TRANSNATIONAL THREATS: BLENDING LAW ENFORCEMENT AND MILITARY STRATEGIES

Edited by
Carolyn W. Pumphrey

November 2000

*****

*****

I would like to acknowledge a special debt to the following persons: Richard H. Kohn and Peter D. Feaver, the outgoing and incoming Executive Secretaries of Triangle Institute for Strategic Studies (1999-2000); Douglas C. Lovelace, Jr., Director of the Strategic Studies Institute (SSI), U.S. Army War College, who conceived this conference and assisted every step of the way; Colonel Bernard F. Zipp of SSI, with whom I worked closely in organizing the conference and who bore all my shortcomings with great patience; Rye Barcott (conference rapporteur) and Jonathan Phillips (transcriber), both of the University of North Carolina at Chapel Hill, without whose excellent and timely assistance my own task as editor would have been so much harder; and Joseph Caddell of North Carolina State University who, as always, provided invaluable critical input when it was most needed.

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute, U.S. Army War College, 122 Forbes Ave., Carlisle, PA 17013-5244. Copies of this report may be obtained from the Publications and Production Office by calling commercial (717) 245-4133, FAX (717) 245-3820, or via the Internet at rummelr@awc.carlisle.army.mil

*****

Most 1993, 1994, and all later Strategic Studies Institute (SSI) monographs are available on the SSI Homepage for electronic dissemination. SSI's Homepage address is: http://carlisle-www.army.mil/usassi/welcome.htm

*****

ISBN 1-58487-037-0

CONTENTS

Foreword v

1. Introduction
Carolyn W. Pumphrey 1

2. An Overview from Law Enforcement's Perspective
Spike Bowman 19

3. Transnational Threats: U.S. Military Strategy
Daniel S. Roper. 41

4. Information and Terroristic Use of Mass Weapons: The Larger Context
Kenneth A. Minihan 51

5. Intelligence Problems as They Relate to International Crime Organizations and Drug Trafficking
William J. Olson 57

6. Transnational Threats Vis-`a-Vis Law Enforcement and Military Intelligence: Lessons on the Emerging Relationship
Elizabeth Rindskopf-Parker 65

7. Terrorism by Weapons of Mass Destruction: A Reassessment of the Threat
Bruce Hoffman. 85

8. Terrorism and Weapons of Mass Destruction: A Review and New Paradigm
Jeffrey F. Addicott 105

9. Bruce Hoffman's View of Terrorism by Weapons of Mass Destruction: Another Perspective
Victor Utgoff. 133

10. The National Information Infrastructure: The Role of the Department of Defense in Defending It
Daniel T. Kuehl 137

11. Daniel T. Kuehl's View of DOD's Role in Defending the National Information Infrastructure: Another Perspective
Phillip E. Lacombe. 163

12. Daniel Kuehl's View of Information Warfare and the Defense of U.S. Information Systems: Another Perspective
Richard Marshall 173

13. Combating Transnational Organized Crime
Phil Williams 185

14. Phil Williams' View of Criminal Organizations and Drug Trafficking: Another Perspective
Thomas V. Fuentes 203

15. Phil Williams' Views on Combating International Organized Crime: Another Perspective
James R. McDonough 213

16. Preparing for War in the Fourth Dimension: A Reality Check
David M. Crane 221

17. Terrorism and National Defense: The Congressional Perspective
William Natter 231

18. New Institutions and New Ways of Operating
Jeffrey A. Hunker 237

About the Authors 253

FOREWORD

On February 2-3, 2000, the U.S. Army War College, the Triangle Institute for Security Studies, and the Duke University Center for Law, Ethics, and National Security co-sponsored a conference in Chapel Hill, North Carolina. The conference examined transnational threats, including terrorism involving weapons of mass destruction, cyber threats to the national infrastructure, and international organized crime. The goal was to evaluate the seriousness of such threats and discuss strategies for dealing with them. In particular, the conference sought to address the question of how military and law enforcement could blend their strategies to better counter transnational threats. A secondary purpose was to clarify the role of the military in meeting challenges that transcend national borders and threaten our national interests.

This book highlights some of the main issues and themes that ran through the conference. After looking at the various threats and undertaking a risk assessment, the book considers the unique aspects of transnational threats, and then identifies the key challenges facing the United States, paying particular attention to the role of the military. To conclude, the book discusses some of the steps that should be taken to secure ourselves against transnational threats. The Strategic Studies Institute is pleased to publish this volume as a contribution to the debate on important national security issues.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute

CHAPTER 1

INTRODUCTION

Carolyn W. Pumphrey

On February 2-3, 2000, the U.S. Army War College, the Triangle Institute for Security Studies, and the Duke University Center for Law, Ethics, and National Security cosponsored a conference in Chapel Hill, North Carolina. The conference examined transnational threats, including terrorism involving weapons of mass destruction (WMD), cyber threats to the national infrastructure, and international organized crime. The goal was to evaluate the seriousness of such threats and discuss strategies for dealing with them. In particular, the conference sought to address the question of how military and law enforcement could blend their strategies to better counter transnational threats. A secondary purpose, as noted by Major General Robert H. Scales, Jr., at the start of the meeting, was to clarify the role of the military in meeting challenges that transcend national borders and threaten our national interests.

Transnational threats are major security threats for the 21st century. They are characterized by their global nature, which means, by definition, that these threats straddle both the domestic and foreign spheres. Whereas responsibility for U.S. national security threats in the past clearly belonged to the military and responsibility for domestic security belonged to law enforcement, these clear-cut divisions no longer exist. This poses some profound constitutional and security challenges. On the one hand, institutions that have developed separately must now learn to work closely together and to blend their strategies in order to ensure our nation's security. On the other hand, the division of military and law enforcement functions is closely linked to the preservation of our liberties, and the task of

merging them is fraught with hazards. In the very act of preserving our security, we run the risk of forfeiting some of our liberties. Blending law enforcement and the military is thus a vital but dangerous balancing act.

This introduction will synthesize some of the main findings of the conference participants and attendees. After looking at the various threats and undertaking a risk assessment, we will consider the unique aspects of transnational threats. We will then identify the key challenges facing the United States, paying particular attention to the role of the military. To conclude, we will discuss some of the steps that should be taken to secure ourselves against transnational threats.

A Threat Assessment.

Our starting point must be to evaluate the nature of the threats we face. Only when we understand what is at stake can we determine what we can put at risk.

Terrorism entails the use of psychological warfare to achieve political goals. The perpetrator of an act of terrorism lacks the legitimacy of a nation-state or other recognized political entity. Terrorism is thus usually (though not inevitably) classified as a crime. Contemporary terrorist networks typically are not state-sponsored. A number of terrorist acts have been perpetrated by sub-state groups, and individual terrorism is also a potential problem. The aims and objectives of contemporary terrorists are often unclear. In part, this is the result of deliberate policy on their part; anonymity enables them to capitalize on the fear and alarm generated by their violence. Their organizations are also far more amorphous than was typical of traditional terrorist groups, making them harder to retaliate against than in the past.

Terrorists today have a frightening capability in that they can now get access to (or manufacture) nuclear, biological, and chemical WMD. In the estimation of Bruce

Hoffman, they are not likely to resort to the use of such weapons for a variety of reasons. In part, it is because such weapons cost a lot to acquire, test, and manage. In part, it is because terrorists can achieve their goals just as effectively by using more traditional weapons. They must also consider the possibility that they will alienate public sympathy if they inflict massive casualties. Hoffman argues that the more likely threat may come from an unconventional chemical, biological, or radiological weapon built on a deliberately small scale. Such an attack would generate just the right amount of alarm and fear to serve the purposes of the terrorists.

Given these realities, the threat of terrorism involving WMD is, in Hoffman's view, less than generally assumed. While rapid technological innovation and opposition to perceived U.S. hegemony suggest that future terrorist use of WMD cannot be precluded, his estimate is that the threat is currently somewhat exaggerated. His assessment is not, it should be noted, fully shared by commentators Jeffrey Addicott and Victor Utgoff. In their estimation, remote though it may be, the mere chance that such a catastrophic incident might take place, makes terrorism by WMD a threat of considerable magnitude.

Cyber threats come in two varieties: information warfare and cyber-crime. Both threats are directed against the U.S. information infrastructure. The distinction between the two types derives from the intent of the perpetrator. If the attacks are carried out with the intent to disrupt or undermine the government, they constitute war. If, by contrast, they are carried out for reasons of personal or organizational gain, they are crimes.

