation on a very objective, quantifiable basis. We are not there yet. Today, we are often-simply trying to inform decision makers and help them be aware of potential unintended consequences or results that defy conventional wisdom.

> *“The third step in the spectrum is what I call the sweet spot: where we are today in most irregular warfare analysis. This includes exercises, role-playing, and war games where SMEs actively participate in the exercise; they take their expertise and apply it to the issues being addressed through the exercise. This portion of the analysis spectrum emphasizes human factors in decision-making.”*

DATA

Traditional warfare data and information needs can hinder the ability to solve a military-on-military problem. Let us say we analyze a joint warfare-fighting problem in a very complex scenario. It is not easy to get the data, even though it is mostly physical, except for combat and control and “fog of war” issues.

In nontraditional, unrestricted warfare, we have all the instruments of national power trying to affect all the key aspects of an affected society in all operational domains (i.e., physical, cognitive, information, and social). It is daunting to consider the cross product of elements of power and components of the affected society, not only in terms of the sheer scope but also the fact that the focus is often more on the cognitive, information, and social domains and less on the physical.

There is a lot of soft power there, and we are receiving a lot of information that we are not even sure how to use. Therefore, the database requirements are very important. The only way to simplify it is to ignore Secretary of Defense Gates when he said, "Never neglect the psychological, cultural, political, and human dimensions of warfare," quoted in Eric Coulter's featured remarks. Neglect it at your own risk.

THE ENTERPRISE APPROACH

To advance analysis in complex operational environments, we need a more collaborative enterprise approach. There are a lot of areas for collaboration and knowledge sharing (e.g., information databases, data mining approaches, M&S techniques, analytic frameworks and processes, best ways to use SMEs, studies analysis, research scenarios, metrics, human behavior analysis, and interagency approaches. There are a lot of areas where we can learn from each other, and we occasionally get together to collaborate and learn in an ad hoc way. What we really need is a community of interest with a more disciplined, institutionalized approach.

Just on the DoD side alone, I have identified at least 40 organizations that are exercising irregular warfare analysis for their own purposes. They tend to loosely collaborate in an ad hoc way, sometimes at symposia or simply by making a phone call, but there is no formal institutional collaboration that really crosses all the service components and all the other players in DoD.

"I hope that the next time I attend a Military Operations Research Society conference that there are more than just two or three interagency participants, and I hope the next time the State Department has a meeting to discuss assessment techniques, valid metrics, or stability operations that there are a lot of people in uniform in attendance."

Looking into the interagency—whatever they have to offer as far as techniques and databases—the nongovernment, the foreign government, the foreign nongovernment, and international organization side, there are a lot of people who work in stability operations and irregular warfare who can really be major players in helping us to understand cultures, people, data, and information and to make valid decisions. However, we are not working on the analysis side as a community.

In November 2007, Secretary of Defense Gates said, "We also need new thinking about how to . . . integrate government capabilities with those in the private sector, in universities, [and] in other [nongovernment organizations] with the capabilities of our allies and friends." I hope that the next time I attend a Military Operations Research Society conference that there are more than just two or three interagency participants, and I hope the next time the State Department has a meeting to discuss assessment techniques, valid metrics, or stability operations that there are a lot of people in uniform in attendance.

I hope that we not only have that kind of meeting attendance but that we have formal ways to collaborate across agencies, including overcoming some of the classification issues. So let the dialogue continue, and let the enterprise begin.

PANELISTS

The panelists that we have for today are Dr. Matthew Levitt from the Washington Institute, who has some very good interagency perspectives, particularly from his time in Treasury and his Intel background; Mr. Andrew Caldwell, who is a U.K. exchange analyst in the Office of the Secretary of Defense and has led MORS workshops on irregular warfare; and Dr. George Akst, the Lead Analyst within the Marine Corps Combat Development Command.

6.2 THREAT FINANCE AND COUNTERRADICALIZATION

Matthew Levitt

INTRODUCTION

Before I discuss analytical support for threat finance and counter radicalization, I want to add one note to the discussion of the interagency issues John Benedict just presented. There is a lot to be said for the structure of the interagency, its ability to deal with the analytical challenges that we face, and its function at an integrated level to deploy people effectively within each other's agencies. When I was a Deputy Chief of the Treasury Department Office of Intelligence and Analysis (OIA), we had a very big problem. Some of our analysts—who we did not call liaison officers; we called them people who were deployed to the Combatant Commanders (COCOMs), in particular—were so well integrated that they were not able to perform properly at their professional development plans. Because they were doing the COCOM work so well, they were not necessarily doing the main work that Treasury required. That should never be a problem. We should

Dr. Matthew Levitt is a Senior Fellow and Director of The Washington Institute's Stein Program on Counterterrorism and Intelligence. 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. From 2005 to early 2007, he served as Deputy Assistant Secretary for Intelligence and Analysis at the U.S. Treasury Department, where he served as Deputy Chief of the Office of Intelligence and Analysis. During his tenure at Treasury, he played a central role in efforts to protect the U.S. financial system from abuse and to deny terrorists, weapons proliferators, and other rogue actors the ability to finance threats to U.S. national security.

find a way to enable people to progress within their own departments and agencies for the good work they are doing in their sister departments and agencies. That is a separate issue.

THE EXPANDED BATTLEFIELD

Instead, I want to focus on our need—our ability—to appreciate the challenges of providing analytical support within this expanded "battlefield." I put "battlefield" in quotes because we have an expansion of an unconventional asymmetric battlefield where non-military threats pose real immediate threats for the military. We are moving beyond the physical domain, and we have to focus on things that we did not necessarily have to focus on before.

Consider, for example, something tactical, such as the full spectrum of the means of finance—the raising, moving, laundering, storing, and accessing funds and resources. Frankly, that spectrum of finance is the same for licit and illicit finance: It is something that absolutely effects people on the ground in Iraq and elsewhere, but it is not necessarily something on which the military has the best expertise.

I want to provide an example of some shared interagency efforts on that particular example and consider some of the more strategic issues such as the problem we are facing today with radicalization, the need to develop robust counter radicalization plans not only to prevent people from doing the things they are trying to do today (e.g., blowing up buses), but also to prevent people from being able to do it tomorrow.

The Counterterrorism Equation

One thing we do not understand and appreciate—and therefore cannot conceptualize well enough—is that there are two halves to the counterterrorism equation. We are very focused on the first half—the tactical half—for all the right reasons; the tactical half includes all of the kill/capture operations, disrupting the flow of finances, etc., and that half is dealing with the threat today.

The strategy half is counterradicalization; it is the battle of ideas, strategic communication used in the battle for heart and minds (ideology, integration, opportunity, and a single narrative). Frankly, that is where we need to improve our efforts. We need to combine our attention, our capabilities, and our interagency authorities across both of these tactical and strategic challenges. We have very acute analytical challenges in providing support to these irregular issues—these unrestricted warfare type of issues.

At the Washington Institute, we recently completed two major studies. One was on combating terrorism finance, as an effort to focus on these tactical issues. As Bruce Hoffman mentioned in his address, "Terrorism–From IEDs to WMDs" (Chapter 1), we also led a bipartisan blue ribbon panel and produced a report on counter radicalization called "Rewriting the Narrative." Bruce was a member of that task force, and maybe that is why it was so successful, because of his membership.

The strategy half is counter radicalization; it is the battle of ideas, strategic communication used in the battle for heart and minds (ideology, integration, opportunity, and a single narrative).

Challenges to Providing Analytical Support

I will draw some examples from both of those studies. I will start with some of the challenges in general terms to provide the kind of analytical support we need in this environment. First of all, it is very hard to quantify or measure. How much money is there out there for terrorism? We cannot answer that. What percentage of the funds travels through the formal financial system? There is no real way to get a grip on that.

Lashkar-e-Taiba includes how many operatives? Of Hamas, how many people are members of the Al Qassam Brigade? What is more central to radicalization: the charismatic leader or the group identity? All of these are questions that we can deal with at a larger level, but trying to quantify them is very difficult. It is a problem not only of quantifying the extent of the problems we are facing, but also of quantifying the effectiveness of our solutions.

For our efforts to disrupt the flow of finances or to follow money for intelligence purposes, there are no good metrics. That is why the Office of Foreign Asset Control (OFAC) at Treasury has many lists of designations. The two main metrics analysts use to measure our effectiveness are both deeply flawed. One is how many entities have been designated and the second is how much money has been seized. They are both flawed for many reasons, not the least of which is that they assume that if you find a terrorism financier or someone who is engaging in proliferation finance or insurgency finance, you will necessarily designate them. The Treasury's authority is the one you will necessarily use. However, that is not the case. Within Treasury's tool chest are toolboxes and within those are implements. This is one implement, and it will not always be the right implement for every terrorism finance case.

You may want to run an intelligence operation, you may want to go toward a prosecution, or you may want to engage in diplomatic engagement or capacity building. To assume that you would use one particular tool and measure that just because it is the only kind of easily quantifiable thing is a cop-out; it is not an answer. We also need to pay close attention to the fact that this is a cross-disciplinary set of issues and requires all kinds of skills, including economists and anthropologists. We need to understand international financial systems, religious ideologies, and social challenges in many regions (e.g., the Paris suburbs).

"I can train a Ph.D. economist to be an all-source analyst, but I am not capable of training an all-source analyst to be a Ph.D. economist."

When Treasury set up the Office of Intelligence and Analysis, one of the things of which I was most proud was convincing people that we needed to hire not only all-source analysts, but also Ph.D. economists, because when the Under Secretary or the

Deputy Secretary asked whether we should use a 311 action to deny someone access to the U.S. financial system or whether we should designate someone's funds under executive order, what they needed to know was what might be the unintended consequences of using one tool as opposed to the other.

For example, in the case of Iran in proliferation finance, what is the impact going to be on the international oil economy? What is the impact going to be on the continued dollarization of the international oil economy? These are issues for which you need Ph.D. economists. I said at the time, "I can train a Ph.D. economist to be an all-source analyst, but I am not capable of training an all-source analyst to be a Ph.D. economist."

We need not only to bring in the right people to our agencies, but also to leverage the expertise we have at our sister agencies and departments. We need to understand all kinds of things that we did not have to understand before. Warfighters on the ground have been doing this for a long time, but people in Washington are only now beginning to fully appreciate the need to fully understand religious ideologies and social challenges—in the northern suburbs of Paris or outside London, for example—to fully understand the radicalization problems there.

Finally, we have to fine-tune our analytical expressions. The nature of the threat today is all about relationships. We do tend to utilize tools such as 1-2 link analysis and other diagraming tools to create wire diagrams and lines to this person and that person. How thick is any particular line? Is it dotted? Is it thick? Someone could draw a line between me and each one of you, even though I have not had the pleasure of really meeting most of you. How significant would those lines be? Would the line be any different for those of you I know well?

We need to find ways to be able to depict analytical nuance. For example, much like some of the 9/11 hijackers who apparently, according to the 9/11 Commission, traveled through Iran without having to have the proper travel documents or having their passport stamped, the cell that was involved in terrorism finance and prosecuted in Bahrain in February 2008, did the same.

They were able to go through Iran, to Pakistan, and the federally administrated tribal areas without the proper documentation.

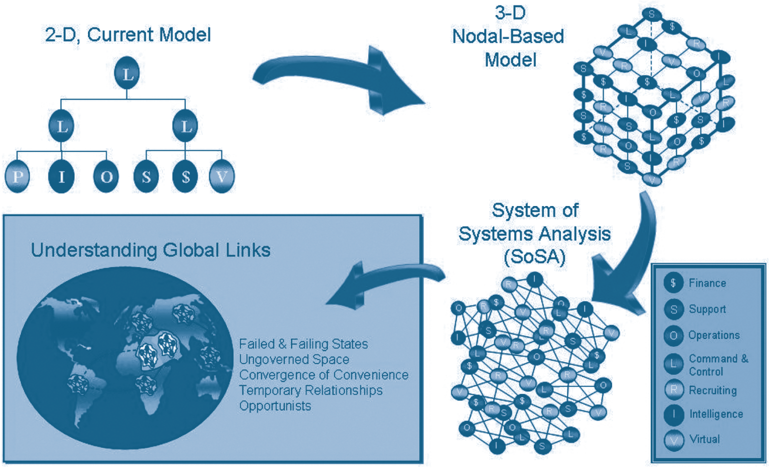
What does that mean about the nature of the Iran–al Qaeda relationship? On 16 January 2009, Treasury designated several al Qaeda senior leadership figures in Iran and declassified information about their close and ongoing ties to Iran's Quds Force and others. What does this mean about the Iran–al Qaeda relationship? It does not mean that Iran is now part of the al Qaeda inner core network that Bruce Hoffman described in his address, but what does it mean? Another example is the problem that the FBI and DHS are facing now with Somalia youth, not only in Minnesota but elsewhere, fighting with al-Shabbab, one of whom has become the first American suicide bomber.

What does this mean about radicalization in the U.S.? What does this mean about the Somalia community and how well it is or is not integrated? What it comes down to, among other things, is an analysis of social networks, which is an area where we do not have as good expertise as we should. When we examine all the levels within these adversary networks, we can generate diagrams with complex interconnections such as those for the 2002 Passover suicide attack on the Park Hotel in Netanya, Israel—the Hamas attacks that led to the Israeli reinvasion of the West Bank. The real issue is trying to figure out how significant is each line in that diagram, and what do they mean? We need to be able to fully flesh out and understand the nature of these interrelationships. If you think about the way terrorism used to be in a basic model, a hierarchical linear structure, and you think about it today as a nodal or system of systems, each one of those lines means something, but it is not equal to every other line. How do you figure it out? The lines may connect the following:

- Leadership
- Operational cells
- Recruiters
- Radicalizers
- Ideologues

- Logistical supporters
- Financiers
- Foot soldiers
- Unwitting supporters

We need to have an analytical system that enables us to get through all of these different things in a way that actually provides us the kind of information we need in a timely manner (Figure 1).



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 New Models to Understand Adversary Networks

COMBATING THE FINANCING OF TRANSNATIONAL THREATS

Take just two examples: one from the tactical side, counterterrorism finance, and one from the strategic side, counter radicalization. When it comes to combating terrorism finance, there are two different components, and sometimes they are mutually exclusive. The first is following the money, financial intelligence, up and down the financial pipeline to figure out who is giving the money, where it is coming from, where it is ultimately going.

Sometimes, you can actually have your Jack Bauer moment—very rarely—but, for example, following the money was one—not the only one' but—critical piece of the puzzle that helped thwart the liquid bomb plot at Heathrow. It is the reason when I fly to New York tomorrow, I am going to have to put my toothpaste in a little zip-lock bag.

All kinds of information come into it, including all sorts of intelligence, specifically financial intelligence, but also suspicious activity reports and currency transaction reports. The private sector can do a lot for us here in cooperation with the public sector. The *New York Times* did not do us any favors when they disclosed that the Treasury and others were doing something through the formal financial sector, looking at transactions that occurred through the international financial system, the terrorism finance tracking program. You probably saw the retraction they ran on page 522Z when they decided no, there really were not any abuses here. We can talk about that later if you like. Anyway, we can look through the formal financial sector. We could even look somewhat through the informal financial sector, e.g., via Hawaladar Registration. There are various ways to follow the money, and because it is a nonstatic target, we must use more and less sophisticated means.