Dan Kuehl and commentators Richard Marshall and Phillip Lacombe all stressed the seriousness of these threats. The national information infrastructure is of critical and growing importance to American economic strength, political vitality, national will, and military power. Cyber attacks, especially if they take place in the

context of more conventional military hostilities directed against the United States, have the potential to do enormous damage. Cyber crimes, too, can be immensely costly. Even if a hacker is penetrating systems for amusement rather than out of deliberate malice, the damage can be considerable. Our increasing dependence on cyberspace makes the United States vulnerable, especially as the private sector owns and controls much of the medium. We are also at risk because we awoke to the threat relatively late, because technology is changing at a pace unmatched in earlier times, and because the environment is a new one. The revolutionary new environment obliges the United States to revise many of our traditional paradigms before we can develop effective strategies. As a result, we find ourselves less well prepared to deal with these threats than with many others.

Organized crime is defined by Phil Williams as the continuation of business by criminal means. It is characterized by association for criminal purposes, corruption, and violence. The international criminal organizations of today are larger in size, scope, and power than those of earlier times. Their composition is increasingly multi-ethnic, and the criminals are showing a growing ability to cooperate among themselves. Many organizations have tremendous resources. They have tapped into the new opportunities presented by the internationalization of trade, finance, and communication. They are adaptable and flexible. They show an ability to exploit states in direct relationship to their vulnerabilities and have a flair for minimizing the risks to themselves.

From the standpoint of the United States, we are not, in Phil Williams' estimate, in direct danger. Organized crime thrives best where the state is weak and corrupt; the United States serves rather as a host-state, i.e., a state which offers good markets. Inasmuch as the intention of organized criminals is to exploit and manipulate the United States rather than destroy it, the threat is limited. As Tom Fuentes puts it, it is not in the interest of a leech to kill the blood

donor. But the threat is certainly not one that can be ignored. Organized crime threatens the stability of strategically important states by instigating corruption and eroding, if not supplanting, legitimate governments. This is no mean threat when we are dealing with states like those of the former Soviet Union that have a nuclear capability. And the profits from organized crime can also be used to bankroll other dangerous groups, including terrorists. Finally, as both James McDonough and William Olson emphasize, drug trafficking in this country exacts an immense human and financial toll.

Two features shared by all of these threats significantly add to the risk they pose. On the one hand, they are transnational and, on the other hand, they are products of the information age. These characteristics enhance their capabilities, obscure their intentions, and increase our vulnerabilities.

Information age technologies provide organized criminals, hackers, and other enemies with all the advantages that the rest of us also enjoy, including greater organizational flexibility and the ability to hide. The transnational nature of the threat creates jurisdictional complications which play into the hands of our enemies, permitting them to escape from justice, put their money in safekeeping, and minimize the risk to themselves in a variety of ways. The intentions of the perpetrators of transnational threats are also harder to determine than has typically been true. While the reasons for this are complex, one explanation lies in the anonymity offered by the Internet. This complicates our task because until we know what harm is intended us, it is hard for us to accurately measure the threat or choose the appropriate response. Open access to information provided by the new electronic environment has eroded some of the relative advantages the United States once enjoyed as a result of our effective intelligence-gathering capabilities. We also find ourselves handicapped because we are currently organized to deal with threats that clearly emanate from foreign or domestic

enemies. We are also conceptually oriented towards a different kind of operational environment.

If the peculiar nature of transnational threats emerged clearly from conference discussions, so, too, did the absence of real consensus as to which pose the most serious risks. This in and of itself is something of a problem since we do not have infinite resources to apply to the problem. As Bruce Hoffman noted, we are in danger of miscalculating danger. We risk either needlessly eroding our liberties or wasting valuable resources.

Challenges.

Balancing Security and Liberty. The heart of the challenge that faces us is how to deal with transnational threats and still preserve our liberties. Transnational threats are characterized by their global nature. They pose both unique security problems and profound constitutional challenges. A variety of protections exist in the United States that have historically prevented the growth of "tyranny." Protection of privacy and clear limits to military authority are among the most cherished of our liberties. However, in the face of transnational threats, these liberties sometimes seem to tie our hands. Were we less protective of our privacy, we might be better able to track our enemies; we might, for example, be able to conduct surveillance using electronic means. This, however, would bring us closer to a world dominated by an Orwellian Big Brother. Again, we fear to use the military to counter the terrorist threat because we fear that this might lead to the loss of civilian control of the military. And yet the military is perhaps best equipped financially, organizationally, and strategically to minimize the consequences of a terrorist attack. We face, that is, a twofold threat. If we underestimate the threats, we run the risk of serious, even catastrophic danger. If we overestimate them, we run the risk of sacrificing our liberties. If we are anything less than rational and objective

in our cost/benefit analysis, we may end up doing more harm than good.

This is not to say that preservation of liberties and maintenance of our security are incompatible. As Elizabeth Rindskopf-Parker stresses, the historical record makes it clear that it is possible to find a balance between the need for security and the need for protection. Not all of the limits that constrain us, moreover, are writ in stone. Some are products of recent times and specific circumstances, and can be circumvented. Provided that we understand the purposes behind our laws and remain true to them, we can adapt ourselves to the new circumstances.

Coming to Terms with a New Environment. The second major challenge of our time is how to cope with a new operational environment. We must move swiftly to adapt our institutions to the needs of the day. We are not really organized to deal with transnational threats. Nor do we have a doctrine that reflects the realities of today's threats. U.S. national defense bears the imprint of the industrial era, when technologies were far less complex and when nation-states and clearly defined national boundaries were the hallmark of political life. The speed with which we move, develop technologies, formulate plans, or anything else, is geared to slower times. Mechanisms that once served to resolve conflict, gather information, or use force are now outdated. One might think here of diplomatic frameworks, procedures, and protocols developed in an era of sovereign states, of intelligence-gathering organizations structured to meet the needs of the Cold War, or of education and training designed to equip leaders for warfare in the industrial age.

The very way we conceptualize is out of date. We are culturally unprepared to see attacks on information systems as problems in the same league as attacks involving the pulsation of violence. Much of our vocabulary is obsolete. Traditional definitions do not fit the realities of conflict in the information age. War, for example, traditionally has been understood as armed and violent conflict between

political entities. An essential ingredient is believed to be force or the pulsation of violence. Under international law, war is legitimate only if it is fought defensively, that is, in response to an attack. In the information age, however, we may suffer catastrophic damage from "attacks" that do not involve the use of force. If we do not know and have not clearly articulated what does or not constitute an attack, how can we respond in an appropriate fashion? At the very least, an absence of clear doctrine and definitions prevents us from acting with assurance and consistency.

Uncomfortable Partnerships. This point closely correlates to the previous one. The changing nature of transnational threats has made it imperative that we achieve greater cooperation at many levels—national and local, national and international, military and law enforcement, private and public. Central to the theme of this conference is the need to blend law enforcement and military strategies. The control of our communication networks by the private sector means that it must be a partner in our national defense. Similarly, cooperation between nations is vital if we are to cope with threats that, by definition, cross borders.

The challenge stems from the fact that, for a variety of reasons, such cooperation is fraught with difficulties. For one thing, it goes against the grain. Business is wary of an alliance with government, fearing that it will lead to regulation or to loss of profits. The American public is traditionally mistrustful of government; as Richard Marshall points out, the average citizen would rather let an American company intrude into its computer systems than any of the Federal agencies, even though the latter are far more carefully monitored. Intelligence and law enforcement agencies have a history of rivalry and very distinct cultures. Their processes do not work the same way, making the development of joint strategies quite difficult. In particular, they answer to different authorities and use their information in different ways. Law enforcement is primarily interested in prosecution, whereas the goal of

intelligence is to collect information in order to preempt threats. Additionally, many of the barriers that exist between agencies are the result of carefully thought out legal considerations and should be dismantled only with caution. As for international cooperation, this is made tricky by the fact that our bedfellows are not always long-standing friends. Moreover, international law is still in its infancy, and working with an infinite number of laws and jurisdictions at the least complicates the task of joint operations.

While these are certainly challenging problems, they are not insurmountable. The uneasy nature of the partnerships stems in part from the fact that different communities do not understand one another very well; as Elizabeth Rindskopf-Parker points out, they are sometimes more suspicious of one another than is warranted. Familiarity may breed respect. On a slightly different note, we should not forget that culture is formed and what has been formed can be reformed or unformed. If we examine our institutions and work out why things are the way they are, we can safely modify those aspects that are not logical. When dealing with the business world the government has leverage; the safety of our networks is clearly of critical importance to their well-being. And we should never forget that for many companies, government is their biggest consumer. As to working with the international community, it should be noted that if there are obstacles in our way, there are also a number of factors which should facilitate our task. First and foremost is the fact that almost all stand to benefit by the elimination of transnational threats.