Every time we take an action—and certainly every time we make a designation—we do declassify some information so that we can engage in a discussion with the public about what we are doing. However, we are also showing our hand a little bit. Our adversaries may become a little more sophisticated or a little less sophisticated. They will use techniques like trade-based money laundering. They will use payments through cell phones. Because of a human rights problem where people were bringing workers from South Asia to work in their homes and then just not paying them, the United Arab Emirates (UAE) decided that when you now register your worker for a visa, you also have to register your bank account and their cell phone and there will be an automatic deduction of the pay into their cell phone. That is great, but from a finance perspective that is also a vulnerability. It is much harder to get inside that type of a transaction. Terrorism networks will also use more tried and true methods such as cash courier techniques, which do not lend themselves to designation, for example, but might lend themselves to a DHS program led by U.S. Immigration and Customs Enforcement (ICE) on cash courier interdiction, which was done and which was very successful.

On the flip side is disrupting the financial flows: preventing people from either getting the money in the first place or much more effectively preventing them from being able to transfer and access the money that they may already have when and where they need it. For this you also need intelligence and you also need analysis, although it will be somewhat different in terms of identifying otherwise licit financial activity, trying to figure out the good from the bad; contending with state sponsorship, which is extremely amorphous when it comes to money, the fungibility of funds; measuring success; and dealing with the fact that there is so much activity now in the information domain through the Internet, etc.

> *"The New York Times did not do us all any favors when they disclosed that the Treasury and others were doing something through the formal financial sector, looking at transactions that occurred through the international financial system, the terrorism finance tracking program."*

The bottom line is—and this may be the most important point here, whether we are considering terrorism finance or any other case—there are various consumers, products, and burdens of proof. Consequently, there are going to be various demands on the same analysts. Treasury OIA only had so many people. In our shop, we were only getting so many new full-time employees a year, and yet we still had policymaker customers, and the intelligence community wanted finished products from us. It was very important to us to be able to do that, to be able to establish ourselves within the intelligence community. We had operators on the ground who were looking for our support too. Treasury and Central Command were, and remain, partners in the Iraq threat finance cell, which has now been so successful that it is being replicated in Afghanistan with the Afghan threat finance cell. I just had the opportunity on 11 March 2009 to testify on its effectiveness before the House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities.

A great example of how you get the right people in the right room—Treasury, the intelligence community, the military in the green zone doing a lot of very cool things to help our people on the ground—did not start off as quite so happy a situation. You had people on the ground who said, "look, this is my space in the green zone, you are in my space, you are going to do what I want," because they did not fully understand what this team could do if it was left to do the job, the mission that was assigned to it by the interagency.

CONFRONTING THE IDEOLOGY OF RADICAL EXTREMISM

We also have problems, not just from the tactical side, but also from the strategic side in terms of analysis needed for strategic counterterrorism. I think it is quite clear now that military force alone cannot defeat radical Islamist extremism. (The Secretary of Defense is probably not the first person to say this.) We need to engage in other types of soft power as well. It is really not soft power or smart power, but utilizing all elements of national power.

Putting in place a precise strategy to counter this threat and empower mainstream Muslims has proved challenging. We have new challenges. We are being asked to analyze how people are radicalized to violence. If you look at those people who have dropped out of terrorist attacks—e.g., Richard Reid's partner who did not get on the airplane to blow up an airliner across the Atlantic—what prompted them to drop out? Consequently, there is a tremendous focus now on multidisciplinary expertise. NCTC is now hiring psychologists and psychiatrists and experts from various disciplines to deal with this.

We have to look at the menu of factors, which are then coupled with an individual's personal experience. If we can identify the particular frustrations of that person in the north of London or north of Paris and see how they are plugged into a radical global narrative, suddenly their experience is just like what is happening in Gaza or just like what is happening in Kashmir. Figuring out the options available to those people who are being radicalized is a challenge in and of itself.

"It is really not soft power or smart power, but utilizing all elements of national power. "

We must analyze the roles of ideology on the one hand—radical ideology—and of failure to integrate on the other. In the U.K., they look at this as we do, for the most part, as both ideology and integration, but there is a premier role for radical ideologies. If you talk to the French, because of their constitutional issues they do not talk about this as a religious or ideological issue. They will only talk about it in terms of integration. When we called French officials about coming over to do some research for this study and we said we wanted to talk about counter radicalization, they said, "thanks so much, we do not do that." We called back two days later, the exact same person, and said, "We would like to come and talk to you about the ability to integrate communities," and the response was, "Absolutely, no problem." So we met with them and talked about counter radicalization, which they called integration.

Assessing how these radical groups are similar and how they are different and how they should be addressed is not only challenging, it is also causing a big debate within the academic community. Hamas and Hezbollah are not al Qaeda, but we do not see them as acceptable in this country, whereas the U.K. has designated the terrorist wing in the military wing of Hezbollah but has now announced that they are reaching out again and communicating openly with the political wing. What about Hizb ut-Tahrir and Tabligh Jamaat, which are not involved in violence themselves, but are conveyer belt groups that radicalize people to then engage in violence?

The second side of it is analytical support to the development of comprehensive counter radicalization strategies. How do we go about drafting an alternative to the radical global narrative? How do we go about getting that message out, whether it is in the virtual world or through our international media campaigns such as Voice of America?

"Just in case my message is too cheery, let us be clear that the problems we face today are not the most complicated we are going to be facing. They are only going to get more difficult."

Many strategic analyses must inform our ability to couple our counter radicalization efforts with democracy promotion, maybe even more importantly with anti-corruption promotion, with economic and political reform. That is very complicated.

How do you find credible partners? How do you engage with political Salafists who may espouse radical ideology but are against engaging in violence right now? How do you reach out—or do you reach out—to the Pakistani Taliban and the Iraqi Awakening? The FBI is now deciding whether it should or should not be working with the Council for American–Islamic Relations. These are difficult issues that need immediate analysis.

GLOBAL TRENDS 2025

Just in case my message is too cheery, let us be clear that the problems we face today are not the most complicated we are going to be facing. They are only going to get more difficult.

If you have not already taken a look at the intelligence community's "Global Trends 2025," the latest installment of "Vision 2015: A Globally Networked and Integrated Intelligence Enterprise," you should. It is available on line, and they have laid out not just a counterterrorism or even a threat document, but a comprehensive vision that looks ahead at what we are likely to face—and we are still going to be facing a terrorism threat, but it will be different. For example:

- **Demographics**: In 2025, there will be a projected new 1.4 billion people, thus creating a youth bulge and presenting increasing challenges.
- **Political Stagnancy**: The large population will require big amounts of energy, ensuring money flow to the Middle East, which could lead to a lack of fundamental change in the region.
- **Shifts in Wealth**: The transfer of wealth from West to East will continue, and oil- and gas-rich nations like Venezuela, Nigeria and Russia, will accrue large amounts of money.
- **Climate Change**: Water and food shortages will become major issues in 2025, and will greatly affect portions of the Middle East.
- **Nuclear Development**: The issues surrounding the Iranian nuclear program must be resolved, whether by a control regime, collaboration, cooperation, or through a nuclear arms race.
- **Terrorism**: Terrorism will persist in the Middle East, especially if the regional governments resist fundamental change and fail to meet the expectations of the youth bulge.
- **Alternative Models of Governance**: These models have begun to spread in influence, with China and Russia providing alternatives to democracy.

Whatever we have developed for today will probably not be sufficient for tomorrow. How are we as an analytical community in an era of constant change going to be prepared to deal with some of the things that we do not yet have to deal with; whether it is climate change or the impact of political stagnancy in key areas in the Middle East, or shifts in wealth, or the fact that over the next 25 years several key Middle Eastern countries are almost certainly going to have major political shifts, regime change that probably will not be bloodless.

"The near future will usher in new instabilities and new possibilities that will create a need for innovative thinking and analysis."

It is unclear what is going to happen over the next 25 years with Saudi Arabia, certainly with Egypt, and many of our key allies. So, we need to be thinking about many issues, and frankly I would argue that if we are not thinking about them today we are not going to be ready to deal with them in 2025.

Sometimes we are just thrown a curve ball. As I mentioned earlier, the New York Times exposed a program that the intelligence community and the Treasury were engaged in, which actually was not an intelligence program. The Treasury was serving an overt subpoena to Swift and its facility in Virginia that was highlighted by the successor to the 9/11 Commission as the ideal type of thing that we should be doing. The 9/11 Commission's public discourse project gave the U.S. government only one grade in the "A" range in terms of the government's ability a year later to start implementing some of the 9/11 Commission's recommendations. That was an A-minus on combating terrorism financing. It was not on the disruption side. It was focused more on the ability to follow information, financial intelligence: to look up and down that pipeline to be able to be proactive and disruptive. Sometimes, even when we are doing the right thing we are going to get thrown a curve ball.

FUTURE ANALYTICAL CHALLENGES

The near future will usher in new instabilities and new possibilities that will create a need for innovative thinking and analysis. I think we need a very comprehensive look at how we do analysis, because, still today, it is difficult to deploy one's analysts to another person's agency and enable them to succeed, even with all of the intelligence and terrorism prevention format reengineering that has gone on, and the fact that now, to become a senior analyst, you are going to have to go into someone else's agency. We do not yet have people with the full skill sets we need. We are still focused on the fact that we do not have enough languages, which is true, but we do not have enough disciplines either. We are so focused on the issues that are facing us today, which are acute, that I do not think we have any focus yet on the things that are going to be coming around the pike not just in 2025, but well before then as well.

6.3 ANALYSIS OF INTERAGENCY ACTIVITIES AND COMPLEX OPERATIONS

Andrew Caldwell

INTRODUCTION

Today, I will discuss analysis of interagency activities and complex operations. By complex operations, I mean operations such as those in Afghanistan and Iraq. In terms of how that fits into the focus of this symposium, I hope you come to comprehend my short history of the key moments of our problem-solving journey: (1) it took us awhile to understand that irregular warfare is not just a defense-related or only a military-related problem, (2) it is actually an interagency problem that we need new tools, techniques, and methods to properly prepare for and counter, and (3) there are actual tools, techniques, methods, and best practices that we have learned along the way, which probably apply to cyber and resource warfare.

THE TIMELINE

My first experience with realizing that there was a new problem out there was in 1995 as a result of Bosnia. We were tasked

Mr. Andrew Caldwell is a British Exchange Analyst currently working in the Office of the Secretary of Defense Program Analysis and Evaluation's Irregular Warfare Division. An engineering graduate in Materials Science, Andy spent the first three years of his career at British Steel as an Operations Research Analyst. Andy moved to the Defense Evaluation Research Agency (now Defense Science and Technology Laboratory) in 1997. Before joining the DoD on exchange, Andy was responsible for 30 analysts providing U.K. force structure advice to the Services. He is an Associate Fellow of the Operations Research Society and is currently enrolled in George Mason's Peace Operations MSc. He is scheduled to return to the U.K. in May 2010.

to look at the deployment of military forces in support of coalition forces that were already in the country at the time. We actually did not have any tools to deal with that; it was a new problem. The alarm bell goes off, why did we not see this? Why is there not something on the shelf that we can use?

In that particular case, we adopted a commercial war game, called Silver Bayonet, a Vietnam-based game. That, however, was the first warning sign that there was a new problem out there, rather like cyber or resource warfare that no one had really tried to tackle, certainly in the last 10 or 15 years prior to this period.

Then, in 1996, the Cornwallis Group was formed. Seeing as this is a predominantly U.S.-based audience, I feel I need to point out this group has nothing to do with the Cornwallis that lost the War of Independence. This group is actually named after his father, who has some Canadian links. The formation of this group was an opportunity to bring practitioners, academics, and people who worked in government and non-governmental organizations across DoD and other departments together to present papers and discuss issues for about a week every year.

This annual meeting continued for approximately nine years, until 2005, and it was the primary mechanism by which people in this community actually came together and talked about analysis products. My observation today is that if there is not something like this in cyber warfare, you need to start one. In 2004 or 2005, there was a critical mass of analysts from all walks of life coming to tackle these types of problems. Certainly in the early stages, a lot of heavy hitters had either presented at Cornwallis or at least been part of the group.

Let me move back to the year 2000 for a moment. The first simulation model of peacekeeping tasks, called Diamond, included diplomatic and military warfare in a non-warfighting domain. This model was the first to look at more than two sides of a conflict; we could model a non-governmental organization. We modeled the population and then could interact with it.

Now, just to mention briefly, fast-forward to 2007, when the Military Operations Research Society (MORS) acknowledged irregular warfare as a mainstream problem. This is a key community; it is not just a fringe group.

Finally, in 2008, the Africa-scenario analysis was a dedicated attempt by Office of Secretary of Defense Peaceful Nuclear Explosion (OSD PNE), the Joint Staff, and a few others to throw half a dozen different tools into looking at an interagency problem. Of those tools, maybe only half actually modeled military forces. The others looked at elements like corruption and negotiation stances. This was analysis done to form military planning and decisions, but also predominantly to deal with interagency issues.

So it has been a long journey over those 14 years, and it is not over yet. We have talked about some of the limitations in dealing with the interagency analysts; they do not have the same critical mass as we do in DoD. But that's been a long journey.

FRAMEWORK FOR INTERAGENCY ASSESSMENT

A number of authors have looked at frameworks for analyzing these issues. I remember, in 1999, the first time a study group put some ink in front of me. They divided this problem into a pie chart with three pieces: military, diplomatic, and economic. You cannot solve the problem just from the military perspective; we have to solve it from an interagency perspective.

We did not know what went in the economic or the political slice of the pie chart at the time, but since then, there has been a lot of work trying to develop a good framework. I will define framework here as a vehicle where if you address all the components within that framework, you pretty much covered most of the problem.

The Measuring Progress in Conflict Environments (MPICE) initiative is a fairly good framework. If you can address all the problems in those particular areas, you probably have a good framework for your analysis at the interagency level. My question to those looking at cyber warfare is: what is the framework for your analysis? Is it .mil, .gov, .com, or .other? Is it the finance sector? Is it the military or power generation sector, or perhaps it is cyber offense, cyber defense, resilience, and redundancy?

I am fairly confident that the MPICE initiative is the right framework for us to look at interagency problems, but what is the right framework to look at problems within resource and cyber warfare? A final observation is that there are three future actions: we need to (1) reduce the drives of the conflict, (2) take the problem away or reduce it as best as possible, and (3) increase our institutional capabilities in each of those areas to deal with any particular conflict. We have seen examples: looking at al Qaeda, you want to remove those individuals or groups that are currently militants and extremists fighting us, but you also want to remove the reasons why people want to join al Qaeda, which removes the drivers of the conflict, and has the capacity and depth to deal with the overall problem.

"My question to those looking at cyber warfare is: what is the framework for your analysis? Is it .mil, .gov, .com, or .other? Is it the finance sector? Is it the military or power generation sector, or perhaps it is cyber offense, cyber defense, resilience, and redundancy?"

USEFUL TECHNIQUES

I have picked six techniques, presented in Figure 1, that have been used or are being used to look at analysis of interagency issues in complex operations. The key point to remember when reading the table is to look from top to bottom because you increase your ability to forecast outcomes; you can look farther into the future. However, inversely your confidence in what you are actually predicting or forecasting decreases rapidly. Right at the top is quantitative data, which include government and United Nations statistics, child mortality rates, or the economy and the Gross Domestic Product. These figures normally lag about a year behind. Consequently, you are looking at historical trends if you are using that kind of information.

Polling and surveys are a good way to get at what people are thinking. Again, though, you are really looking at what they are thinking at the time of the poll. You can ask future focus questions, such as how would you vote if there were an election now? However, answers do not necessarily properly represent time-sensitive issues.