Resources. Resource limits pose yet another challenge. Our armed services, as Jeffrey Addicott emphasizes, are already stretched thin by their existing missions. The United States must deal with transnational threats, which are widely dispersed. We also face a rather different kind of shortage. Our national security very much depends on getting access to the finest technological minds of the day, but competition with the business sector has led to a brain

drain from the public to the private sector. Our financial resources are similarly strained. Some organized criminal groups in particular are extraordinarily wealthy. William Olson notes that drug traffickers earn more every year than the United States spends on all of its counter drug efforts. The annual income of these and other criminal organizations is frequently greater than that of many governments around the world.

Our challenge is to find ways to use our existing resources wisely, minimizing waste and duplication of effort, and balancing all our disparate needs. The American public, ironically, may complicate this task. William Natter and Bruce Hoffman both address this issue. Our government is responsive to public demands. The public is, however, often reactive and emotional. It seems to have overreacted to the terrorist threat and quite possibly under-reacted to the cyber threat. When sufficiently aroused, public opinion can put pressure on the government to allocate resources in ways that are not necessarily balanced. We must find ways both to evaluate threats in a sober and logical manner and to accommodate, but not manipulate, the public fears.

The Role of the Military.

One of the goals of the conference was to consider what role the military should play in the struggle against transnational threats. As already noted, the ambiguities of the situation stem from the fact that transnational threats are neither uniquely foreign nor domestic. Terrorism always treads a fine line between crime and war. International organized crime is still largely a law and order problem as far as the United States is concerned, but indirectly touches on issues of national security. Information warfare and cyber terrorism are even more nebulous since they do not involve the use of force as this term is classically understood. But because of what a cyber attack can do to our national security, it often seems more

like an act of war than a crime. In all cases, moreover, jurisdictional and geographic boundaries are crossed by perpetrators of the threats, and networks operate both within and outside the United States.

How extensive the role of the military should be is clearly a matter of debate. For a number of reasons, many feel that the responsibilities for transnational threats should not rest primarily with our armed forces. Phil Williams makes the point that force is often "a blunt instrument"—too blunt to use against criminal organizations which are businesses and which should be hit where businesses can be hurt most (in their purses). Military organizations, moreover, are organized hierarchically and, as such, are not well suited to dealing with networks. Spike Bowman makes the point that the use of force (as for example the launching of missiles against Afghanistan) is a narrow way to respond to a problem and not particularly useful against such dispersed threats. He also points out that the use of force is not likely to be universally acceptable in the international community and thus is not going to carry the weight of other solutions. Jeffrey Addicott raises a quite different concern: the military forces of the United States are currently overtaxed and, even if they are well equipped to deal with these threats in principle, in practice they will not be of much use. These rather pragmatic arguments are reinforced by legal considerations. Since Reconstruction and the enactment of the Posse Comitatus Act, the active duty military has been prohibited from performing police duties in the United States.

This does not mean, however, that the military has no role to play. Dan Roper distinguishes between a leading role and a supporting role for the Department of Defense (DoD). The leading role must be taken only where national security is at stake. Most transnational threats do not fall into this category. An exception may prove to be information warfare. At the moment cyber threats fall into a shady area between crime and war, and our definitional ambiguities cloud our ability to assign clear responsibility to the DoD.

But, as Dan Kuehl stresses, cyberspace is critical to America's security and well-being. In his view, at least, the DoD has both a role and a responsibility, albeit in conjunction and cooperation with law enforcement and the private sector, to protect this environment from all enemies, foreign and domestic. If we do conclude that this type of transnational threat is a mission for the DoD, one of its tasks will be to develop suitable new strategies. General Kenneth Minihan, for example, notes that the military might think about defending U.S. strategic sanctuaries by asynchronous means, developing an equivalent of our Cold War deterrent strategies.

For the most part, the military is likely to play a supporting role only, where the primary initiative and responsibility lies elsewhere. How this might work in detail is well illustrated by Addicott, who notes current plans to use the military in counter-terrorism. In these plans, state and local authorities still have primary responsibility to respond to emergencies within their jurisdiction, but can get extensive assistance from DoD in the event of a WMD attack. Addicott also discusses plans for the use of the National Guard and Army Reserves as primary response forces to a WMD episode. As he points out, the reserve components are not subject to the same legal constraints as the regular military.

In general, conference participants agreed that the military has much to contribute. It can provide transportation, emergency medical care, and translators. It can assist in large-scale disaster relief and humanitarian operations. It can play a constructive part in the interdiction of drugs and criminal products and make useful contributions in the area of intelligence. It can provide training to other agencies; the 1996 Defense Against Weapons of Mass Destruction Act (also known as the Nunn-Lugar-Domenici [NLD] Act), which envisions the use of DoD personnel to help local metropolitan authorities respond to a WMD event, is an example of this kind of thinking. Finally, the DoD has developed useful concepts

and functional strategic approaches. It has developed models for jointness which could provide very useful insights to other groups as they seek to learn how to work together. It already has provided a model which has modified the way law enforcement understands intelligence.

Overall, however, there was considerable agreement among conference participants that the role of the military in dealing with transnational threats should be a limited one. In their view, the experience of the military is its most valuable asset. And, except when dealing with information warfare, it should play a supporting rather than a leading role.

Agenda.

The purpose of the conference was to define the nature of transnational threats and to consider how best to meet these threats. The conference participants offered a number of general principles as guidelines for action as well as a number of concrete proposals. These, interestingly, fit rather well with some of the programs and strategies that are already being implemented by the government. The chapters by Jeffrey Hunker, David Crane, and Jeffrey Addicott, in particular, reflect this.

As far as principles are concerned, six stand out.

1. Widespread agreement exists that speed is vital. The hallmark of the information age is an extraordinarily rapid rate of change. To maintain our current edge, we must move faster than we have in the past in addressing a range of tasks, from fiscal planning to technological retooling.

2. Adaptability is another key requirement. This relates to the previous point; situations evolve so quickly that we do not have time to undertake massive restructuring of existing bureaucracies. Rather, we should develop flexible plans and make use of assets already in existence.

3. Jointness. Existing barriers between agencies and between the public and private sectors must be reduced.

4. Clear thinking is another essential ingredient for success. Until we gain a clear conceptual grasp of the nature of conflict in the information age, we will not be able to develop clear strategies, and our responses are doomed to be fragmented, indecisive, and even contradictory.

5. Creativity. Given the new operational environment in which we move, it is imperative that we do what Elizabeth Rindskopf-Parker calls out-of-the-box thinking.

6. Finally, it is essential that we keep within the bounds of the law, whatever the temptations might be to cut corners for security's sake.

Proposals for Action.

Suggestions as to how to improve our abilities to deal with transnational threats are too numerous to list in their entirety, but a few deserve mention because they were frequently reiterated in the course of the meeting.

Interestingly enough, one of the points to emerge quite strongly and from a variety of sources was the need to be respectful of the law. This is significant, because as danger looms large, it is easy to betray this principle. The fact remains, however, that remaining true to our constitutional principles at home and fostering democratic principles and the rule of law abroad are likely to serve us well; they garner respect for agencies like the Federal Bureau of Investigation and will ultimately help address the root causes of international violence and crime. Corruption, it was noted, is the soil in which crime grows, and terrorism is rarely, if ever, the tool used by democratic states.

Along similar lines, it was noted that international law and diplomacy promise to offer some real advantages over the use of force as a means of countering transnational threats. At the moment, however, many existing

mechanisms for conflict resolution are geared to the existence of sovereign states. As a result, in the borderless environment that characterizes transnational threats, it is often extremely difficult to know with whom, or in what manner, to carry on negotiations. It is clearly imperative that we develop avenues of conflict resolution that better reflect current realities.

A number of recommendations were made as to how to make better use of our limited financial resources. At the top of the list was the call for improved financial planning. The government lacks a clear plan outlining how to deal with transnational threats and establishing logical priorities. As a result, spending by Congress tends to be reactive, directed against whatever threat is in the headlines rather than to the best programs. Research and Development tends to be market-driven. Steps should be taken to ensure that resources are applied in such a way as to address specific weaknesses. Special attention should be paid to meeting our technology needs. On a slightly different note, international financial controls should be established to make it harder for criminals to transfer money. This would make their activities less lucrative and not only hit them where it hurts—in their purses—but would undercut some of the resource advantages they currently enjoy.

Another theme to emerge with clarity was the need for rather substantial organizational reform. Conference participants here targeted the U.S. intelligence community. There was considerable agreement that its current structure prevents it from dealing with transnational threats in anything other than a fragmented and patchwork way. There was less agreement as to what to do about this. Some participants suggested a massive restructuring along the lines of the National Security Act of 1947. Others felt that this would not be feasible, given the entrenched nature of the existing bureaucracy. They recommended a more remedial approach such as opening up lines of communication between the different government agencies.

The need for planning and vision was another theme to emerge with frequency. Congress needs to be given a plan for how to deal with transnational threats. This should be clear, comprehensive, and well crafted. This will make it less susceptible to pressure groups and be proactive rather than reactive in how it handles threats. The government also needs to be able to present to industry a vision of our national security needs. And the military must continue in its efforts to develop flexible plans capable of meeting rapidly evolving threats. These plans must be based on new and more fitting paradigms of war. On a rather different note, James McDonough raised an important point when he spoke of the need to develop an operational approach that would integrate regional and local efforts into a larger strategic effort.

The importance of education and training was also recognized. Several initiatives were identified as being of value and in need of further development. Jeffrey Hunker noted the existence of several pilot programs designed to bring into the federal government a cadre of highly skilled information technology security professionals, including the creative scholarship for service program whose purpose is to attract young people to careers in this area. Spike Bowman noted some interesting programs that are being undertaken to train other nations in investigative techniques so that they may be better able to assist us in our common efforts to combat international organized crime. The conference participants also stressed the value of education. Federal authorities, it was agreed, need to be educated so that they more fully understand the nature of the threats with which they are dealing. And for many participants public education was also a priority; suggested initiatives included introducing courses on Transnational Threats to university curriculums.

Last, but not least, was the call for cooperation. This indeed may be viewed as the keynote of the conference. If we are to deal effectively with the problem of countering transnational threats, we must find ways to bring about

more effective cooperation among a whole host of different entities: cooperation between state and local government, between business and government, between federal agencies, and among nations.

Strongly emphasized was the need to forge an effective partnership between the public and private sectors. This is crucial because the private sector now controls a very high percentage of our communications networks and because business often has cutting-edge skills which we need if we are to maintain our technological superiority. Such cooperation should be based on an understanding of the mutual benefits that will accrue from a secure Internet and might come about as a result of the development of new types of institutions combining public and private groups in innovative ways.

Cooperation among defense, intelligence, and law enforcement must be improved. Threat analysis, warning, incident response, and investigation would all benefit from serious efforts in this area. Preliminary steps have been taken; the National Infrastructure Protection Center (NIPC), intrusion detection monitoring systems, and information sharing and analysis centers referred to by Jeffrey Hunker, are examples of programs that are being discussed or have been initiated. All could be improved. To ensure a better understanding between different agencies, other steps were recommended. These included mandatory rotational jobs for persons in intelligence and law enforcement communities.

There is also much legal work to be done that will enhance the ability of law enforcement to work together with other agencies. Among the recurrent themes of the conference was the need for new laws. These could help bridge the gaps between the traditional use of intelligence to prosecute criminal cases—and strategic intelligence, which is used to predict, preempt, and defend against attacks on the United States and its citizens. With such new laws in place, one of the major frustrations of today would be

alleviated: information would flow more freely and criminals would find it more difficult to escape detection. Also addressed was the need to develop international investigative and evidentiary standards as well as electronic access protocols. These steps would go some way to assist law enforcement in tracking down criminals and bringing them to justice.

Conclusion.

In sum, international organized crime, terrorism, and information warfare all pose serious threats to our national security. Because they constitute a threat that is simultaneously both foreign and domestic and because they are able to take advantage of the new high-tech operational environment, they pose rather unique challenges to our security and to our civil liberties. Dealing with these transnational threats calls for a joint effort on the part of our law enforcement and the military. It is of paramount importance that we learn how to do this and how to do it while remaining within the limits of the law.

CHAPTER 2

AN OVERVIEW FROM LAW ENFORCEMENT'S PERSPECTIVE

Spike Bowman

This is an introduction to the problem of modern transnational threats and the role of law enforcement in meeting them. Some clarification, first, is in order. Transnational threats of many kinds have been with us for years. Some of these threats are truly significant, but are ones with which this introduction will not be concerned. Espionage, for example, is a traditional transnational threat, but not one on which these introductory comments will focus. Nor will this overview be directly concerned with traditional intelligence threats, like efforts made by other countries to ferret out the secrets of our defense programs, or even such nontraditional threats as economic espionage.[1] Indirectly, however, all of these threats intersect the subjects of primary concern, making the fundamental problems encountered that much more difficult.

The focus for this introduction to transnational threats is fourfold: terrorism, international organized crime, weapons of mass destruction (WMD), and cyber crime. The purpose is to define the nature of these threats and briefly discuss the remedies available to deal with those threats. Finally, with a singular and, some might argue, parochial focus I will address the increasingly appropriate and necessary role of one traditional remedy—law enforcement—to meet and deter these threats.

Terrorism.

Terrorism, though not a new phenomenon, fortunately is still foreign to the experience of most Americans. Despite our relative insularity from terrorism, however, we have

had a few wake-up calls in the last few decades. The first time we faced a threat that significantly affected U.S. interests was in 1983 with the Beirut bombings of our Embassy and the Marine barracks.[2]

While Beirut spawned our first real challenge regarding terrorism, one that persisted throughout the 1980s, that challenge was really quite different from today's threat. Then, terrorism was still at a distance from our shores, and the state-sponsors were more easily identified. At the time, much of the collective attention of the U.S. Government was focused on merely trying to figure out who the actors were, how states were supporting them, and, occasionally, which states. We devoted a lot of energy to the issue of state-sponsored terrorism, and our anti-terrorism efforts were focused more on states than on individuals.

In the ensuing years, however, the nature of the terrorist threat changed dramatically. Nations quickly recognized that state-sponsored terrorism was an unhealthy activity and one that would make them international pariahs.[3] With an evolution born of necessity, the responsibility for terrorism devolved to large, hierarchical, and generally well-organized groups of terrorists—which received covert rather than overt funding from sponsor states. Those concerned with threat analysis concentrated their attention on the activities of large terrorist groups such as the Hezbollah, the Hamas, and others. They focused, in particular, on locating the whereabouts of the leadership and the members. To a large extent, concern remained with states who funded these organizations.

Today, with evolutionary logic, those engaged in terrorism represent a further devolution of responsibility and organization. Hamas, Hezbollah, and other large groups associated with terrorism have taken on roles more commonly associated with states. They are energetic fundraisers; they organize people, build hospitals and schools, provide social welfare, etc. For the same reasons that states could no longer afford to be associated with

terrorism, the large, organized groups usually seek to distance themselves from overt acts of terrorism, although they do claim responsibility for terrorist acts from time to time.[4]

The result is that terrorist actors today are more loosely organized than they have tended to be in the past. Some, it is true, do retain a degree of homogeneity. Osama Bin Laden's organization is a case in point. Though loosely structured, it nevertheless is held together by a rudimentary hierarchy and a lot of money.[5] Many groups around the world, in contrast, organize on an ad hoc basis. They may be homogenous, or they may be drawn from a variety of different terrorist groups; the Palestinian Islamic Jihad (PIJ), the Hezbollah, the Hamas, and others may contribute the occasional "pick-up" terrorist. When they do organize like this, it is often so they may work together for a specific purpose and to engage in a specific operation.[6] This devolution of authority makes them particularly difficult to deal with because the terrorists become harder to identify. More than ever, it is hard to determine who the terrorists are, where they are, where the hierarchy is located, and who is in charge.

International Organized Crime.

Organized crime is nothing new to Americans. Those of us who grew up on the East coast were raised on stories of the Mafia. We all saw the *Godfather* movies, which were largely based on fact. But organized crime is no longer quite the same as it was 50 years ago. Protection rackets are no longer the bread and butter of organized crime, whiskey smuggling is an arcane memory, and computers are replacing guns. Perhaps more significantly, however, whereas terrorist organizations have tended to become smaller over time, criminal organizations, aping the growth of large international corporations, have tended to become larger.