	Analysis Method	Description	Examples
↓	Quantitative Data	Collection of input/ output data associated with activities and generic country indicators	Country indices on corruption, economic growth, security, etc.
	Polling and Surveys	Public opinion or opinion of targeted groups	View of the U.S. before and after USNS Comfort port visits to South America
	Content Analysis	Survey popular media for identified themes	Failed States Index (Fund for Peace)
	Historical Analysis	Analysis of quantified data describing the actual behavior of systems across a wide range of historical cases	Success/failure factors in counterinsurgency operations
	Expert Opinion	Subject-matter Expertise and Focus Groups	Combatant Command Theater Security Cooperation Working Groups
	Modeling/ Simulation and Gaming	Simplified representation of a complex system	COMPOEX

Figure 1 Six Useful Techniques

Content analysis is an interesting technique; it is under used. You look for key themes in a range of media publications, official documentation or other sources. For example, if you wanted to look at consumer confidence to spend money in the U.S. economy, you could survey all the media in the U.S. for phrases like "foreclosures up" and "unemployment up," which are indicators of a declining consumer confidence, at least media reported confidence, in the requirement to spend money. Then, you can look for positive phrases, such as "job gains" or "pay rise" in a particular industry.

Historical analysis is an interesting technique, also under used. Historical analysis describes the actual behavior of a complex system, but it does not provide reasoning for such behavior. For example, I can tell you that if you put a British rifleman on the foreign range and he can hit 100 targets on that range, if I put him in an exercise and he only hit ten of those targets, you will actually only hit one in combat operation. I do not know why the degradation factors are 100 to one from the range to the actual combat environment, but once I know that number, I can put it into a model to create computer-generated forces, calculate their range, calculate the number from the firing range, divide that by 100, and determine the probability of a hit.

Dr. Andrew Horsack's work in counterinsurgency operations is a good example of how historical analysis can track enduring, key factors. We talk about hearts and minds; do you know what having the number behind hearts and minds adds to your side? If the populations support you, and populations support the government in a particular counterinsurgency operation, those hearts and minds act as a force multiplier of 40 for your activities. The opposite is also true if they support the insurgency, which is why we have trouble dealing with small numbers of terrorists, hundreds or thousands ties down hundreds and thousands of our troops.

"Maybe the target we should be aiming for is validation in some of these complex systems. The same principle applies to the economic stimulus plan; we have tossed that coin three times now, at a trillion dollars a toss. It would be nice to have some confidence that it will come up tails if we have to toss that coin for a fourth time."

One of the problems with historical analysis is that you always come back to the question: how can history always be a predictor of the future? My rifle range example is true for the rifle barrel, and that is still current technology used today. If we replace the rifle barrel with a direct energy weapon in the British infantry, would that factor still be true? I do not know; that touches on the different issues with historical analysis.

I mentioned a little bit about expert opinion earlier, it is still one of the main techniques that were used to tackle some of these complex issues. There are a lot of different ways to use subject-matter experts other than to put them in a room and tell them to discuss national security. There are other techniques that can allow you to have more or less confidence in your subject-matter experts, even in terms of selecting potential subject-matter experts.

Certainly within DoD, if anyone from the State Department turns up to one of our war games, we are really pleased. It does not matter what they do in the State Department; we say we have a subject-matter expert, which may actually not always be the case. I will not talk a lot about modeling, simulation, and gaming. It is, however, a technique with a lot of potential.

MEASURING PROGRESS

Your structure objectives should include a context, an object, and a direction; that is from Ralph Keeney's book *Value Focused Thinking*, which has been used the last 15 years or so in a lot of DoD analysis. Let us say your object might be drugs; the context might be drug trafficking from Columbia, and the direction might be reduced drug trafficking from Columbia.

This example objective may seem simple, but when you start to get into interagency problems, your objectives start to get very complicated: which agency is in the lead and which is supporting? Are you supporting the overall objective? Are you just supporting part of the objective? It is very easy for strategy staff to get tied up in building very complicated objectives, but it does not really help the analyst when he/she measure potential success.

How to write and measure objectives is the 101 guide, but it is important to understand the difference between inputs, outputs, and outcomes in your system. A good example is an output-based focus in Iraq, going back four or five years when the target was 70,000 megawatts of power generation. That is an output measure. We focused on that at the expense of the outcome, which is what we really want to improve power generation in Iraq, so people were content with that.

Minimize the number of items that you need to measure. I say opinion differs. There are a lot of people that will tell you a way to direct hundreds of different measures. However, I have always viewed that as a menu to choose from; never try to apply the whole thing. I call it the rule of five. I do not know if there is any empirical evidence to support this, but whenever I see an objective, if someone wants to add activities, each objective tends to generate about five sub-activities on average. If under an activity, you want to create measures, each activity tends to generate about five measures. You can see, if you have 30 objectives, how very easily you can end up with a complicated number of measures. It is very difficult for a decision maker to deal with a large number of measures. You really have to focus on the key ones that tell you enough about the system.

A legitimate measure can be listed as "do no harm to related objectives." For example, if you are in a stabilization operation and wanted to improve security, you are given two options: you can either patrol or you can institute a curfew. Looking exclusively in the security area, the curfew option is the more effective way to gain security.

> *"Certainly within DoD, if anyone from the State Department turns up to one of our war games, we are really pleased. It does not matter what they do in the State Department; we say we have a subject-matter expert, which may actually not always be the case."*

However, if you think about it politically and economically, that will damage those other objectives; if people cannot leave their houses, then they cannot trade or improve the economy. If they cannot leave their houses, then they will perceive you as an occupier, rather than someone there to protect, which will damage your political legitimacy. Therefore, measuring an objective and ensuring that it does no harm to other objectives is a legitimate measure, looking for the nil effect.

The real world is easier than the simulated world. As a community, roughly over the last 60 years, we have become very comfortable in coming up with fictitious countries and corresponding fictitious peoples and enemies. Because we do not understand the relationships in these complex environments, the minute you create a fictitious country and two fictitious people that maybe do not like each other, you have already created two assumptions that will dwarf any other analysis or variables that you might change in that analysis. Referring to real world data when and where you can will be much more useful in the early stages.

BRINGING IT TOGETHER

We learned earlier, through Jim Locher's presentation, how Czars do not work. Lead agencies do not work either, and departments tend to be capability-focused, rather than mission-focused.

I will offer an observation from the United Kingdom about one way we tried to tackle the requirement for issue teams. The Stabilization Unit is a mix of 30 personnel drawn from the Department for International Development, the U.S. Agency for International Development, the Foreign Commonwealth Office, the State Department, and also the Ministry of Defense. I would really describe them as a dating agency; their purpose is to introduce people from different agencies and departments in an effort to get them to work together. They know enough about what is going on in those other departments that they can do this effectively.

Certainly, when you have an interagency meeting and there is someone from the Stabilization Unit, you are reassured because you have a neutral referee in the room. Although they have no authority to tell you how it should be done, just having them there to, for example, simply translate from Department for International Development language into Ministry of Defense language is a very useful tactic.

"Therefore, measuring an objective and ensuring that it does no harm to other objectives is a legitimate measure, looking for the nil effect."

The Stabilization Unit is supposed to focus on any United Kingdom-related stabilization issues. Because of demand of operations, 95 percent of their time is dedicated to Afghanistan. You could almost view that as an Afghanistan issue team, as a potential template for what Jim Locher was suggesting we do.

Analysis of Complex Environments

Cause and effect in complex systems will continue to be elusive. This is every Prime Minister and President's number one issue in the world. We have Nobel Prize winners, and the will of the entire population on this planet, working to solve this issue. All we need is to get people to spend more money.

It sounds simple, does it not? However, it is a complex environment, and as a result, we cannot quite work out which levers to pull to make it work. That will continue to be elusive for some considerable time. As analysts, you want to break everything down into two or three simple factors that dominate any particular decision or outcome. However, we just need to accept that it will be uncomfortable for us and we will not be able to determine a cause and effect for quite some time, if at all.

We have also been conditioned for years to think that we understand traditional warfare by breaking it down into those two or three variables. For example, in an air-to-air combat simulation, we might look at who sees whom first and the range and type of the missile. We might think these are the three most dominant factors in an air-to-air combat, but somehow we inadvertently removed training as an issue. I would suspect that in real world engagements, the lack of training in the pilots, that we have come up against and shot down as a result, is probably the biggest issue. It is perfectly legitimate for us to see another way because we have assumed that worst-case pilots are as well trained as our own. In the real world, that is not the case. Maybe we lost sight of the fact that there is a bigger variable in this that we no longer consider analysis.

Let me give you another example that relates to resource warfare. In World War II in August 1942, the British Navy needed to run an urgent convoy to Malta, considered then a thorn in Hitler's side; he could not take it, and without it, we had some ability to conduct sea denial in the Mediterranean. August 1942 was a rough time for us; things were not going as well as they should have been for us. Malta was about to surrender if we could not resupply it.

"Cause and effect in complex systems will continue to be elusive. This is every Prime Minister and President's number one issue in the world."

The analysts looked at that problem, and they came to the conclusion that if you loaded the ships so that every ship took a little bit of everything, you would only need to get two ships (i.e., one tanker and one dry store ship) to Malta to make it hold out, covering ammunition, cement, medical supplies, aviation fuel, petroleum, diesel, etc. They decided that 14 merchantmen would be enough to guarantee that at least two got through, with an escort of 44 warships.

That was a dangerous run. I think, in the end, only five merchantmen actually made it to Malta. We lost an aircraft carrier on the way, but it was important. They had done their operation analysis part well. They did not fight. How many vessels could we afford to lose to have some guarantee of getting vessels through?

As long as any two got through, one tanker and one other ship, then we would be fine.

A sobering thought, but 40 years later, in the Battle of the Falklands, the Atlantic conveyer was hit by a missile and took all but one of the British Army's helicopters that they were going to use to conduct air maneuvers on the Falkland Islands with it. Consequently, this impacted our fighting technique. We had to load troops on auxiliary landing ships and move them up the coast; one or two of those were hit during the battles, and we lost a lot of people as a result.

You would think, 40 years later, that we could identify a lesson learned about how to build convoys, but we had forgotten that lesson. Do not assume that the operations research in your community on cyber or resource warfare considers those techniques that we learned 60 or 70 years ago. We tend to forget about the simple techniques, but they can be very powerful.

Imagine gaming in the 1950s and 1960s and how we used nuclear escalation. It was one of the most useful techniques, but it was very hard to get anyone to escalate. Whenever you put anyone into any scenario, they immediately try to de-escalate, even if they are wearing the red hat, which says a lot for employing rational actors to be in charge of our nuclear arsenal. That is a good thing, but it was not very good from an analytical perspective. In the end, they had to start a scenario with phrases like "There are 100 warheads bound to the U.S. What do you want to do to get people to go to the escalatory stage?"

"Do not assume that the operations research in your community on cyber or resource warfare considers those techniques that we learned 60 or 70 years ago. We tend to forget about the simple techniques, but they can be very powerful."

We have come a long way with gaming since then; we have learned, for example, that if you want to get at those sorts of issues with non-rational actors, you need to employ role players who can really get into character. You need to profile the cultures or the particular individuals you are trying to represent to effectively read and play into that role.

And then you will get a more interesting game. And if you cross out nuclear escalation and put cyber escalation there that's a potentially powerful technique that we could use to identify who would do what, when, and what our responses would be.

As analysts, we are always looking toward being certain about our results so you can say, "You can hang your hat on that result." Maybe the target we should be aiming for is validation in some of these complex systems. The same principle applies to the economic stimulus plan; we have tossed that coin three times now, at a trillion dollars a toss. It would be nice to have some confidence that it will come up tails if we have to toss that coin for a fourth time.

6.4 ANALYSIS SUPPORT FOR UNRESTRICTED WARFARE

George Akst

INTRODUCTION

John Benedict, in his moderator's summary, discussed symposia like this and how there is usually little interaction, so I thought I would mix this up a little and inject more human interaction into my presentation. Let me start off with a question for you to consider. I am confident that I know what unrestricted warfare "is not" because of the terms used to describe it: unrestricted, irregular, nontraditional, asymmetric, and operations other than war. The real question is: do we know what it "is"?

THE CHANGING NATURE OF CONFLICT

When we discuss unrestricted or unconventional warfare, we assume that the nature of conflict has changed and that we are moving from one aspect in which we understood the nature of conflict and how to analyze it to a new form of conflict. Certainly,

Dr. George Akst is the Senior Analyst for the Marine Corps Combat Development Command. He also provides oversight of all Marine Corps analytical modeling and simulation efforts. He entered the Federal service in 1998 as the Deputy Director of the Studies and Analysis Division, where he managed all studies and analyses performed under the Marine Corps Studies System. Dr. Akst graduated cum laude from the City College of New York and received his Ph.D. in Mathematics from the University of Illinois in 1974. He also graduated from the Engineer Officer Basic Course at Fort Belvoir in 1972. Dr. Akst's decorations include the Department of the Navy Senior Professional Meritorious Presidential Rank Award, Navy Superior Public Service Award, USMC Certificate of Commendation, and the Center for Naval Analyses Phil E. DePoy Award for Analytical Excellence.

as analysts, we understand the kinetic aspects of operations that underlie conventional warfare, beginning with Lanchester's equations and included in the various types of campaign models. However, analysts today must focus on counterinsurgency and radicalism, sociological, religious, and cultural factors. In fact, the 1940 *Marine Corps Small Wars Manual* describes exactly what we are currently focused on, in terms of nonkinetic, human factors within this new type of warfare, where it states, "Strategy should attempt to gain psychological ascendancy over the outlaw or insurgent element prior to hostility." Secretary of Defense Gates stated a similar focus in a recent article. Perhaps the nature of conflict has not changed as much as many think, but our analytical focus has shifted from the kinetic to the non-kinetic types of conflict of concern today. The Marine Corps was very concerned with understanding and defining this type of warfare dating back to at least the early parts of the last century.

We need to look at the kinds of challenges we face today from a different perspective. We need to think out of the box and ensure that conventional thought processes do not burden us. As analysts, we need to focus outside of our comfort zone.

AKST'S AXIOMS

I am about to unveil, for the first time ever, a set of five axioms that, I purport, characterize analysis, modeling, and simulation in the context of unrestricted warfare.

It's Not Your Father's Enemy

This new concept of conflict, which we discovered might not be so new after all, does not conform to the kind of thinking, types of battle, or sorts of objectives that analysts have applied to conflicts in the past. We must begin thinking about some of these problems from the enemy's perspective. I have heard many people talk about the kinds of "irrational" enemies we see today, whether it be Hezbollah, al Qaeda, the Taliban, or others. They may be irrational from a U.S., or Western, perspective, but I do not think that they are at all irrational from their own perspectives.

There is typically a rationale and motive for why groups and individuals act the way they do. It is critical that we understand that rationale before we try to solve these problems with analysis. The way I like to think about working within unrestricted warfare analysis is to start at the strategic level and determine our key objectives. Many have criticized U.S. efforts in Iraq because they say we have not thought through some of those long-term strategic objectives as carefully as we should have. We must ask: what are our objectives? What are the insurgents' objectives and what are they trying to achieve? Only then can we begin to work our way down to the operational, military objectives, and the tactical analyses required to address the type of questions we are being asked. Only then are we able to develop measures of effectiveness (MOEs) to meeting those objectives. As analysts, we are constantly asked to develop MOEs, but we must first answer the question, "what are we really trying to measure . . . what is our ultimate strategic goal?"