Organized crime has become so ubiquitous it is impossible to define the scope of it for any but limited purposes. For this primer on transnational threats, the focus will remain on a small number of very large organized crime groups. Six of them stand out—the Italian Mafia,the Russian mobs, the Mexican and Colombian cartels,the Japanese Yakuza, and the Chinese Triads.[7] Though there are others, these six are especially noteworthy in that the groups are large enough and have a sufficiently well-structured hierarchy to be able to organize large logistical networks and even to work together for profit. They can trade knowledge and expertise, offer each other protection, and even trade drug routes with one another.[8] To give just one example, during the early 1990s, at the end of the Cold War, we observed numerous Italian organized crime figures at work in Eastern Europe. They were teaching the Eastern Europeans how to become organized and make crime a business.[9]

International organized crime is frightening. It poses a serious potential threat to both political and economic institutions throughout the entire community of nations. The Russian mobs offer an illustration of the extent of the problem. Organized crime in Russia and Eastern Europe has expanded to an alarming degree. According to police from Eastern Europe and Russia (with whom the Federal Bureau of Investigation [FBI] works on a daily basis), *50 percent* of their banks are controlled by organized crime.[10] Where the rot has set in, countries must deal with entrenched corruption—the corruption of elected officials, of leaders, of the military, corruption, in fact, of all social institutions.[11] In the case of Russia and Eastern Europe, this could eventually lead to the creation of a series of oligarchic criminal states. Russia alone could develop into a criminal-syndicalism state that spans no less than 12 time zones. The consequence for economic relations worldwide is obvious. Moreover, the already fragile control mechanisms for an increasingly unstable nuclear arsenal represent a frightening concern for the entire free world.

Weapons of Mass Destruction.

WMDs are increasingly a concern for Americans. It is hard to pick up a newspaper today without finding at least one story involving a WMD threat. One of the best known incidents took place in Japan where members of the Aum Shinri Kyo cult unleashed a nerve gas attack in the subway on March 20, 1995.[12] This event demonstrated the frightening ease with which WMDs can be employed by terrorist groups or even disgruntled citizens. The ongoing drama in Iraq has highlighted another aspect of the problem, which is the difficulty of locating and identifying the exact nature and scope of highly portable WMD threats. The weapons inspections teams assigned the task of locating and destroying Saddam Hussein's WMDs have been seriously frustrated in their efforts.[13]

Nor is America itself immune from WMD threats. On the home front, the explosion in Oklahoma City made it clear that putting together a weapon of mass destruction is a relatively simple matter.[14]Just recently, the FBI caught two men in Miami with ricin, a very deadly poison.[15]This material has no legitimate uses, which should, in theory, make it very hard to obtain. Yet the FBI has had several cases concerning it in the past few years. An Ohio man recently ordered three vials of bubonic plague bacteria from a pharmaceutical company and was able to get them.[16] The FBI responds weekly to anthrax threats. Although these, so far, have turned out to be hoaxes, the number of these is, in and of itself, indicative of the extent to which the resort to WMD threats is being contemplated.

Cyber Crime.

The cyber age is demolishing paradigms. Traditionally, counterterrorism operations have been directed towards physical threats. Similarly, criminal enterprise has normally occupied a physical dimension. Today, however, a new reality is dawning. Many of the harms that once were wholly physical in nature can now be visited on us

electronically and anonymously. Financial transactions can now be instantaneous and anonymous. Information, the basis for commerce, can be transferred instantaneously and without leaving a trail, even innocently, as by academic exchange. Computer technology has made our service sectors vulnerable.[17] Cyber threats pose a danger to our power grids, our air traffic control systems, pipelines, emergency services, and a host of other communications systems.[18] Moreover, the incidence of identity theft has been on a spectacular rise.[19]

The cyber threat has been driven by our own desires. Commercial industry needed to find effective ways to transfer money and information, thereby taking better advantage of world markets.[20]This led to the dramatic and rapid mastery of cyber space. As the cyber highways became busier, however, economic and industrial espionage also increased to the point that they virtually became industries of their own. The threat from espionage of this sort has become so acute, indeed, that in 1996 a new federal statute was enacted to address the problem.[21]The statute has two different applications as regards those engaged in espionage. It applies, on the one hand, to the individual working on his own for a commercial purpose or for a company, and, on the other hand, to a person working on behalf of a foreign power. The statute calls for different penalties depending upon whether the person involved in espionage falls into the first or the second category. The person working for a foreign power is punished much more substantially than the person working solely for the private sector.

Dealing with Transnational Threats.

Terrorism, organized crime, WMD, and cyber threats have much in common. None of the threats are confined by borders—hence the fact that we speak of them as *transnational threats*. In fact, organizations engaged in such activities have every incentive to spread out as far as

they can, extending across borders to diffuse national responsibility and capability to keep them in check.

The transnational threat poses a unique set of problems. In the first place, it is hard to enforce any kind of legal mechanism across borders. Nations tend to guard their sovereignty fiercely and dislike it when foreign nations intervene in their affairs, even if it is to deal with a problem that afflicts both parties alike. In the second place, it permits the members of such organizations to escape responsibility for their actions. Since the nerve center of a group like the Russian mobs or the Hezbollah cannot be found, one cannot target it with sufficient certainty to make the criminal members believe there is a probability that they will have to pay for their actions.

Taking this as a given, what are our options when it comes to dealing with transnational threats? Our first, and always preferred, option is to use diplomacy. Since the late Middle Ages, this has been the traditional starting point for solving problems between nations. In 1648 the Peace of Westphalia set the pattern for future conflict resolution by establishing the idea of national sovereignty defined in large measure by physical borders.[22] The treaties arising from that event determined that nations would be sovereign within borders; that nations would deal with each other as physical entities; that they would exchange diplomats and negotiate with each other as equals, regardless of size or stature.

Unfortunately, when nations deal with transnational threats of the sort we have been discussing here, diplomacy proves to be largely inoperative. There is no sovereign-to-sovereign contact. There are no opportunities to do business with or negotiate with members of the other party. There is no framework, no procedure, and no protocol with which to work.

Other state-to-state persuasive tools are equally ineffective when it comes to dealing with transnational threats. For example, a second option normally available to

resolve international issues is to encourage the international community to bring political pressures to bear in order to bring about change. Like diplomacy, however, political persuasion holds no utility whatsoever when dealing with amorphous, dislocated, and dispersed transnational threats.

Economic sanctions are a third frequently used option. Economic sanctions, even in the best of circumstances, have rarely proved to be a highly effective tool. Nations have a way of belt-tightening that withstands this recourse more often than not.[23] For the transnational threats we face today, however, it is virtually useless as a means of coercing organizations, which lack a vital nerve center.

A fourth method of responding to transnational threats is, of course, the use of force. Launching missiles into Afghanistan in response to an act of terrorism is, in the view of this author, a legitimate way of responding to the problem.[24] Legitimate or not, however, it is also a very narrow way of responding to any problem. It offers only a limited solution and one which has proved to be effective more often when followed by political reconciliation, which, of course, presumes a polity with which to reconcile. Because the threats we view in this forum are so decentralized and physically dispersed, military force will have minimal deterrent effect and likely will be useful only when it can be used to physically stop the terrorist or WMD event. It is far less likely to be effective in combating organized crime or cyber intrusion.

This brings me to the fifth traditional option to remedy the international threat—law enforcement. The existence of defined borders has serious implications for law enforcement. They make it difficult for law enforcement agencies to deal with transnational threats. Just like the military or the private person, the police officer has to stop at the border. He has no jurisdiction beyond his own territory. As a result, law enforcement has always been the least favored means of dealing with transnational threats.

It is what we might call the poor stepchild of the traditional responses to international problems.

The Role of Law Enforcement.

The Limitations of Law Enforcement. The constraints faced by law enforcement in dealing with transnational threats should be fleshed out here in a little more detail. First, to some degree, domestic law, foreign law, and international law will inevitably be somewhat mismatched. Our domestic laws in the United States do not always take into account international law and, in fact, some of our domestic laws, or their implementation, deliberately ignore traditional international law.[25] All domestic laws account for the unique needs of each nation. The result is that every country in the world will find it difficult to apply domestic laws when the causes and/or actors are transnational.

Naturally enough, this characteristic of Westphalian politics means that a continuing problem will be jurisdiction. When U.S. law enforcement agents travel abroad, their guns and their badges stay at home because they are not, by international or foreign laws, authorized to exercise the trappings of sovereignty within the boundaries of another sovereign nation. Jurisdiction, by definition, is consigned by a sovereign, and even if it is extended beyond the sovereign's borders by domestic law, foreign nations need not, and virtually never will, recognize that presumed authority within their own sovereign territory.[26]

Another problem is venue. How does one determine where to hold the trial of a member of an international organization? If, for example, we look at the organized crime entities that blanket all of Eastern Europe, we find it remarkably difficult to answer very basic questions. Where *is* the crime taking place? (Usually it is occurring in a series of places.) Who *is* responsible? Choosing the venue, moreover, proves to be a major problem because, once again, venue is tied to the sovereign border.