Focus on the Model . . . Not the Simulation

A number of years ago, I became much more involved in modeling and simulation when I began representing the Marine Corp on the Modeling and Simulation Steering Committee within the Office of the Secretary of Defense (OSD). I have since become very careful about distinguishing between models and simulations—I believe many people often use these terms interchangeably.

A model is the underlying methodology for describing a relationship; for example, $E = mc^2$ is a model developed by Albert Einstein to find the energy in matter; you multiply the mass (m) by the square of the speed of light (c = 300,000 kilometers per second). The equation $P_k = P_h \times P_{klh}$ is the "model" for calculating probability of kill as a function of the probability of hit and the probability of a kill given a hit. How you implement that methodology with computer software, such as an Excel spreadsheet, is the "simulation." All too often, analysts jump into building simulations without completely understanding the underlying models and methodology upon which they are based.

As an analyst, I often hear: "Why can't you guys build a model of Iraq, or build a model of Afghanistan, or build a model of irregular warfare?" My retort is simple: "We will build a "simulation" (which is what they really meant) as soon as the community understands the underlying methodology (i.e., "model")." Senior level decision-makers appear to view a computer printout or the results of a simulation as much more valid than scribbled notes on the back of a piece of paper. However, I would argue that until I know the goals and objectives of the operation, it is virtually impossible to build a conceptual model and underlying methodology, and certainly not a simulation.

Ultimately, I think we need to take a step back from generating computer simulations and work more with our interagency partners to define, understand, and build the necessary underlying models. Unfortunately, there is a lot of activity in the analysis community building simulations, and not so much in terms of building models.

It's the Data, Stupid

In 2008, I wrote an article for the Bulletin of the Military Operations Research Society entitled "It's the Data, Stupid." In that article, I discuss my discovery that we build many models without regard to the data requirements of those models. Analysts tend to worry about the data later, often inserting modifiable parameters or factors, like dials, into the model, so they can dial a variable up or down to see the effects of varying a particular parameter.

Unit cohesion and leadership are two parameters inserted in this manner in several models. As one dials up leadership, the force becomes more effective. But how are we going to get the leadership value for a particular unit? What is the value for an Afghan unit versus a U.S. unit versus a British unit?

My contention is that before you begin to build these simulations, or even build the underlying conceptual models for the simulations, you either need to have the data, or have a good idea of how you will ultimately get the data. I think many in our community are looking at this the other way around, so I may be called a heretic for saying: worry about the data first, and about the model and/or the simulation second.

"If we build models for which we have neither data nor the means to obtain the required data, I would contend that these models are useless."

The data for irregular warfare models are very different than data we have traditionally used, and that is okay. The level of rigor, from the perspective of a seasoned analyst, may be very different, but we still need to be able to get at the data. For example, we may need to obtain data through a rigorous polling of subject-matter experts, as opposed to performing field tests to determine P_ks. If we build models for which we have neither data nor the means to obtain the required data, I would contend that these models are useless.

Processes Themselves May be Changing from Deterministic to Stochastic

Older analysts, like me, talk about simulations or models being either deterministic or stochastic in that the approaches that we use to model inherently deterministic processes are either deterministic or stochastic. When you shoot a bullet at a target, that bullet is either going to hit the target or it is not—it is a deterministic process.

Now factor in all the complex variables involved in determining the probability of hitting the target—how much jitter there was when you pulled the trigger, how accurate was your range estimation, what environmental factors affected the bullet? We can accurately estimate the overarching probability of hitting the target by using rigorous testing methods. This may be implemented in some models deterministically, accepting fractional losses. Others prefer to model this stochastically. Both are reasonable approaches to modeling this essentially deterministic process.

With some of the processes involved in unrestricted warfare, I question whether the processes themselves have changed from deterministic, like the bullet, to stochastic. For example, is the outcome of handing out lollypops or bags of grain to "win the hearts and minds," and gain U.S. sympathizers, pre-determined (i.e., deterministic)? Is there a way of knowing for certain, accounting for all the possible factors and all of the data, whether or not that lollipop or bag of grain will turn that person into to your side? I would argue that perhaps it is like the flip of a coin; the process itself may very well be stochastic, and consequently, we may never know in advance whether it will "convert" that particular person or not.

Most Analyses are Not Predictive

I wrote down a note from Andrew Caldwell's talk on the ability to forecast outcomes. "Cause and effect in complex systems will continue to be elusive." I have been an analyst for 30 years, and my story has not changed, even though the elements of the story may have. On every project that I have ever worked, whether it is a model of small unit tactics, operations, and outcomes, or determining the number of Marines that were killed in an operation, or how far the enemy moved, the results were not predictive.

Let us talk about casualties as an example. DoD produced many models and simulations leading up to Desert Storm, and we had a number of predictions for casualties. The order of magnitude of those predictions was in the tens of thousands, and we were off by many orders of magnitude in this case. Such traditional analyses, whether at the tactical level or at the campaign level, are not predictive. It is not the purpose of all analyses to predict or to forecast outcomes, and this is clearly the case with much of my analyses. Much of the purpose of analysis is to provide the decision-maker with a menu of alternatives and some relative impacts for each possible solution. I want to emphasize the word "relative." The fact that such analyses are absolutely not predictive is even truer now in unrestricted warfare.

We need to ensure that the decision-maker understands that when we produce results from new models, we may not be contending that models predict the future outcome. Rather, they may simply provide a relative sense of value for different alternatives, force structures, weapon system combinations, tactics, or other actions.

"It is not the purpose of all analyses to predict or to forecast outcomes, and this is clearly the case with much of my analyses. Much of the purpose of analysis is to provide the decision-maker with a menu of alternatives and some <u>*relative*</u> *impacts for each possible solution."*

CONCLUSION

I hope these simple axioms provide you with a new and different way to think about analyzing unrestricted warfare. While this may appear to be strange and unfamiliar territory to many of you, just follow your instincts as analysts. Try to think outside the box on occasion, and put yourselves in the mind of the enemy from time to time. Don't find yourselves shackled by the conventional wisdom of traditional analysis. And above all, ensure you first strive to fully understand the problem, and the data needed to address that problem, before you jump feet first into the solution.

6.5 QUESTIONS AND ANSWERS HIGHLIGHTS

Transcripts

Q&A

Q: What can the Pentagon do in the new Quadrennial Defense Review (QDR) to boost the analysis community's ability to support interagency efforts and better address the threats tied to unrestricted warfare?

George Akst – We have strived, in a number of recent study efforts, to try to be more inclusive with the participants in these study efforts. We want to get people from the U.S. Agency for International Development, the Treasury Department, the State Department, and some of the various interagency organizations that really do play in the overall outcome of these operations.

If we are truly serious about involving and cooperating within the interagency, we need to be more embracing and more inclusive of the interagency partners in the individual efforts during the QDR. I have seen methods for producing QDRs range from somewhat moderately open analysis into much like a bunch of seniors in the backroom with a lot of analysis. The suggestion I have is the more open and inclusive we are, the better and more inclusive the analytical efforts will be that underlie the next QDR.

Matthew Levitt – From the perspective of the small agency that receives these requests, the Treasury Department only has so many analysts—they get requests like these all the time—and wants to participate but often cannot because its own management has immediate analytical demands; there just are not enough people.

Often, what you hear is, "I have four people detailed out to the Commands, and they will be the people to do it." However, they are actually detailed to the Commands and are hopefully doing the job tasks that the Command needs them to do. It is difficult for the Command to remove these people from the analysis they are doing. Therefore, we should begin the discussion for the request for this input as far in advance as possible. I would often receive requests for next week to send someone for a day or two, which is unrealistic because usually this person is working for the Secretary or the Director of National Intelligence; it just cannot happen right away.

Also, often when you are dealing with different and smaller departments and agencies, you simply have to make it clear how this impacts them as well. Usually we are supporting the Pentagon, but we need input from other people, and it is not made clear how a temporary transfer will impact them as well. We have been talking about leveraging all elements of national power (i.e., soft power, smart power).

Andrew Caldwell – I cannot comment on a QDR, but I can comment on British defense reviews, which have always worked well because they take place at senior levels. The cabinet secretaries have come together and worked cooperatively to identify how British defense policy supports the work of departments for international development and, for example, the Foreign Commonwealth Office.

One of the key problems that we always run into is when the Ministry of Defense processes focus on long-term planning, which does not always fit easily into these other departments. That is a very difficult issue because if you want to hand off part of the ownership to the problem to someone else, you need someone that actually has resources to handle it. That is where we always come unstuck. It can work very well at the strategy level, but it does not actually work so well at the working level because our departments simply do not match up like jigsaw pieces in the way that we want them to.

John Benedict – Quickly from my perspective, I am involved in a study on irregular warfare for OSD intended to inform the QDR, but with only limited interagency participation. It was difficult to recruit interagency people because they are very busy and they do not have some of the capacity to handle these issues.

The main point I want to make is that with their participation, we did go beyond other organizations, as far as informing the QDR, and we talked about authorities and policies that would enhance interagency collaboration, including planning and potential analysis. We are trying to get it up to the QDR level, but it remains to be seen whether it will survive that drill.

Q: *Matthew, you talked about some of the financial intelligence tools that are being used in the money and banking system (e.g., cash transfers, wire transfers, cash carrier, hawaladars, and so forth). Do we have any tools that are being used to monitor capital and commodities markets, stocks, bonds, derivatives, etc?*

Matthew Levitt – The simple answer is no, which does not mean that it is not being done, but not as such. First of all, there is a technical capability in terms of the ability to see those things real time. Secondly, there is a difference from the national security side, which is where I sat, of not dealing with the Bernie Madoff side, dealing with what you actually see and know to be current threats and vulnerabilities.

There is a difference in the way the government traditionally, for better or worse, deals with these issues. There are the people who deal with the known threats right now, and there are people who think through the vulnerabilities and how to deal with them. Everyone is dissecting these issues, but not necessarily from the national security perspective.

Q: *In light of modeling forecasting in complex environments, how do we tackle benchmarks or milestones in Afghanistan, in Pakistan? What benchmarks do you recommend we measure?*

Andrew Caldwell – That is a great question. I do not have a great answer, unfortunately. My philosophy is to tackle issues that are easy to measure, by minimizing the amount of resources you need to measure, but really get at the heart of the problem. For example, if I were looking at Afghanistan, I would focus on freedom of movement, safety and security where people are living and what threats they face, and what level of intimidation for murders that might reside in that particular area.

The reason why I would just focus on those elements is because everyone has freedom of movement to conduct trade and participate in the political process. Also, if they are safe in their houses, then they have safety and security in those environments.

Although this information does not tell me what is going on and why the problems are getting better or worse, it does at least simplify what I am actually measuring, as opposed to analyzing 150 measures and then trying to aggregate that into a question: are we safe or secure in this environment? If I measured these components and discover that the trend is heading in the right direction, although I may not put my finger on what we are actively doing to make it go in that direction, I would have some confidence that we are in fact moving toward turning the situation around in our favor.

Matthew Levitt – I agree. To me, the question is too broad. You really have to ask what part of Iraq or Afghanistan you are trying to measure. You could have a whole set of measurements in the security side and on the political side. I would ask: what are the key issues and critical areas within each of the components you are most interested in? I am not a big fan of trying to measure democracy promotion.

We did a study on political reform on the Arab world and met with a group of reformers within the Arab world. One of the questions that we asked them is, "Do you think the U.S. should be tying foreign assistance to democracy promotion? They said, "No way; they should be tying it to anti-corruption because it is very difficult to measure democracy promotion." However, you can actually measure anti-corruption programs and the space that anti-corruption programs provide, which enables democracy promoters to thrive.

On the security side, for example, in Afghanistan, one of the biggest problems we have is narco trafficking, and not just the actual production, but then where is it going to market? There is a legitimate market that is primarily cornered by Turkey. Can we open some of that up for Afghanistan? Simply trying to destroy all the poppy fields is not going to take care of it. In particular, what can be done for the issue of freedom of movement to secure roads?

A large amount of the Taliban control of the narco industry is not because they control the fields but because they control and toll the roads as well as the security for people in those areas. What are the small niches you can focus on within the areas that you are most interested in analyzing?

George Akst – We need to ensure that we do not just gather together concepts that we can measure for the sake of measuring them. We need to link them to the overall objectives of the operation and the administration, both the U.S. administration and the Afghanistan government, and make sure that the measures that we then collect can be reasonably linked to the overall theater objectives.

We often think in traditional ways of "measuring," and we might have to step out of the box so that "measure" encompasses a broader definition of what we have traditionally interpreted it as: there are certain types of measurements that are absolute; you can somewhat measure the number of people killed in insurgent attacks, which is a fairly straightforward number, based on surveys that you conduct. Of course, there has been a lot of analyses on whether surveys are misleading, depending on whether you have really good answers and representatives. We recently used an interview technique in a study in which we did not ask people for any sort of measurable outcome but asked what they thought about the issue. We then applied a theory called *semantic differential*, a theory that I believe comes from the marketing world and various words have meaning and value that are translated into numbers, to their answers.

If you think about it as a technique used to evaluate a television pilot, you might ask the people who viewed the pilot, "What did you think about, not through a numerical score from one to ten but just your thoughts." The various words that they use to describe their experience have already been assessed and have associated values based on lots of research.

We might use techniques like this, which are very out of the standard realm for the way we have conducted analysis in the past. We would have to scale it based on the Afghani way of thinking, not the American way of thinking. Therefore, we may want to think of metrics in a broader sense than we have thought of in the past.

Q: *Dr. Levitt commented that he would train a Ph.D. economist to be an analyst, but he could not train an analyst to be a Ph.D. economist. That may be true, but I would have little confidence that the Ph.D. economist would be an exceptional analyst; would Dr. Levitt?*

Matthew Levitt – There is no necessity here, of course. You could have someone who is an incredibly skilled Ph.D. economist and simply is not a particularly good all source analyst. Your goal is to find someone who is a skilled and accomplished Ph.D. economist who actually has the same type of skill set that you would be looking for in a fantastic all source analyst.

We were successful in the few full-time employee positions that we were able to carve out from our small, annual apportionment for all source analysts. We hired young people mostly right out of their post docs who had completed relevant work as Ph.D. economists and were interested in this type of thing, maybe had already had some experience elsewhere in government, but not as pure analysts, and sent them very quickly to some critical training courses. We were very fortunate.

However, you are right; you could say that about anyone. There are a lot of elements: your background, personality, and training.

Andrew Caldwell – I am not sure if I agree that you cannot train an economist to become a great analyst. I will give an example from the Apollo program. It is very hard to train geologists to become astronauts, but it is easy to train an astronaut to be a geologist. Therefore, Apollo program personnel took astronauts, I think it was, to Greenland and identified features and structures (e.g., glaciers, rock formations, etc.) that the experts had actually missed themselves in all the time that they have been in that part of the world.

Ultimately, I think it can be done. I guess it comes down to selection of the individuals. There are clearly some astronauts who are only interested in flying spaceships, and there are others who are fairly open minded about learning new skills to get the most out of their mission. This divide applies to economists and analysts as well.

Chapter 7

Senior Perspectives

7.1 UNRESTRICTED WARFARE—SENIOR PERSPECTIVES

G. Peter Nanos

INTRODUCTION

I think it is interesting that we are going to be discussing interagency issues with those of us who actually do work together on a fairly regular basis; thus, we can give you a good demonstration of what it is all about. Let me talk first about irregular warfare. I think by its very nature, irregular warfare, which seeks to deal with the asymmetries in a country, its infrastructure, its forces, and its alliances, calls for an interagency exercise because there is no single agency that encompasses all of these aspects.