Another obstacle in the way of law enforcement agencies is their limited access to information. It is vital that they know what is happening. Yet, to get a clear picture of transnational threats, they must rely on external resources, both foreign and domestic. A federal agency seeking to curb the criminal activities of drug traffickers, for example, must know where the players are. Law enforcement officers have to know what methods are being used to control people. They have to know how and when the money of drug organizations is being transferred. They have to know what the drug routes are. Vexingly, such information is often very hard to obtain when it must be obtained from sources located beyond one's own sovereign borders.[27]

The collection and use of evidence pose another problem. It is extremely difficult to bring international criminals to justice in the United States, in part because our requirements for criminal evidence are so strict. If the FBI wants to use information it has obtained from another country, first the Bureau and then the courts must ascertain that it is reliable. If the FBI does not know the source of its information, it often cannot use it in court. Calling on foreign witnesses also poses difficulties. Even if willing and available, they must come to the United States in order to testify and present evidence.

Finally, extradition is always a challenge. Extradition from one country to another is a technique that, once again, is tied to the Peace of Westphalia. It is a very cumbersome process.To some extent, the United States has been able to deal with this and several of the other problems by executing mutual legal assistance treaties (MLATS). MLATS harmonize U.S. laws with those of other countries to the extent possible. Such bilateral arrangements do help facilitate the transfer of witnesses, extradition of suspects, and collection of evidence.[28]

The Utility of Law Enforcement. The reality is that there are many reasons why law enforcement is not always an effective tool to use against transnational threats.

Nonetheless, for all of the limitations, and there are many, it is a tool that we ought to take very seriously. Why?

First of all, the threats we are examining here are universal threats. All of the civilized countries in the world are faced by the same problems we are. Most nations, in fact, are threatened to a far greater extent than we are.[29] Organized crime, for example, is a much bigger problem in Eastern Europe than it is in the United States. Regardless of the size of the problem, nations share transnational threats in common, giving them a common purpose in working together to eradicate or at least diminish the threats.

In addition, despite the fact that all nations have different laws, most of the countries of the world do criminalize the same type of activity. Murder, burglary, and crimes of that nature are widely condemned and formally criminalized. Hence we at least have some basis in law for cooperation. Similarly, police, for the most part, have a common purpose worldwide. For most of our lifetimes, the great enemy of the United States was the Soviet Union. Yet today, the FBI works on a daily basis with the Ministry of the Interior (MVD) in Russia, assisting them in their struggle with organized crime.[30] This type of cooperation is increasingly common throughout the world. There are honest law enforcement officers all over the world, and they are fighting for the same thing—preserving the institutions of government, law, and civilization of their country.

Additionally, other remedies are simply not proving effective. Some remedies, such as military force, are effective for a brief moment. They provide a temporary solution for a particular problem. If, however, we wish to find a way systematically to control transnational threats, we must do so on a legal basis. Law provides the foundation for human society, and criminal law is internationally acceptable. A solution rooted in international law will be much more acceptable to the international community than any other type of remedy we may attempt. Launching

missiles into Afghanistan was certainly permissible, certainly lawful, and certainly, whatever the critics may say, a morally responsible thing to do. It was not, however, universally accepted. On the other hand, when we arrest terrorists or international criminals and try them, that is accepted.[31]

Finally, law enforcement promotes the rule of law. The significance of this cannot be overestimated. In the final analysis, the rule of law offers the best chance for all of us. This is what the developing countries of the world are looking for. They are trying to find a stable basis on which to build their society. Promoting the rule of law plays a key role in assuring them that they will eventually achieve stability.

Proposals for Action?

It is useful to consider some brief suggestions as to how law enforcement may be used to deal with transnational threats.

Develop international financial controls and legal standards. One of the serious problems confronting us at the moment is that criminals have the ability to transfer money all around the world with total anonymity International financial controls need to be established to deal with this problem.[32] Our national laws must be harmonized with standards acceptable to the international community.[33]

We need to develop investigative and evidentiary standards that will transfer from one country to another. One way to accomplish these goals is through education and training. We have, in fact, already founded a law enforcement academy in Budapest and are building another one in Thailand. We also bring foreign nationals engaged in law enforcement activities to study at the FBI facility in Quantico, Virginia. These initiatives serve a dual purpose. On the one hand, they help build relationships. On the other hand, they help law enforcement agents develop the

necessary expertise in carrying out criminal investigations, teaching them how to preserve evidence on a day-to-day basis.

We also need to deal with cyber crime. Here law enforcement can play an important role by developing electronic access protocols. We simply must find a way to determine more effectively, more efficiently, and more quickly the origin of cyber threats. This is quite difficult. Once again, it the transnational nature of the threats in a world defined by national borders that compounds the problem. While law enforcement agents can relatively easily determine the immediate source of an attack, it is rare that they can determine its ultimate source. They may be hot on the scent of a trail only to find themselves stopped at the border. By the time they have negotiated the right to proceed, the trail is cold. We need, therefore, to find some way of getting countries to work together so that law enforcement agents can follow the thread of a crime all the way to a resolution.

Education and training. Worldwide training is also needed in the fight against cyber crime. We are making some progress in that direction. The FBI, as noted, has developed some educational programs. So has the Department of Defense (DoD). Worthy of mention here are the efforts made by the Marshall Center in Europe to develop social programs that will foster democracy.[34] More, however, can and should be done.

Here in the United States further education and training are likewise needed in a variety of areas. More time and energy should be devoted to helping Federal agents and state and local authorities understand the nature of the threats facing them and how to handle them.

Interagency cooperation. Law enforcement agencies and other agencies need to learn how to work together to find solutions to the transnational threats. We need, for example, to have a coordinated surge capability. The police cannot handle all existing problems. In the United States,

the FBI has the authority and (at least within this country) the venue to deal with threats. However, we do not have the logistical ability to move everything where we need it. We need, therefore, the assistance of all the different branches of the U.S. Government. Many of them have a lot to offer. The DoD may be something of a 600-pound gorilla, but it can provide the logistical support needed in a time of crisis.[35] We need the expertise of the Environmental Protection Agency and Department of Health and Human Services. We need the help of FEMA whenever there is a disaster.

Of course, this is not a new concept. Federal agencies already work together to deal with transnational threats—the task is to improve the synergy. Members of different agencies practice and run exercises together, for example. However, such coordination efforts are still in their infancy. We need a lot more practice; we need many more joint exercises; we need to have far more determination.

Fiscal Planning.

Of course, we must find a way to fund such coordinated efforts. When we respond to an Oklahoma City bombing or indeed any terrorist attack, it is vital that we have fiscal backing. We need to give some thought ahead of time to what our needs will be. We need to develop legislation that will determine how the Economy Act will handle the multiplicity of agencies responding to a single threat.[36] To date this area has been badly neglected; the police are not very good at exploiting the entire U.S. Government in a crisis solution, even if they were funded for it, and the National Security Council has focused its primary attention on how to deal with overseas threats.

Conclusion.

In sum, terrorism, international organized crime, WMD, and cyber crime, all pose real threats to the United States. They are tricky to deal with, in part because they are

transnational in nature and because we must overcome a worldwide preoccupation with national sovereignty before we can effectively begin to counter the threats. Traditional remedies ranging from the use of diplomacy to the use of force prove to be of limited utility in dealing with this kind of threat. So, too, is law enforcement. Yet, though it traditionally has been the least favored of all remedies, law enforcement does offer some unique advantages. Above all else, it promotes a resort to the rule of law. The spread of the rule of the law is in the best interest of all nations. We should, therefore, give considered thought to how we, the government as a whole, can enhance and increase the role of law enforcement in dealing with transnational threats.

ENDNOTES - CHAPTER 2

1. Because economic espionage relates only tangentially to the issues with which this work is concerned, no direct discussion is devoted to this subject. Nonetheless, it is clearly an area of concern, particularly as it relates to cyber crime. The threat from economic espionage is on the increase, and the technologies that we share with other countries can now be used against us. Also, the number of joint ventures we see occurring today in commercial industry is significant. The idea of national ownership is virtually anachronistic today, and the transnational dispersal of proprietary information and technology simply increases their vulnerability.

2. In October 1983 some six tons of explosives were detonated in a suicide bombing that killed 241 Marines. The Marines had been sent on a mission intended to help stabilize the region; but as political events unfolded they came to be viewed by warring factions as partisan. The result was a series of sniping attacks on Marines, with the finale being this suicide mission. Often forgotten is the fact that a simultaneous bombing of the French military encampment killed 58 French paratroopers.

3. There has been a proliferation of international agreements providing that every signatory nation shall have jurisdiction over specified terrorist offenses, e.g., the Aircraft Sabotage Act of 1984, 18 USC 32 (1984) (applies to anyone who destroys a civil aircraft registered in a country other than the United States); and the Hostage Taking Act, 18 USC 1203 (1984) (resting on a universal crime principle, it allows trial whenever the offender is found in the United States). Additionally,

unlike the unaffiliated terrorist actors, a state is subject to political pressure. The G-7 nations (before Russia's entry into the Group) effectively threatened South Africa with the cancellation of air traffic because of a failure to punish terrorists.

4. The larger the group, however, the harder it is for the group's activities to escape detection. In consequence, the larger terrorist-oriented groups have not escaped designation by the Secretary of State as terrorist organizations. See Department of State Public Notice No. 3031, October 8, 1999, 64 FR 55112. Most of the claims of responsibility that come from the larger, well-organized groups are for actions directed at Israeli interests, for which they claim a military right.

5. See Bruce Austen, "An inside look at Terror Inc.," *U.S. News and World Report*, October 19, 1998, pp. 34-37.

6. A case in point may be the millennial conspiracy that was frustrated when a would-be terrorist attempted to cross into the United States in the state of Washington and was apprehended by alert Customs agents. Although we may never know for sure, a strong supposition has been that Algerian militants were engaged by Osama bin Laden to carry out an unspecified terrorist action in the United States. The forthcoming trials of those charged may yet shed more light on that event.

7. See "Mafia," Encarta Learning Zone, *http://encarta.Msn.com/index/cenciseindex/4F/04fb5000.htm*.For the Russian-speaking mobs, see, generally, J. Michael Waller and Victor J. Yams, "Russia's Great Criminal Revolution:The Role of the Security Services," originally published in the *Journal of Contemporary Criminal Justice*, Vol. 11, No. 4, December 1995. Russian law enforcement agencies, security organs, and intelligence services are institutionally part of the problem. Posted on American Foreign Policy Council web cite, *www.afpc.org/issues/crime.htm*. For the drug cartels, see U.S. Department of Justice web sites, www.usdoj.gov/dea/traffickers/colombia.htm and *www.usdoj.gov/dea/traffickers/mexico.htm*. Colombia-based drug traffickers are responsible for most of the world's cocaine. For the Japanese Yakuza, see Adam Johnson, "History of the Yakuza," posted at *http://members.tripod.com/~orgcrime/yakuzahistory.htm*. The Yakuza, tracing its origins to as early as 1612, were folk heroes, organized into crime families. As Japan modernized, so did the Yakuza, moving into construction, dock working, and even the rickshaw business. For the Chinese Triads, see Sin-Ming Shaw, "Dealing With the Godfather," *http://members.tripod.com/~orgcrime/dealgodfather.htm*. Triad origins are deeply rooted in

Chinese history. Chiang Kai-shek used warlords to take over Shanghai and to slaughter communists. Today, a former justice minister of Taiwan reports that one-fifth to one-quarter of Taiwan's elected officials are known to have criminal records or links to the mob.

8. See "Russian Organized Crime: Global Organized Crime Project," *Center for Strategic and International Studies Task Force Report*, 1997 (hereinafter "ROC Report"), pp. 42-43.

9. This observation is based on the author's experience. From 1991 to 1994, the author was assigned as an active duty U.S. Navy Captain to the U.S. Embassy in Rome, Italy.

10. This number may be too low. The Center for Strategic and International Studies pegs the figure at between 50 and 85 percent ("ROC Report," p. 2).

11. See, generally, "ROC Report" (describing corruption in all aspects of Russian life).

12.The terrorist attack by Aum Shinri Kyo, a Japanese-originated cult that was prepared to bring about catastrophic damage, has been described as follows:

> They released the deadly sarin gas in Tokyo's subways . . . . Although the leaders were captured and have been or are being tried, and the cult outlawed, recent reporting by Radio Free Europe indicates the possibility that Aum Shinri Kyo members may have acquired classified data on nuclear facilities world-wide "on behalf of" the Japanese Foreign Ministry, ostensibly to offer assistance to other authorities.

See "Could Japanese Sect Sabotage Russian, Ukrainian Nuclear Systems?" *Radio Free Europe/Radio Liberty*, *http://www.search.rferl.org/-results-en.asp*, March 30, 1998.

13. See, e.g., "U.N. vows to resume Iraq weapons inspections," October 31, 1997; "Iraq bans U.S. weapons inspectors—White House calls action 'unacceptable,'" October 29, 1997; "Iraq moves to suspend ties with U.N. inspectors," October 27, 1997; "U.N. to vote on scaled-back Iraq resolution," October 23, 1997; "U.N. workers alarmed by attacks in Iraq," October 9, 1997, *World News*, CNN Interactive at *http://www.cnn.com/WORLD/ 9710/31/un.iraq.htm*.

14. See David Kaplan and Mike Tharp, "Terrorism threats at home," *U.S. News & World Report*, December 29, 1997/January 5, 1998.

15. See David Kaplan, "Terrorism's next wave," *U.S. News & World Report*, November 17, 1997, p. 28. Ricin is 6,000 times more deadly than cyanide. It has no legitimate use, and there is no antidote.

16. *Ibid*.

17. Science Applications International Corporation (SAIC), "Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance," A Research Report for the Chief, Information Warfare Division (J6K), Command, Control, Communications and Computer Systems Directorate, Joint Staff, The Pentagon, July 4, 1995, pp. 206-208.

18. *Ibid*.

19. Jack McCarthy, "National Fraud Center: Internet is driving identity theft," posted at *CNN.com/2000/TECH/comp...g/03/20/net.identiy.theft.idg/index.html*, March 20, 2000.

20. See M.E. Bowman, "Is International Law Ready for the Information Age?" *Fordham Int'l L.J*., Vol. 19, No. 5, June 1996, pp. 1938-1939.

21. Economic Espionage Act, 18 USC 1831 (1996).

22. On October 24, 1648, the Peace of Westphalia readjusted the religious and political affairs of Europe. By terms of the treaty, the sovereignty and independence of each state of the Holy Roman Empire were fully recognized, making the Holy Roman Emperor virtually powerless and raising to the highest pinnacle of independence, the sovereign nation. See Germot Sydow, "1648—Peace of Westphalia: Turning Point in German History, *German News: The Magazine*, October 1998, cited at *http://www.germanembassy-india.org/news/GN98Okt/gn08.htm*.

23. Economic sanctions have been in existence against Iran, Iraq, North Korea, Cuba, and others for decades. Certainly there have been demonstrable effects, but none of which forced the desired results.

24. International law recognizes the right of self-defense, including anticipatory self-defense. For a contemporary review of the situation, one of the few which actually got the argument right, See Robert F. Turner, "In self-defense, U.S. has right to kill terrorist bin Laden," *USA Today*, October 26, 1998, p. 17A.

25. In 1980, the Office of Legal Counsel issued an opinion that the FBI has no authority under 28 USC 533 to apprehend and abduct a

fugitive residing in a foreign state when those actions would be contrary to customary international law. 4B Op. OL.C. 543 (1980). On June 21, 1989, the Office of Legal Counsel formally reversed the 1980 opinion, concluding that 28 USC 533 (1) and 18 USC 3052 do authorize that type of activity, notwithstanding customary international law, to include Article 2 (4) of the United Nations Charter.

26. The basic principle is that any exercise of law enforcement by one state on the territory of another is a violation of the latter's sovereignty. See, generally, F.A. Mann, "Reflection on the Prosecution of Person Abducted in Breach of International Law," *International Law at a Time of Perplexity*, p. 407, Dinstein, ed., 1989, reprinted in Mann, *Further Studies in International Law*, p. 339, 1990.

27. In our system of government, that information is difficult to obtain without foreign cooperation. Our intelligence services are capable of obtaining much of that information, but they are appropriated for foreign policy purposes, not law enforcement purposes. In many cases, those purposes are coincident, as with international terrorism and international organized crime. Still, the primary purpose of the collection effort must be for intelligence purpose, not for law enforcement. Additionally, the sources and methods of intelligence acquisition must be protected, often making use of intelligence information problematic for discovery and evidentiary purposes.

28. Extradition is carried on primarily under bilateral treaties which enumerate a list of extraditable crimes that are mutually agreed on, but which virtually always exclude political offenses (espionage, treason, etc.). William W. Bishop, *International Law*, 1971, pp. 572-577. The process is formalistic, slow, and cumbersome, and many nations exclude their own citizens from the process. All of this is a relic of a distant era. Today, Mutual Legal Assistance Treaties (MLATS) are widely being used to streamline the increasingly arcane practices of extradition.