ORGANIZATION

This theory really hit home to us at the Defense Threat Reduction Agency (DTRA). We ran something called an evil genius seminar to bring together all the "Lex Luthers," the evil geniuses that actually had gone straight as young people and had

Dr. G. Peter Nanos, Jr., is the Associate Director of the Defense Threat Reduction Agency, where he is now responsible for the Operations Enterprise. The Defense Threat Reduction Agency Operations Enterprise stands at the forefront in combating weapons of mass destruction. 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 of 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.

not gone over completely to the dark side, to charge them with figuring out how best to destroy the U.S. with the fewest tools and at the lowest cost. They devised some amazing results.

Tom Clancy led the band because he invented the concept behind 9/11. I thought that he would be an appropriate leader. They did not disappoint us. It turns out that there are a lot of techniques to destroy the U.S., but almost none of the cleverest geniuses were clearly within the scope of the DoD. Therefore, the first conclusion is that irregular warfare almost guarantees interagency activities that involve everyone.

The second important point is in the nature of interagency functioning. Interagency activities are very interesting because success always requires strong yet unstructured involvement of its actors. There is no Goldwater Nichols Act, as has been pointed out, not even a 1947 Defense Unification Act. There is no Joint Staff, other than the oversight that comes down from the National Security Council (NSC) or the Homeland Security Council (HSC). Quite frankly, interagency action is more or less coordinated based on relationships; it depends on who feels that the particularly problem is in their lane, as well as their degree of initiative and willingness to reach out to others who are working similar problems and conducting business in that area. You would like to think it was extremely formal: if a problem arose, somebody would blow a whistle and say, "I want you, you, and you to all come into the room." Everybody that was needed would be there, and it would be well organized, but the truth is that progress gets made based on personal initiative and relationships. Yes, there is some formality involved in it, but probably less than anyone would like. Because such interagency activities are often based on personal relationships, these relationships have to be continuously renewed to reaffirm everyone's roles and to keep people interested.

BUILDING RELATIONSHIPS

An example is the work against nuclear terrorism threats involving nuclear detection. In the beginning, five years ago, it was thought that by creating the Domestic Nuclear Detection

Office within the Department of Homeland Security (DHS), everything to do with nuclear detection would be handled by that organization. They proceeded to work on making our borders secure. However, the Department of Energy (DoE), and also DoD to a certain extent under the Nunn-Lugar Cooperative Threat Reduction Program, which created the mandate to secure and dismantle weapons of mass destruction and their associated infrastructure in the former Soviet Republics, was involved in nuclear detection. That involved a lot of detection work.

Of course DoE was heavily involved. Then DoD had to be brought in because a stolen weapon directed at either an ally or U.S. forces overseas cannot be treated passively; our defense forces have to find and secure it. That means active high search rate capability not being funded by other agencies was required.

Initially, I do not think DoD was that enthralled with putting additional money into that program, but they soon recognized the need for their role and today have a Memorandum of Agreement (MOA) that involves the DoE, the National Nuclear Security Agency (NNSA), DHS Nuclear Detection Office, and the Science and Technology Office of the Director of National Intelligence. All these organizations now work together to deconflict our programs in nuclear detection and to counter nuclear terrorism. This was a grassroots group that together put forward a rational program for the U.S., and it is a good example of cooperation that was not originally designed when the responsibilities were assigned.

EXERCISES

Another example is military exercises. We in the Defense Threat Reduction Agency (DTRA) get involved in a lot of these exercises, particularly nuclear accident incident exercises as well as consequence management exercises and a variety corresponding training. A good example of an exercise that turned into a tremendous paradigm of interagency cooperation was one that occurred in Hawaii a couple of years ago. We ran an exercise that included a terrorist nuclear detonation; the Governor of Hawaii played in this exercise, and the whole civil support structure in the state played along with all the military departments and the interagency actors concerned with this threat. It was an amazing exercise. It cost an awful lot of money to run, but it was a singular example of people recognizing that they had a mutual problem and taking the time on a fairly large scale to work through the issues.

We recognize now our dependence on the national laboratories, particularly the weapons laboratories, which are one of the few places where first rank science meets national security on the same piece of ground. Among those of us who know what has been done over the years to the DoD laboratories to reduce their effectiveness scientifically, we recognize that our national laboratories are true assets for national security.

Another notable example of cooperation is that we created a Memorandum of Agreement (MOA) with NNSA for mutual DoD and DoE support of the national laboratories. There is a program where we both contribute on shared mission areas, and it is the first time where I have done work with a national laboratory and not felt taxed to work with or for others because it is truly a shared mission space.

We are working in our jurisdiction; we are charged to consider concepts like radiation hardening (RADHARD) and nuclear effects on DoD forces. We have now started some work with the Networks and Information Integration (NII) in the Office of Secretary of Defense (OSD), along with the National Security Agency (NSA) and others, to look at all threats to the national command and control infrastructure, not just RADHARD or electromagnetic pulse, but also the coordination of cyber and direct physical attacks and their related threats. This brainstorm is important because, in addition to DTRA and the OSD, it eventually brings together the Science and Technology Office and the Office of the President because a lot of that command and control will involve DHS and a broad spectrum of laboratories: the DoE and NNSA Lab, Sandia National Laboratory, Los Alamos National Laboratory, Lawrence Livermore, Idaho National Laboratory, The Johns Hopkins University Applied Physics Laboratory, Massachusetts Institute of Technology Lincoln Laboratory, companies like the

Science Applications International Corporation (SAIC), think tanks like the Institute for Defense Analysis (IDA), as well as several universities (e.g., University of New Mexico and Penn State).

An extremely broad consortium is required to bring the skills together to assess future threats to national command and control. The Global War on Terror, Overseas Contingency Operations now, is another example that brings together a large number of players into a single plan. I have listed several above. It includes DoE, DoD, the National Counterterrorism Center, the National Crime Prevention Center, the national laboratories, the technical support working groups, FBI, DHS, the Joint Improvised Explosive Device Defeat Organization (JIEDDO), etc. Basically, when you get to that level, you see coordination on a massive scale.

FUTURE OBJECTIVES

The question is: what should our objective be over the long haul? I think that we need to start at the very basic level to instruct those who are starting their careers in either the military or other areas in government to understand right from the beginning that there is an interagency venue and they do not stand on the planet alone. It was in 2006 that I first began to recognize that there really was an interagency and that it was important to me and important to my mission. We need to start that education early. If someone happens to come to DTRA and get involved in some of our programs, they will come into contact with the interagency sooner rather than later. However, even with a fairly large military contingent, we do not get enough people cycled through DTRA to really satisfy that education requirement.

The existence and need for interagency collaboration needs to be integrated into professional military training, and included in training at every federal bureau and agency.

Next, we should seriously ask ourselves whether serendipity, individual initiative, and an honest attempt by a lot of people to coordinate well is sufficient enough to carry the day for our needs in the future as threats become more and more severe and complex.

I think that sometimes bureaucracy stifles initiative. There is a lot of good in what we have already done, but we need to give some serious thought to how we are going to govern ourselves in the future in that regard. There is a lot of opportunity here, and hopefully future efforts will be successful in a way that does not detract or destroy our previous efforts, so that we will in fact build upon what is good and change what is not. Maybe we need a reward system that offers promotions for interagency cooperation so that people know that this is a key element of our future.

To summarize, obviously I think the interagency is important; every year I recognize how much more important it has become. I do not think the American public has any real sense of how much of their well being is really carried by a consortium of the willing that are largely self-selected and self-motivated. To this voluntary group of people, you are doing a tremendous job for this country.

7.2 UNRESTRICTED WARFARE—SENIOR PERSPECTIVES

Bernd McConnell

INTRODUCTION

I am happy that I have already heard some of my favorite words like exercises, private sector, and, in our case of course, other governments at the U.S. North Command (NORTHCOM) side who are our neighbors and share relationships in general. I have heard about the project on national security reform, and I am a big fan. I think Dr. Locher is going to be a power in shaping interagency collaboration.

However, other than the North American Aerospace Defense Command (NORAD) and NORTHCOM, there are some fairly unique challenges in working within the homeland and our Constitution. We worry about how that all fits together from a DoD point of view. To relate a short anecdote, some time ago, a national magazine came to Colorado Springs—I will not further identify that magazine other than to note that they use a lot of

Mr. Bernd (Bear) McConnell leads the Dual Command Interagency Coordination Directorate for North American Aerospace Defense Command and United States Northern Command, where he coordinates DoD operational activities to ensure unity of effort in homeland defense and support to civil authorities. Previously, Mr. McConnell was the Director of the Office of U.S. Foreign Disaster Assistance in the Agency for International Development; he served more than 26 years in the U.S. Air Force, retiring as a Colonel. Mr. McConnell is a Naval Academy graduate and holds a M.S. from the University of Southern California. His awards include the Defense Superior Service Medal, the Legion of Merit, and the DoD Award for Distinguished Civilian Service.

spandex on the cover. Their role, we heard, was to write an article on how NORTHCOM was spying on the American people.

I spent some time with that reporter, and we talked about one of my, and our, concerns: how do you engage the private sector? You could see the eyes light up as he said to himself "Aha, the smoking gun." I tried to explain by saying that in the event of some sort of a disaster, if DoD, the Federal Emergency Management Agency (FEMA), and let us say Wal-Mart each have a truck of water, we should know each other well enough not to send all three of those trucks to this little town that only needs one truck of water.

TWO COMMANDS

Resource management is really the basis of why we would like to engage many partners, and principal among them is the private sector. The reporter said, "Ah, I got it," went away, wrote an article about NORTHCOM spying on the American people. So there are those kinds of challenges that we work on and deal with all the time. Remember there are two commands out there. NORAD is 50 years old and pretty well established in most of what it does. NORTHCOM, however, is not a bi-national command but a U.S.-only command, about seven years old at this point, and very young in bureaucratic terms.

NORAD has three missions:

1. Aerospace warning, which includes surface to forever, what is going on above us, and the dissemination of that information.

2. Aerospace control, which is somewhat of a misnomer because it is actually air space control, the kinetic part that deals strictly with air breathers. If necessary, a decision would be made to shoot down an airliner, which is quite a serious operation.

3. Ratified maritime warning that monitors what is occurring in the seas. Two governments developed

> this new concept two to three years ago, and instead of building a giant new structure, they will combine existing sensor systems to increase the awareness among the appropriate authorities, which is a major challenge. Both governments are struggling with that as we speak.

NORTHCOM, on the other hand, has two missions:

1. Homeland defense, which everyone somewhat understands. Every combatant command has the mission of defending the U.S. homeland.

2. Defense support to civil authorities, which is more difficult. The concept of support is tough for the uniformed community because, generally speaking, the uniformed community would like to have a mission along with some resources and ask everybody to kindly step aside while that mission is pursued, which is not always the case in the homeland when we have to pay attention to the U.S. Constitution.

If a major part of our role is supporting civil authorities, it seems like a good idea to know something about the people you are going to support. In fact, on any given day, there are 40 resident agencies by Peterson Air Force Base, mostly federal agencies, but some nonfederal as well. There is a Defense Threat Reduction Agency (DTRA) representative and a large intelligence community presence at NORAD. The Federal Bureau of Investigation (FBI) is present also, both full time and part time, including some of you attending this symposium. Forty agencies are on post, and if we draw a circle around Denver, we are up to a total of 60 agencies; these people are pre-identified, pre-cleared, and precommitted that we know and they know us. When an incident occurs, whether exercise or real, they would join and support us. Program analysis and evaluation, on the other hand, is not represented there, mostly because of fear. Support is a two-way street, which we try to emphasize.

CHALLENGES

A major challenge is state engagement. Everybody remembers Lieutenant General Russel Honoré marching around New Orleans while there were 70,000 uniforms involved in Katrina, 50,000 of which were under the command of governors. I think we all know there are 50 independent nations and four that are called territories, each of whom has an Army or an Air Force division working for the Head of State or the Governor of that state or territory.

A constant challenge is determining how so-called active duty (Title 10) people work with what is truly the power of the nation, the uniformed power. There is tension. Those guardsmen, not federalized, know very well who they work for, and it is not NORTHCOM. Governors do not work for the President, so I guess it is not the President either. This is the issue we work on a lot. I have been working for NORTHCOM four years, and we are maturing at what is not a comfortable mission for the Title 10 uniformed community.

We have another challenge concerning the national exercise program. The name leads you to believe that everybody participates. DoD continues to be fascinated by a nirvana of exercises, which are two weeks around the clock, and if you are a logistician, they are probably two months around the clock.

The FBI does not want to run through duplicate exercises, but DTRA will do it. This is not something that other agencies are prepared to do, whether they just do not want to or, more than likely, they are too busy. Therefore, we need to figure out a way to exercise both the anticipation events and the response events of a disaster, whether natural or manmade. We need to be able to exercise that in such a way that other federal agencies will participate.

Even beyond this, we need participation from more than federal agencies. How do you get the states involved? How do you, and not just the National Guard in the states, get Wal-Mart involved? We are working on that, and there is a lot of work to do. Tapping into the private sector is a major challenge, I would think, anywhere, certainly in the homeland. We are very aware of the fact that the private sector holds 85 percent of the critical infrastructure in the U.S.

Once again, we need to know each other, not in a command and control sense but in a noninterference and resource management sense. How do you make use of the power of the private sector, the states, and the larger community?

Admiral Nanos and I met each other not too long ago to talk about tunnel detection, a long running critical problem that has not been solved. We are trying, on an interagency basis, to collaborate with DTRA, the Department of Homeland Security, and U.S. Customs and Border Protection (CBP) to develop or actually field some existing technology.

This is not a big research and development effort, but this symposium is the first Joint Capability Technology Demonstration to address this subject; it is the first time that there have been co-sponsors across bureaucratic lines that clearly benefits DoD worldwide but also benefits the CBP. DoD does not have authority at our borders, but we certainly would like to know whether someone is using tunnels to transport drugs, people, and, more importantly, even weapons of mass destruction.

7.3 UNRESTRICTED WARFARE—SENIOR PERSPECTIVES

Vahid Majidi

INTRODUCTION

Over the past two decades that I have been involved in weapons of mass destruction (WMD) defense, one thing I have noticed is that the WMD milieu is pretty much like NASCAR: all the players are pretty much the same; the cars are all identical; we always take left turns; and from time to time, the sponsor changes.

Many of the people you see today are the same players that have been in this game for a very long time. The concept of interagency cooperation has become somewhat of a moot point because if you know your counterparts, over the historical perspective of this WMD game, you should have a much easier time of dealing with them and starting a more reasonable collaboration. I wish I could tell you that this is just natural and second nature. It actually takes work to do it, even though you know everybody in this game.

Dr. Vahid Majidi is the Assistant Director for the Weapons of Mass Destruction Directorate, appointed by Director Mueller. He came to the Federal Bureau of Investigation from Los Alamos National Laboratory, where he served as the Chemistry Division Leader. In 2003, the Deputy Attorney General appointed Dr. Majidi to Chief Science Advisor to the Department of Justice, where he served as the lead Department representative for programs on biosecurity, DNA technologies, and others. Dr. Majidi earned his B.S. in Chemistry from Eastern Michigan University and his Ph.D. from Wayne State University, after which he spent two years as a Postdoctoral Research Fellow at the University of Texas (Austin). Dr. Majidi has published numerous scientific articles in peer-reviewed journals.

UNCONVENTIONAL METHODS

In the specific case of the Federal Bureau of Investigation (FBI), we have been working with chemical/biological/radiological/nuclear explosives (CBRNE) issues for more than 15 years. Right after the subway attack in Japan by the Aum Shinrikyo terrorist group, the FBI decided that they needed to have the capability to deal with unconventional material and evidence as well as particular cases that involved the use of chemical, biological, and radiological material.

It was not until roughly three years ago that the Director specifically asked me to put the entire CBRNE portfolio under one umbrella and create a concerted effort to deal with WMD issues. Because I had a blank slate in a way, it was both a challenge and an opportunity; how do you start a program so that it meets all of your requirements, recognizing what you have seen in the past two decades? I have tried to put a program together that actually meets the citizen's needs; it has reasonable costs, but it has high productivity.

The first thing that came to our minds is that this is not an arena in which anyone has sufficient resources to support a standalone organization, be responsible for everybody, and conduct a productive program. There are simply not enough resources in a country. We looked both internally and externally and decided to set up an organization that met the overall requirement through integration, both internally and externally; every organization has their own columns of excellence, but sometimes those interactions are difficult to maintain between these columns of excellence within the organization.

As you work outside your organization, the interactions become even more difficult. One thing that is apparent in the FBI is that we do have very good legacy, established organizations (i.e., the counterterrorism, counterintelligence, criminal, and cyber divisions). The criminal and cyber divisions obviously are not within the national security branch but nonetheless have significant impact on the FBI's overall mission.

For the WMD Directorate to work well, the first thing we did was to decipher everyone's function. A very rudimentary interpretation of what columns of excellence do, in the example of counterterrorism, is to look at people and groups. They look for that one lone wolf (e.g., al Qaeda, Hezbollah, White Supremacists, or even the Animal Liberation Front).

To proceed further with our examples, counterintelligence is very country focused. They want to know adversaries (i.e., countries like Iran, North Korea, and Russia). If you look at the criminal division, they look at criminal enterprises and violent gangs, such as Cosa Nostra, the Italian and Russian Mafia, or MS-13. Obviously, the cyber division looks at computers and networks for specific subsets of activities. In the WMD area, we look at expertise and materials. To be frank, you cannot be a player in this game unless you have a reasonable background in CBRNE sciences and access to precursor materials.

Without one of those two, you certainly will not be a credible threat in WMD, whether a single person is trying to achieve a disturbance or a country trying to develop a WMD program. Having those two points of focus causes us to intersect very extensively with all of the divisions within the FBI. You could be a terrorist group trying to get the expertise and the material, you could be a criminal enterprise trying to benefit from a financial windfall of a transaction, and you could be a country trying to establish a WMD program.

Thus, WMD defense was inherently integrated within the FBI, and our challenge was how to design a new program that meets the needs of the FBI. This, however, is just the first challenge because as you go outside the FBI, you have many different government and non-government agencies with which you must be able to integrate well. That is exactly the way we decided to go forward. We used a social networking concept, without presenting the overall structure of the way we put it, which is much the way hobbyists interact.

SOCIAL NETWORKING

Everyone is familiar with social networking; everyone and their brother have a Facebook page; they have blogs and so forth. You may be familiar with the whole Kevin Bacon game: you can connect everybody in Hollywood to everybody else within six degrees of separation, and often, the actor, Kevin Bacon, is one of the nodes.

When you scientifically analyze social networking, there are two parameters that stand out. Parameter number one is called a super node. These are nodes that are much more effective than other nodes. When tracing the connectivity through these network nodes, the super nodes have very high density. If you look at the overall worldwide web, 10 percent of the websites take 90 percent of the traffic. That 10 percent are the super nodes.

The second parameter that we use to define these social networks is called a path link. The shorter the path link is, the easier it is to connect two people together. To define and design those social networking criterion within the FBI' WMD functions, it was pretty straightforward that what we really needed to do was to have an integrated approach and be able to reach out to internal and external organizations.

The best way to discover a super node is to ensure the existence of personal exchanges; we call them detailees. If you look across the organization, we have a very extensive detailee program within the WMD Directorate. We have very close connectivity with the Counterterrorism Center (CTC); we have a number of people actually embedded in that organization.

Some of the other organizations that we have a large investment in are the Domestic Nuclear Detection Office (DNDO), the Central Intelligence Agency (CIA), the National Counterproliferation Center (NCPC), national laboratories, the few biological laboratories that have a bio-safety level four facility, and the White House. We also have representation at the State Department, the Department of Commerce, and the National Security Agency (NSA). Then, we have also exchange information with the Department of Energy (DoE), the Defense

Threat Reduction Agency (DTRA), CIA, and the Department of Homeland Security (DHS). These are our super nodes.

HEADQUARTER ELEMENTS

We also have a number of short path-linked organizations. The way we set up our overall structure is that we split our activities into three parts: The first is countermeasures and preparedness. As we heard earlier there is a lot of consternation about organizations not doing enough exercises. As a part of that preparedness, we do in fact develop some exercises. One of the reasons we actually do not do too many exercises is that we deploy a lot.

You have heard anecdotally, from either the Graham Commission, the WMD Commission, or various other studies, the chances of the U.S. being hit with a WMD is high, and some say the chance is 50/50 within the next five years. I argue that we have roughly 24 WMD attacks annually. If you look at a definition of WMD from the statute's point of view, it is the use of any chemical, biological, radiological, or nuclear material in any criminal activities.

In fact, annually we receive roughly 1000 leads or 1000 threats that we dissect. Out of those 1000, 800 of them end up being junk. Two hundred of them are really what peak our interest and actually develop to full cases. Out of the 200, the majority of them are hoaxes, which are crimes in their own right, and we chase those as well.

About two dozen or so become cases that actually involve chemical, biological, or radiological materials, never nuclear. You may say there is a lack of exercise within the FBI, but actually last year alone, we had 170 deployments of all of our response assets. That by itself becomes the annual exercise that we do. Nonetheless, we do engage with many of our partners to study outside-the-box activities because what we know is routine; that is our deployment, and what we anticipate beyond the routine is what we exercise.

As a part of preparedness and prevention, we conduct exercises and develop training, but, more importantly, we develop trip wires or pre-event indicators. These are methodologies to determine if someone is trying to gain access to expertise or material.

The second pillar of our organization is intelligence analysis, which includes our Intel analysts that have an extensive scientific or analytical background, who are brought together to establish an analytical cadre that can deal with our day-to-day activity in strategic intelligence. If they come across something that we have never seen before, it becomes a new trip wire for our countermeasures. If it is case relevant, it is translated for our investigator so we can actually go forward with the case. As always, we have to disseminate the rest of the information to the rest of the community.

The last pillar of the main headquarter element is investigation and operations. Investigations and operations are exactly what we have done over the past 100 years, which is investigate every one of these cases, except these agents are actually trained to look for WMD nexus on all materials. We have developed a whole new set of investigative techniques that actually use the scientific methodologies in our case investigations.

We developed a technique for biological threats; it is called forensic epidemiology. We pair our FBI agents with the Center for Disease Control (CDC) or public health representatives and send them to the investigation so that they can ask parallel questions simultaneously and then come back for a conference to help resolve the issues. We do that with public health all the time.

Every field office actually has an entity or a person, sometimes a whole squad called a WMD coordinator (e.g., an FBI agent with an appropriate education that certifies him/her to be a WMD coordinator). Thus, there is a singular individual in every field office that actually interfaces with public health, universities, and industry; that person is that short path link seen in social network science. Any time we need expertise or access to these facilities, we exercise through that WMD coordinator.

Furthermore, we have a multi-tier program that can do this both nationally and internationally. Internationally, we work through our legal attachés and have started a program putting

WMD coordinators overseas in conjunction with the blessing of our intelligence community partners; the first one was placed in Georgia because there is an inordinate amount of transfer of highly enriched uranium ore, special nuclear material. We want to make sure that we are there, we can understand the problem, and we can help our partners; the entire University System of Georgia can be made available to resolve some of these issues.

The last thing I want to leave you with is that interagency collaboration sometimes is more difficult within your own organization than outside your organization. What I found is that when the day comes that you need your agencies or interagency partners, everybody comes to the table with the best intentions in mind. I have rarely seen parochialism in any of these issues.

Sometimes, it is a little bit more challenging when you work with the internal elements because then we do have to worry about the delineation of intelligence versus law enforcement. Information sharing is really not an issue, to be honest with you. What is at issue is that sometimes, from the law enforcement perspective, we do take the case to its full fruition and an individual is actually going through the court hearing. As they prepare that case, it becomes somewhat of a black hole; we cannot take that information now and actually shove it the other way. However, taking the information from the intelligence community is not difficult at all because we already have the methodologies and mechanisms in place.

7.4 QUESTIONS AND ANSWERS HIGHLIGHTS

Transcripts

Q&A

Q: We know that further interagency cooperation or legislation is coming. What is the low-hanging fruit in terms of what can be done now without legislation to make things better, move the ball down the field, and increase cooperation? On the other side, what are the real tough nuts to crack? What will require hard negotiation and legislation as well as some hard feelings to ensure forward motion?

Vahid Majidi – I will talk about the tough nuts. One of the biggest challenges is that as you look across different organizations, including the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and NORTHCOM, there is a certain mission space given to each one based on a certain set of statutes. The tough nut is that as the mission space starts to expand, these go to the places that no one had anticipated, intentionally or unintentionally, before; there is always an overlap of mission space. One of the biggest challenges today is delineating that space well enough so that everyone understands the boundaries of their lane.

Karen Monaghan – I would talk a little bit about the low-hanging fruit. I think it was mentioned earlier, but we should somehow give credit for cooperation, whether in your personnel assessment or awards. I know that the Director of National Intelligence has given out a number of intelligence awards, and we try, at the National Intelligence Council, to annually give credit for joint projects. I think that is really important. Often, it is done but you feel that you do not get credit for it. Another method would be to increase the number of detailees, not just mandated but also body swaps, even for short periods of time. This enhances cooperation, just having people that you know and can reach out to.

On the tough nuts to crack question, consider limited resources, whether the cause is funding or personnel. We will need to rationalize those resources so that they are used in the most efficient way and allocated to people who can best leverage them. There is always a challenge when someone's resources are threatened.

Eric Culter – Let me follow up with what Karen said. When Henry Kissinger ran the National Security Council (NSC), he actually sent out a task that challenged the federal government on a particular problem. I have never seen such a document that basically said, "federal government, here is your problem, here is the issue, and here are some assumptions so go study it and come back to me when you have an answer." I have not seen that since, though maybe it has happened.

We asked some senior leaders not too long ago what keeps them up at night. They basically said, "A loose nuke scenario." Imagine, similar to Jack Bauer in the television series "24," our President gets a call from the leader of a country who says, "I just lost control of a nuclear weapon six hours ago. Now what do we do?"

First, if you want to try and secure it in the country that lost it, it is a serious military and diplomatic challenge; I do not know the chances of success. However, much like the pace of "24," every second more on the clock widens the circle of uncertainty as to the location of that weapon. I am trying to argue for a systems analysis approach to understand what actions to take, the probabilities of success, and the possible capabilities required at every step of the way.

Clearly, it is a layered defense. It may be a military diplomatic action in a country (e.g, maybe you close the borders of that country or the maritime approaches). I have not yet seen anyone take a systematic approach to discover what it would take to respond to certain situations and at what cost. If you actually had to do it, how would you do it? To make it easy, someone from the NSC could probably direct a response.

It is not something that would be done overnight. It would get a lot of people's attention because Homeland Security, who has responsibility for defense of the country and its borders, has their equities, as do DoD and others. At some point in time, though, you have to lay all the facts and the analysis on the table and show the senior leaders the choices that they have to make.

Some of this information may be readily apparent; there are some areas you need to invest in that have a huge payoff. I do not know, however, what they are relative to others. Again, I think someone with some leadership could direct a response fairly quickly, much as Kissinger did back in his era: give people a year or two to work it out and come back with an answer.

G. Peter Nanos – Actually, the truth is that this is a wonderful opportunity to tell you a little bit about what has gone on in the past. I mentioned that part about the nuclear detection that was laid out, but actually we did a systems analysis of what it takes.

If you look at the piece parts, the first element is intelligence. I want to point to what I think is one of the most successful interagency collaborations with intelligence: the Hard Target Research and Analysis Center (HTRAC), which is the hard target defeat cell where there are essentially 150 Title 10 full-time equivalents working inside the Title 50 boundary with the most difficult targets that our military has to face. We have started up a Counter WMD Analysis Cell to provide that combined modeling engineering and Intel support to this mission.

Then there is the range issue; if you lose a weapon, you need high search rate detection. At DTRA, we have supported, as our part of the nuclear detection business, four long-range detection programs using four different methods: all the way from proton beams at one extreme to relatively low energy neutrons at the other. The nearest term is probably a bremsstrahlung machine that can achieve detection at ranges of 500 meters to one kilometer.

Right now, detection ranges are so short that search rate is almost so negligible that you have almost no prayer of an un-alerted detection of a weapon. Then, you have to deal with what happens if you have a "nuclear martyr," and there is a balance in the portfolio that is dealing with how we manage a situation where someone is hardwired to a weapon; how do we take it away from them without detonating the weapon? There is an investment part of the portfolio that is looking at that.

There has been a fair amount of thought given to who has to be in the decision process. Clearly, if you are going to get aggressive with someone else's nuclear weapon, the President is involved; therefore, you need a command and battle management structure that reaches to the highest level of the government and integrates all of the components. A lot of that analysis has in fact been started, and there is a balance portfolio, albeit not overwhelming, to address these.

I think the big problem of getting this process moving faster, and making it more noticeable, is the fact that some of the areas that we are dealing with (i.e., the standoff detection piece, the spoiling-the-yield piece, and those sorts of things) are so technically difficult that we have had to convince the technology community that there are reasonable investments to be made. I think as we have received data, now we are starting to get traction, but there has already been a substantial amount of analysis done.

I would like to add on to the lower hanging fruit discussion in terms of balance, and I am torn between poverty and riches, frankly. On the broader question of how do we get better, how do we avoid cylinders of excellence and foster interagency cooperation? Wealth spawns cylinders of excellence. Poverty spawns cooperation. In some cases, some of our best work has been on the edge of oblivion as we fight to perform missions in that sense. We have often felt there has been overwhelming risk—we have poured a lot of money into it—and that is when a lot of the cooperation starts because pouring money into a project means they put someone in charge, who tends to freeze out everyone else and start everything anew. Consequently, a lot of the good work from before gets erased. I think we need to find a way of managing these difficult programs in which we foster innovation and cooperation and yet can also feed the resources in a way that does not tend to reset the clock.

We need interagency coordination, but it is a difficult process. The intractable part is that it is easy to tell someone to reform the band and create a new organization, but as we look at the Department of Homeland Security (DHS) example of what happens when you start anew, you spend the first two years in organizational food fights. It is the third year before you start to become effective, which we have seen over and over again.

In the middle of a very dangerous world, we cannot afford to black out for two years while we conduct organizational drills. The biggest difficulty that I see is the sociology of bringing us together in the interagency without destroying all forward motion. That is not a simple thing to do, and I do not know exactly how we are going to do it. I think anybody who could contribute by writing papers that deal with this issue in a substantive way would be a big help to us all.

Bernd McConnell – If somebody lives with you, and you look in their bloodshot eyes all the time, you are going to understand each other better even though they might come from a different culture. On the hard side, that change in culture allows unfettered communication in a non-command and control relationship, and it seems to me that DoD has it the easiest because when they tell someone to carry out a directive, oftentimes they do. When you are working across bureaucratic lines, there is no such cause and effect, NSC aside. There is an old saying: when the President makes a decision, that is when the negotiation begins; I think it is a very accurate saying.

Another component is DoD's propensity for classifying everything. The law enforcement sensitive classification is everyone's ugly mess. A lot of the interagency business in the homeland at least deals with people who are able to communicate freely. We have a problem in NORAD, even after 50 years, because we still have foreign entities that do not understand a lot of what we do, precluding the Canadians. How do you facilitate the communication necessary to hold a government or maybe even a society together?

Q: *In Dr. Locher's keynote address, one of the points he made concerned forming teams from the interagency. I think he advocated that the President of the U.S. would pick five to seven issues, and that each issue would have a dedicated interagency team formed around it by pulling individuals from different organizations. I would like to know your thoughts on that.*

Bernd McConnell – Those interagency teams exist now. That is the interagency process that we have come to love, our deputy and principal committees. What does not exist now, that I think Dr. Locher is interested in, is a private sector representative within the membership of those committees as well as maybe even state and local representatives. I am for it.

G. Peter Nanos – I would like to add to that. I agree that that is often the modus operandi now. However, the key idea is that the resources should follow the teams and actually get the work done. The teams often are very good at planning and bringing people together for a common point of view, but then I think the follow-on step has to be resourcing the agencies that sit behind the teams with the parts that need to come together to actually push actions forward. Progress is often generated by investment, so that part of it has to flow also.

Q: *I also heard Dr. Locher address a parochialism and stovepipe element within the organizations and how that might deter an effective team. Do you think this is true?*

Karen Monaghan – On the intelligence side, certainly when we produce national intelligence estimates, a team is required. We may have one drafter, but, in a lot of cases, we have multiple drafters; it is the responsibility of one person to put the document together, which may contribute to biases or parochialism among members of the team, but the document is a consensus and therefore includes any significant differences of opinion among the team.

I do not necessarily think there is anything wrong with biases and parochialism. Sometimes they can lead to better analysis. It is not necessarily good to have everyone in agreement.

G. Peter Nanos – I mentioned earlier that we have a lot of people actually working in the intelligence community, but we are not an intelligence agency; there is not anything that says DTRA on any of the reports because, even though they are intelligence agency reports, we are a silent partner. We do our work and help out. However, I think there needs to be a recognition and a willingness to work together, not always in an effort to have your name appear on the byline, which is sometimes hard to do in federal Washington.

Eric Coulter: – My experience, and I think my staff would say the same thing, is that there is always the concern of parochialism, but we think we cooperate very well. We think, for the most part, that the people we work with from other agencies are really there to help in any way they possibly can.

However, I think there is another kind of problem, even in DoD, because if the President wants something done, you typically send your best person; however, the work piled on your desk back in your office does not go away. It is very hard sometimes to let your best people go to work on these really important problems, and the organization usually suffers, but it is just a sacrifice you have to make.

Q: *To improve the ability to work effectively with civilian agencies in addition to incorporating interagency education in military education, do you believe we should have interagency specialty officer credit awarded based on training, education, and experience, including rotations with other agencies similar to a Joint Specialty Officer?*

Eric Coulter – Yes, they have actually started a new initiative in the last six or 12 months called the National Security Professional (NSP). The theory behind this position is you would designate certain people throughout the organizations that deal with national security and these people would rotate and get credit, much like the Joint Staff.

I hope it works. I have not seen it yet. Many of us have already been designated as NSPs. Now, I want to wait and see if the resources exist to actually move people around and distribute the experience in different organizations.

Q: *This NSP initiative is civilian-only, though, right?*

Eric Coulter: – It is civilian only, but I think the military already has a similar initiative in place.

Karen Monaghan – We may also have an advantage with a younger cadre that likes to move around. For my generation, you stayed with your agency and were credited with loyalty and a long career with that agency. However, my experience with many younger employees is that they are looking for change, excitement, challenge, and new opportunities and influences in new organizations. Therefore, the receptiveness among these younger employees to actually move and carry out these exchanges is probably much higher.

Q: *Dr. Nanos made an interesting comment encouraging the introduction of new government professionals to the practice of thinking and acting within the interagency. Given that the next generation's impulse is to network ad-nauseum, is achieving a mature interagency going to be a young person's game, keeping in mind that this is a senior panel.*

G. Peter Nanos – I will twitter you on that. We are starting to see the networking tools [e.g., the Secret Internet Protocol Router Network (SIPRNET) and the Joint Worldwide Intelligence Communications System (JWICS)] and the development of our ability to communicate face-to-face, share information, and use portals and chat rooms. I can remember the first time we conducted a war in a chat room. About 10 or 15 years ago, we started to use Lotus Office in a tactical scenario, and we started to see discussions. I have been watching and sitting in on some major exercises in the Pacific arena, where virtually all of the interactions in the video teleconference were electronic tactical interactions from widely dispersed sites; the coordination was very high, and the communications were in two languages.

I agree that those people who are comfortable with the technological capability and can exploit it to the fullest are going to have an opportunity for great impact. Technology, and our ability to exploit our own advances, in this country has always been our edge because we have seen in irregular warfare that our enemies, particularly the terrorist enemies, are living on our technology to develop their own ability to conduct command and control coordination across the Internet using these networking tools; we just happen to be better at it.

Vahid Majidi – You know my mantra is trying to get people together, but I will mention one caveat: being able to network is not the end of the road; instead, it is executing that network and achieving forward motion on projects and directives. We have a lot of folks who have an extensive connectivity with a large network of people (e.g, via Facebook or Friendster). You talk to young folks who say, "I have 4,000 friends on Facebook," but there are not real friends; they are all electronic friends, so there is no two-way communication. You just add the links.

Networking in a real business world is the same way: you can know a lot of business folks or even other people in your business but not necessarily execute any action with those individuals. Therefore, networking only becomes practical and relevant when there is actually bidirectional connectivity.

Q: For years, people have talked about how we need an interagency Goldwater Nichols Act, but are there some downsides to that? I think most of the people on the panel know a good bit about Goldwater Nichols or the recent Intel reorganization—Dr. Nanos talked a bit about the first couple of years of DHS—but are we looking at the right models? What should we be worried about when we talk about reorganization based on what we know in our careers?

Bernd McConnell – We have good limited systems of interagency interaction, whether within the intelligence community or whether it is a deputies or principals committee. The problem with the current system is identifying who all is in the group; it is limited. DoD is comfortable talking to DoD. We are not comfortable venturing out of the federal family.

To be able to include a private entity in a policy recommendation body is probably a stretch that would make just about everybody uncomfortable, but it seems to me it is the next step. We need to be more inclusive if we are going to benefit from the power of the country. I do not think we can afford to be comfortable.

Karen Monaghan – If a reorganization or legislation enhances fluidity, then it is a good step to take. However, if it creates a new bureaucracy, then it is a bad path to follow.

Q: *Is a re-organization possible without creating a new bureaucracy?*

Karen Monaghan – I would hope so.

G. Peter Nanos – When I grew up through the phase of Goldwater Nichols, I remember what really made it work. What really brought people around in Goldwater Nichols is when the path to success lay along the joint path, and the rewards, the carrot part, were what caused military folks to come out from hiding; if they think it is in their best interest to themselves and their service, they will do what is required.

When it became clear that the power was shifting to the Combatant Commands (COCOMs) and the rewards and potential promotion opportunity became dependent on your degree of jointness in your career, people were dumbstruck because their world drastically changed. We should not forget that it the reward system is a tremendous motivator.

Eric Coulter – One of the problems with the Goldwater Nichols Act is that it has taken 20 or 25 years to get where we are today. Even if we pass a new Goldwater Nichols Act—it is going to be decades away in my view—in fact it is going to be harder to facilitate an interagency approach than the DoD joint approach. You would be looking at two, maybe three, decades before you really see results. I personally do not think we can wait that long.

I know there are a lot of committees that meet here, there, and everywhere—and again I am looking from a narrow view as an analyst who serves in an analytic community—but in the DoD perspective, that province is for policy people. They meet, and for the most part analysts are not included, do not participate.

Not that they have to, but there is no parallel committee or group of meetings for analysts who provide decision support. We are working from the bottom up. This symposium is extremely useful to us because we do the networking and we get to meet interesting people who can help us and who we can help.

Q: *Interagency so far looks at the foreign/domestic split or schism that we have within our government. Karen Monaghan mentioned that the National Intelligence Council (NIC) is essentially tasked with looking outward. Do you have the flexibility, as the National Intelligence Officer (NIO) for economics and finance to look at the U.S. international economic imbalances, some of which are mirror images of our domestic economic imbalances, and assess the national security implications of this?*

Karen Monaghan – We would look at global imbalances, focusing on if we have a surplus here and a deficit there. We would tend to look at who the surplus countries are, why they are surplus countries, how they can be encouraged, and what they are doing to reduce those surpluses. We do not look at the other side.

Having said that, the CIA, Treasury Department, and the NIC certainly are well aware of the other side of that imbalance, and it is their responsibility to figure out, from the U.S. perspective, what we should be doing to move more from a deficit to a surplus.

Q: *What specific steps can DoD take in the upcoming Quadrennial Defense Review (QDR) to improve interagency action?*

Bernd McConnell – We have really tried to include categories in the last QDR's building-partnership-capacity roadmap that gave all of us an awareness of the fact, for the first time, that if we build the capacity of others, then maybe we would not have to do it ourselves. That is something that I certainly hope survives the current QDR process, and I think my J8 pals and I at NORTHCOM are certainly going to try to do our best to make sure that it survives.

One international advantage we have is that our major international partners happen to be our neighbors. Commerce does not stop in El Paso. Because we are working with our neighbors, it seems to me in some ways that it is easier for us to focus on the interagency aspects and to, for example, try to build up Mexico's civil protection by providing chemical ensembles to empower the civil side, which allows the Mexican military to deal with the drug wars along the border.

G. Peter Nanos – Now there are aspects that the new administration emphasizes in terms of partnerships, but if you look at what will be the new focus on treaties, which often lead to new international relationships and also renewed security cooperation, you will see perhaps enhanced emphasis on those areas of improvement. There are also now 75 nations involved with the Global Initiative Against Nuclear Terrorism, the Bush-Putin initiative.

We have established information portals. We are running international nuclear detection and material detection seminars; we have one this summer in Paris, and the next one will be in Russia. The State Department is starting to play a bigger role, particularly in the threat reduction arena aimed overseas, which fits in with their security cooperation programs. We should see that list grow, and I do not think that will it be ignored in the QDR.

Q: *I have heard a lot of discussion regarding interagency cooperation, but what are we doing in terms of an overall national strategy or architecture that is looking at all the different agencies' expertise levels and how we all play in this new threat strategy? For example, we talked about using anthropologists in different ways of looking at the problem. Do we have any new national strategy or architecture that will combine all of the strengths of the different agencies and departments and using them in new and innovative ways to combat this threat? Is that strategic over the next 20 years? Are we looking into what all these agencies need to confront these new threats?*

Karen Monaghan – The Department of the Interior has something called an analytic resource catalogue. You have to enter your information yourself; it is a voluntary system, and you basically catalogue your areas of expertise. From an architectural point of view, if you needed to surge on a particular country or region, you conceivably could go into this database and identify the core economists, how many there are available, how many have energy expertise as well, where they are located, and how you can recruit their help. That is one way that we are trying to identify what resources we have in a more strategic way.

I do not really know of any other strategic thinking about identifying specific resources and how to mobilize and leverage them against new threats.

Vahid Majidi – For a certain area, when we know there is a specific shortage, we have worked within the interagency to bolster that area, to the extent of investing in universities to do specific research to increase student interest in that area. Radiochemistry is one of those areas, for example. We know for a fact that we are going to have a shortage in the next two decades or so; therefore, there is a significant interagency investment in that particular field.

I do not believe there is a strategic interagency document that specifically identifies the short areas and subgroups of people to recruit. Within every organization, because I know it is true within the FBI, we actually look at a broad spectrum of individuals with different backgrounds to see which ones will fit our needs best.

In my organization, believe it or not because I rigorously keep track of it, I have folks that have advanced degrees in chemistry, physics, and biology; there are veterinary specialists, sociologists, psychiatrists, and even a mortician. I am just throwing that in there as an example. The reason for this professional diversity is because our adversaries also have a very broad spectrum of backgrounds. You do not want to pigeonhole yourself; you want to have the staff that can provide a complete, analytical point of view.

Once the analytical products are developed, you can then sit down around the table and argue, “Does this really make sense? Would it make sense from a technical point of view? Does it make sense from a socio-economic point of view?” We call that threat credibility, a process we follow scrupulously.

Afterthoughts

AFTERTHOUGHTS

Thomas Keaney

The Senior Perspectives panel, with the collective experience to really make connections, drew together some of the themes of this symposium, interagency action in particular. I would like to review some of the interagency imperatives that have been introduced these last two days. As you may recall, Mr. Jim Locker began the symposium by presenting a call for interagency cooperation within a new system. He first pointed out the National Security Act in 1947, which constructed our national security system and was already outdated when the system it created came into being. With the new threat environment, that system is woefully inadequate for dealing with the many issues with which it has to deal, particularly in agility, and has an inability to focus on interagency action. These kinds of issues gives purpose to this symposium. In its inception, the National Security Act was very focused on traditional measures of national security and only involved the original members of the National Security Council (i.e., the State Department, DoD, and the Central Intelligence Agency (CIA).

Professor Thomas A. Keaney is the Acting Director of Strategic Studies, Executive Director of the Merrill Center for Strategic Studies, and Senior Adjunct Professor at the Paul H. Nitze School of Advanced International Studies (SAIS), the Johns Hopkins University. His publications include Armed Forces in the Middle East: Politics and Strategy (2002) and War in Iraq: Planning and Execution (2007). Until 1998, he was a Professor of Military Strategy at National War College and Director of its core courses on military thought and strategy. He is a graduate of the National War College and has a bachelor's degree from the U.S. Air Force Academy and M.A. and Ph.D. degrees in history from the University of Michigan. He retired from the U.S. Air Force in 1991 as a Colonel.

When Locher talked about the need for change, my mind referred back to one of the major revisions of the 1947 Act: the 1986 Goldwater Nickel's Amendment. This revision is now in its 23rd year, but its usefulness, considering the threats we are now discussing, is still really quite limited. The 1986 Amendment tried to create more joint activity and interaction, which has been difficult. The many speakers and panels have discussed four new dimensions that really exacerbate these difficulties: cyber attacks, resource attacks, financial/economic attacks, and nuclear terrorism, probably the most severe threat.

These threats call for expanded interagency activities; the needed actions go far beyond what the military services would have called for in traditional military defense because of the profound differences and difficulties that we now encounter. Let me mention just several of them. First of all, in this new world of interagency activities, increased, more extensive involvement of people from the private sector, as well as local and state governments, is needed. Also, we will need to cooperate with other governments, although that has not been addressed here. Other governments will certainly be involved.

Secondly, the federal government, in many ways, is going to be a minor participant in some of these interactions, when you start talking about the federal government and local agencies. Although the federal government, or parts of it, will be the prime integrators, there will be much greater interaction outside the government.

Another issue is that we are going to have to anticipate great difficulties, depending on the context, in trying to decide on priorities and timing and even identification of the targets. Most important question to ask is who is in charge? Whatever the context, I think the answer will need to shift greatly, and getting people to understand and agree to that is going to be very difficult.

Nuclear terrorism seems to call for bringing together the most agencies; the discussion this morning really brought that out. Not only does it take many agencies but which agencies that are involved appears to be changing throughout the different phases of a nuclear terrorism threat: detecting, preventing, or recovering.

Another issue is that there is going to be a need for many new skills, models, simulations, and technologies for financial and economic accounting to defend against new threats in this area. It was mentioned yesterday that the tools of the hedge fund manager may become increasingly important to understand the movement of sovereign wealth funds and other funds that could be used against the U.S. Such intelligence developments may have to come from the Federal Bureau of Investigation (FBI) and the Securities and Exchange Commission.

Another aspect that developed from our discussions is the usefulness of exercising. The military has been very adept at this; they have great experience with using exercises to get everyone to identify and confront different scenarios. I was struck by Eric Coulter's DoD analytical agenda for providing structure to such analyses. We may find that the other agencies outside government are not as used to exercising as DoD. Someone also mentioned that analytical collaboration has been very unsuccessful in bringing together experts from these organizations, and I think that is going to continue to be a factor.

Finally, under almost any of these circumstances, effective interagency actions are going to depend on individual initiative. Even if we start right now with this type of system, it will require people to not simply rely on someone to tell them what to do but to use some initiative. The one thing that I must remember, however, is that every one of these people is already very busy and focused on his/her own immediate problems. I must say finally that this next step cannot happen without the participation of the senior leaders in all of these organizations to support the new system. If they do not encourage this forward motion, I think it is probably not going to happen, which places even more importance on the judgments of the individuals of the Senior Perspectives panelists.

Appendix A

Symposium Agenda

APPENDIX A

UNRESTRICTED WARFARE SYMPOSIUM AGENDA

DAY 1
(24 March 2009)

8:00–9:00 Keynote Address

The Honorable James R. Locher, III, Project for National Security Reform, Author of Victory on the Potomac: The Goldwater-Nichols Act Unifies the Pentagon

9:00–9:15 Welcome and Insights from 2008

Interdependent analysis, strategy, and technology perspectives will be given on how unrestricted warfare and increased globalization create imperatives for interagency cooperation and action.
Dr. Ronald R. Luman, JHU/APL

9:15–10:00 Cyber Attacks

The threat of cyber attacks on networks, computers, data, and information systems and the potential impact to national security.
Mr. Dan Wolf, Cyber Pack Ventures, Inc.

10:00–10:15 Break

10:15–11:45 Roundtable 1: Responding to Cyber Attacks

Panelists from the strategy and technology communities will discuss imperatives for interagency action and identify policy and technology innovations to counter or respond to cyber threats.
Mr. Thomas M. McNamara, Jr., JHU/APL (Moderator)
Mr. Robert Gourley, Crucial Point, LLC
Mr. Anthony Bargar, OSD(NII)
Mr. Dan Wolf, Cyber Pack Ventures, Inc.

11:45–12:30 Lunch

12:30–1:15 Resource Attacks

Unrestricted warfare threats to national resources are characterized and include agriculture, power, oil and natural gas, water, and the physical infrastructures that support these resource assets.
Prof. Michael Klare, Hampshire College, Author of Resource Wars

1:15–2:45 Roundtable 2: Responding to Resource Attacks

Panelists will discuss how attacks on natural resources create imperatives for interagency action and will identify options for enhancing appropriate interagency capabilities.
Ms. Lesa McComas, JHU/APL (Moderator)
Dr. Khatuna Salukvadze, Ministry of Foreign Affairs of Georgia
Prof. Michael Klare, Hampshire College
CAPT Jan van Tol, USN (ret), CSBA
Ms. Celina Realuyo, CBR Global Advisors

2:45–3:00 Break

3:00–3:45 Economic and Financial Attacks

Attacks in this line of operation include targeting or acquiring sensitive financial, trade, or economic policy information, proprietary economic data, or critical technologies, and the potential impact to national security.

Mr. James Rickards, Omnis, Inc.

3:45-5:15 Roundtable 3: Responding to Economic and Financial Attacks

Panelists from strategy and technology communities will discuss how economic and financial attacks can create imperatives for interagency action and will identify options for enhancing appropriate interagency capabilities.

Col Edward (Ted) A. Smyth, USMC (ret), JHU/APL (Moderator)
Prof. Pieter Bottelier, JHU/SAIS
Prof. Richard Cooper, Harvard University
Dr. William Overholt, Kennedy School of Government, Harvard University
Mr. James Rickards, Omnis, Inc.

5:15–6:00 Social

6:00–6:45 Dinner

6:45–7:30 Resiliency in the Face of URW Attacks

Dr. Stephen Flynn, Council on Foreign Relations, Author of The Edge of Disaster: Rebuilding a Resilient Nation

DAY 2
(25 March 2009)

8:30–9:15 Terrorism – From IEDs to WMDs

An interagency approach to successfully countering the full range of terrorism threats requires not only the military but fundamentally parallel political, social, economic, and ideological activities.

Prof. Bruce Hoffman, Georgetown University, Author of Inside Terrorism

9:15–10:45 Roundtable 4: Responding to Nuclear Terrorism

Panelists from the analysis and strategy communities will discuss how the threat of nuclear terrorism creates imperatives for interagency action and will identify options for enhancing appropriate interagency capabilities.

Mr. Todd Masse, JHU/APL (Moderator)
Mr. Brian Jenkins, RAND
Dr. Jonathan Medalia, Congressional Research Service
Dr. J. Scott Cameron, NCTC
VADM Harvey Johnson, Jr., USCG (ret)

10:45–11:00 Break

11:00–11:45 Analysis Support for the Interagency

Analytical approaches that integrate diverse agency interests and provide real-world illustrations of their application and how they may be employed for national security.

Mr. Eric Coulter, OSD PA&E

11:45–12:30 Lunch

12:45–2:15 Roundtable 5: Analysis Support

Panelists from the analysis community will discuss how unrestricted warfare creates imperatives for interagency action and will identify options for enhancing the community's ability to support interagency efforts.

Mr. John Benedict, JHU/APL (Moderator)
Dr. Matthew Levitt, Washington Institute
Mr. Andrew Caldwell, OSD
Dr. George Akst, Marine Corps Combat Development Command

2:15–3:00 Intelligence Support for the Interagency

How unrestricted warfare creates imperatives for integrating and synthesizing intelligence collection and analysis to support interagency efforts.

Ms. Karen Monaghan, National Intelligence Council

3:00–3:15 Break

3:15–4:45 Unrestricted Warfare Imperatives for Interagency Action: Senior Perspectives

Senior Government Personnel will provide their individual perspectives on how unrestricted warfare creates imperatives for interagency action and identify opportunities to integrate strategic, analytical, and technological developments to support such efforts. In the remaining time, the panelists will field questions from the floor.

Prof. Thomas Keaney, JHU/SAIS (Moderator)
Mr. Eric Coulter, Deputy Director, Strategic Assessments, OSD PA&E
Dr. G. Peter Nanos, Jr., Associate Director for Operations, DTRA
Ms. Karen Monaghan, National Intelligence Council
Mr. Bernd "Bear" McConnell, Director, Interagency Coordination, USNORTHCOM
Dr. Vahid Majidi, Assistant Director, Weapons of Mass Destruction Directorate, FBI

Appendix B

Acronyms and Abbreviations

APPENDIX B

ACRONYMS AND ABBREVIATIONS

AIG	American International Group, Inc.
ARG	Accident Response Group
ASD(HD&ASA)	Assistant Secretary of Defense for Homeland Defense and America's Security Affairs
ASEAN	Association of Southeast Asian Nations
ASPAC	Asia Pacific Network of Science and Technology Centres
ASW	Antisubmarine Warfare
AWOL	Absent Without Leave
BTU	British Thermal Unit
CAARS	Cargo Advanced Automated Radiography Systems
CAG	Consensus Audit Guidelines
CAL-ISO	California's Power Control Supervisory Operations Center
CARRI	Community and Regional Resilience Initiative
CBIRF	Chemical Biological Incident Response Force
CBP	Customs and Border Protection
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CD	Compact Disk
CDC	Center for Disease Control
CENTCOM	Central Command
CEO	Chief Executive Office
CERT	Community Emergency Response Team
CERT	Computer Emergency Readiness Team
CFIUS	Committee on Foreign Investment in the United States
CFO	Chief Financial Officer
CFTC	Commodity Futures Trading Commission
CIA	Central Intelligence Agency
CIKR	Critical Infrastructure and Key Resource
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection

CIVIS	Corporate Information Management Vision System
CNCI	Comprehensive National Cybersecurity Initiative
COCOM	Combatant Commander
COIN	Counterinsurgency
CONOPS	Concept of Operations
CP	Counterproliferation
CPB	Customs and Border Patrol
CSBA	Center for Strategic and Budgetary Assessments
CSIS	Center for Strategic and International Studies
CSPAN	Cable-Satellite Public Affairs Network
CT	ounterterrorism
CTC	Counterterrorism Center
CTO	Chief Technical Officer
DA	Department of Agriculture
DECON	Decontamination
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNA	Deoxyribonucleic acid
DNDO	Domestic Nuclear Detection Office
DNI	Director of National Intelligence
DoD	Department of Defense
DoE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOS/CT	Department of State's Coordinator for Counterterrorism
DPS	Defense Planning Scenarios
DTRA	Defense Threat Reduction Agency
EAA	Export Administration Act
EIB	The Economic Intelligence Brief
EMAC	Emergency Mutual Aid Compact
EMH	Efficient Market Hypothesis
EPA	Environmental Protection Agency
EU	European Union
FBI	Federal Bureau of Investigation
FCO	Federal Coordinating Officer
FDA	Food and Drug Administration
FDNY	Fire Department City of New York
FDR	Franklin Delano Roosevelt
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FERMAC	Federal Radiological Monitoring and Assessment

	Center
FFRDC	Federally Funded Research and Development Centers
FINSA	Foreign Investment and National Security Act of 2007
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FSU	Former Soviet Union
FY	Fiscal Year
GAO	Government Accountability Office
GARCH	Generalized Auto-Regressive Conditional Heteroskedasticity
GDP	Gross Domestic Product
GDRAS	Gamma Detector Response and Analysis Software
GIG	Global Information Grid
GOM	Gulf of Mexico
GSPC	Group for Preaching and Combat
HEU	Highly Enriched Uranium
HFAC	House Foreign Affairs Committee
HHS	Health and Human Services
HSC	Homeland Security Council
HSPD 7	Homeland Security Presidential Directive 7
HUMINT	Human Intelligence
IA	Information Assurance
IAEA	International Atomic Energy Agency
IC	Intelligence Community
IC&T	Information, Communications, And Technology
ICE	United Arab Emirates
IDS	Intrusion Detection System
IEDs	Improvised Explosive Devices
IEEPA	International Emergency Economic Powers Act of 1977
IND	Improvised Nuclear Device
INFORMS	Institute for Operations Research and the Management Sciences
INR	Bureau of Intelligence and Research
IPCC	Intergovernmental Panel on Climate Change
IPS	Incident Planning System
IPv6	Internet Protocol Version 6
IRGC	Islamic Revolutionary Guard Corps
ISAC	Information Sharing and Analysis Center

ISP	Internet Service Provider
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
JFCOM	Joint Forces Command
JHU	The Johns Hopkins University
JIATF	Joint Interagency Task Force
JTF-CND	Joint Task Force on Computer Network Defense
JWICS	Joint Worldwide Intelligence Communications System
LAAUSC	Latin American Anti-U.S. Coalition
LANL	Los Alamos Nuclear Laboratory
LTCM	Long-Term Capital Management
MEND	Movement for the Emancipation of the Niger Delta
MIA	Missing in Action
MIM	Mine Warfare
MIT	Massachusetts Institute of Technology
MIW	Mine Warfare
MMS	Minerals Management Service
MOA	Memorandum of Agreement
MORS	Military Operations Research Society
MOTR	Maritime Operational Threat Response
MPICE	Measuring Progress in Conflict Environment
MSFD	Multi-Service Force Deployment
MTSA	Maritime Transportation Security Act
NASA	National Aeronautics and Space Administration
NASDAQ	National Association of Securities Dealers Automated Quotations
NATO	North Atlantic Treaty Organization
NCC	National Counterterrorism Center
NCPC	National Counterproliferation Center
NCTC	National Counterterrorism Center
NDIA	National Defense Industrial Association
NERC	North American Electric Reliability Corporation
NGO	Nongovernmental Organizations
NIC	National Intelligence Council
NIE	National Intelligence Estimate
NII	Networks and Information Integration
NIO	National Intelligence Officer
NIPP	National Infrastructure Protection Plan
NNSA	National Nuclear Security Administration
NNSA	National Nuclear Security Agency
NOAA	National Oceanographic and Atmospheric

	Administration
NORA	Nonobvious Relationship Awareness
NORAD	North American Aerospace Defense Command
NORTHCOM	Northern Command
NPC	Near-Peer Competitor
NRC	Nuclear Regulatory Commission
NRF	National Response Framework
NRF	Nuclear Resonance Fluorescence
NSA	National Security Agency
NSC	National Security Council
NSP	National Security Professional
NSPD	National Security Presidential Directive
NSPE	National Society of Professional Engineers?
NSWC	Naval Surface Warfare Center
NUSC	Naval Underwater Systems Command
NYSE	New York Stock Exchange
OASD(NII)	Office of the Assistant Secretary of Defense for Networks and Information Integration OASD(NII)
ODNI	Office of the Director of National Intelligence
OIA	Office of Intelligence and Analysis
OIF	Operation Iraqi Freedom
OMB	Office of Management and Budget
ONR	Office of Naval Research
OPEC	Organization of Petroleum Exporting Countries
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OUSD(D)	Office of the Undersecretary of Defense for Policy
PA&E	Program Analysis and Evaluation
PCC	Policy Coordination Committee
PDB	President's Daily Briefing
PDD-63	Presidential Decision Directive 63
PLA	People's Liberation Army
PVT	Polyvinyl Toluene
QDR	Quadrennial Defense Review
QNSR	Quadrennial Homeland Security Review
R&D	Research and Development
RADHARD	Radiation Hardening
REPP	Radiological Emergency Preparedness Program
ROE	Rules Of Engagement
SAIC	Science Applications International Corporation
SAIS	School of Advanced International Studies
SCADA	Supervisory Control and Data Acquisition

SCDA	Supervisory Control and Data Acquisition
SEC	Securities and Exchange Commission
SIGINT	Signals Intelligence
SLOC	Sea Lines of Communication
SME	Subject Matter Expert
SNM	Special Nuclear Material
SOLIC	Special Operations/Low-Intensity Conflict (Assistant Secretary of Defense)
SOUTHCOM	South Command
SRFC	Senate Foreign Relations Committee
SS7	Signaling System No. 7
SSP	Sector-Specific Plan
STRATCOM	Strategic Command
SWF	Sovereign Wealth Fund
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TALF	Term Asset-Backed Securities Loan Facility
TARP	Troubled Assets Relief Program
TCP/IP	Transmission Control Protocol - Internet Protocol
UAE	United Arab Emirates
UAV	Unmanned Aerial Vehicle
UCLA	University of California, Los Angeles
UEI	Undersea Energy Infrastructure
UNH	University of New Hampshire
URW	Unrestricted Warfare
USAID	U.S. Agency for International Development
US-CERT	United States Computer Emergency Readiness Team
USCG	U.S. Coast Guard
USCG HQ	Coast Guard Headquarters
UUV	Unmanned Undersea Vehicle
VTC	Video Teleconferencing
VV&V	Validation, Verification, and Accreditation
WMD	Weapons of Mass Destruction
WMDD	Weapons of Mass Destruction Directorate