29. Consider the problems facing Russia. A massive, ethnically diverse nation even after the breakup of the Soviet Union, Russia still spans 12 time zones, has no history of democracy but a long cultural and social tradition of black markets. The people mistrust authority, and public servants are underpaid. It is only natural that organized crime found a fertile petri dish in which to germinate in Russia. The still extant question is whether Russia will be able to survive as a democratic experience in the face of massive corruption and capital flight. The all-too-possible alternatives are a criminal-syndicalist state or a reversion to authoritarianism.

30. Director of the FBI Louis J. Freeh emphasized the cooperation between the FBI and the MVD during a speech given at the MVD Academy in Moscow, Russia, on November 19, 1997. *Http://www.fbi.gov/pressrm/ dirspch/dirspch97/moscow97.htm*.

31. To give just one example, even the pariah state of Libya has, many years later, yielded to political pressure in surrendering the accused bombers of Pan Am Flight 103. Although specific procedures were required, the resort to an instrument of international law to settle the issue is significant evidence that there is a forum in which nations can find common ground.

32. Presently there are no legal standards to control the means by which money can be electronically transferred. Until such time as electronic transfers of money consistently carry with them transactional data, the who, when, and where, information that identifies the senders and recipients, money laundering and surreptitious payments will be a fact of life.

33. Will Knight, "G-8 to clamp down on cybercrime: World's strongest nations take Net crime seriously," *ZDNet News Special*, October 14, 1999, at *http://www.zdnet.co.uk/news/1999/40/ns-10668.html*. The world's most powerful countries met in Moscow on October 19, 1999, to discuss ways to coordinate the fight against organized international cybercrime.

34.The Marshall Center is an innovative German-American partnership specializing in the resolution of Atlantic-Eurasian security issues. It offers postgraduate studies, conferences, research programs, foreign area studies, and language courses to civilian and military professionals from more than 40 countries. The Center's primary mission is to develop shared values reinforcing respect for human rights, individual dignity and integrity, and democratic institutions.

35. DoD has, for example, airlift, mobile hospitals and mortuaries, engineers, food and medical stocks, and manpower that can be brought to bear rapidly.

36. PDD-39 assigns lead agency responsibility for the crisis of domestic terrorism events to the FBI. A terrorist event, however, likely will require the expertise of various agencies of government and the transition from crisis to consequence management. The responsibility of FEMA will also require government-wide resources. The result is that most agencies of the federal government will have a role to play and all will have to be coordinated with state and local authorities where primary responsibility for many crisis and consequence management

issues reside. Great care has gone into constructing a framework within which all these organizations can work together, but no congressional attention has been paid to funding. Without legislative intervention, the Economy Act poses a significant problem. Neither lead agency, FEMA or the FBI, is funded in a way to pay for all the logistics necessary to respond to significant crisis events. For example, without Congressional intervention, it is difficult for DoD, which expends the equivalent of the FBI budget every 2 1/2 days, to forgive the expense incurred from airlift support, etc., supplied at the request of either FBI or FEMA.

CHAPTER 3

TRANSNATIONAL THREATS: U.S. MILITARY STRATEGY

Daniel S. Roper

Introduction.

Transnational threats pose an increasingly serious threat to the United States, one that calls for a serious collaborative effort on the part of those concerned with our national security. This chapter will discuss U.S. military strategy as regards transnational threats. It will provide the readers with the perspective of, though not necessarily the official position of, the Joint Staff. The Global Division, Joint Staff, Strategic Plans and Policy Directorate, of which this author is a member, was established in 1997 in response to the challenges presented by emerging transnational issues.

This chapter will focus on how the Department of Defense (DoD) responds to transnational threats. It will include three topics of special relevance to our goals. First, the chapter will provide an overview of the National Security and National Military Strategies. It will discuss what these strategies tell us about the transnational environment in which we operate. Second, this chapter will review the derived imperatives of the Chairman of the Joint Chiefs of Staff (CJCS) and the conceptual framework used by the U.S. military to address these imperatives. And third, this chapter will consider what role DoD should play. What support can DoD provide to civil authorities? What inherent challenges does it face and under what constraints does it operate? What are the specific support criteria and imperatives that all departments and agencies should consider as they tackle these problems? This chapter, in short, will not seek to offer any specific solutions. Rather, its

purpose is to help illuminate the issues and challenges before us.

The National Security Strategy and the National Military Strategy.

The National Security Strategy (NSS), most recently updated in December 1999, identifies six strategic priorities of the United States. For our purposes here, note particularly the last two:

1. To promote peace and security in key regions of the world;

2. To create an open and competitive trading system that benefits Americans and the world;

3. To strengthen international arms control and nonproliferation regimes;

4. To protect the environment and health of U.S. citizens;

5. To increase cooperation in confronting security threats to critical infrastructures and U.S. citizens that defy borders and unilateral solutions; and,

6. To strengthen intelligence and military, diplomatic, and law enforcement tools.

The NSS establishes how the elements of national power—diplomatic, informational, military, and economic—may best be used to protect American interests in the new century. The reader should note that the last two strategic priorities clearly relate to the issue at hand, that is, how to deal with transnational threats and how to maximize the effectiveness of military and law enforcement strategies.

The objectives and priorities outlined in the NSS form the basis for the National Military Strategy (NMS). The NMS is an unclassified public document that communicates to other government officials, U.S. citizens, and other

nations how the U.S. military supports the NSS. It provides military advice to the president, National Security Council, and Secretary of Defense, and offers broad strategic direction for the services and combatant commanders. It looks ahead about 5 years, basing its calculations on current or programmed forces. The NMS of Flexible and Selective Engagement was derived from the NSS. It is updated and published on an as-needed basis.

Revisions are in part driven by a continuous assessment process called the Joint Strategy Review. The Joint Strategy Review 1999 upheld the major components of the NMS through the year 2010 and beyond. The three major components of the NMS are to (1) shape the international environment through engagement, (2) respond to the full spectrum of crises in a dangerous and uncertain world, and (3) prepare now for an uncertain future through focused modernization and improved business practices. Our national military objectives are to promote peace and stability by encouraging the just, political resolution of international disputes, and to defeat adversaries who threaten the United States, our vital interests, or our allies.

The NMS characterizes our current strategic environment as one that includes transnational dangers, asymmetric challenges, regional dangers, and wild cards. Transnational dangers are defined as challenges that transcend national borders and threaten our national interests. Asymmetric challenges are defined as unconventional approaches or inexpensive means that circumvent our strengths, exploit our vulnerabilities, or confront us in ways we cannot match in kind. As with the NSS, our NMS clearly reflects our growing concern with transnational threats.

Transnational Environment.

So what does this environment of transnational threats and asymmetric challenges look like? To borrow a phrase from the distinguished politico-military analyst Yogi Berra,

the future ain't what it used to be. Analysis reveals a cluster of diverse and complex missions, showing what kind of military operations may be needed to meet national security needs in the coming decades. A list of potential operations makes clear the diverse and often noncomplementary functions that the armed forces may be called upon to perform. In some cases, the military will naturally play a leading role. National missile defense and joint force operations are obvious examples. In most cases, however, the military will play a supporting role only. The military may be called upon to engage in such activities as counterterrorism, counterdrug operations, and disaster relief. These functions combine domestic and extra-territorial requirements. American constitutional law makes a military lead inappropriate in these circumstances.

A variety of government agencies, including the military, will be involved in all of these missions. This does not mean that these agencies will have to undergo radical institutional change or even adapt themselves dramatically in order to face these challenges. But what is needed is flexibility. The government agencies must develop a clear sense of how their existing expertise and resources can be used to help carry out these missions. This includes the military.

Transnational Perspective.

Legality becomes a significant issue when our armed forces engage in operations that do not fall unambiguously within the military sphere of authority. These include operations undertaken to deal with transnational threats such as critical infrastructure protection, counterdrug, international organized crime, counterterrorism, and information operations. For the military, these are, in one or more respects, unconventional issues.[1] The Joint Staff is well aware of the complications that can arise when the military participates in such missions. Rather than waiting

to deal with such challenges as they arise, the military takes the initiative. By taking a dynamic approach, it ensures that the legal ramifications of such joint missions are considered in advance, that potential issues are quickly identified, and that the security implications of legal issues are clearly articulated. It sees to it that these concerns are addressed with minimum delay in the National Security Council (NSC) and interagency councils. It also makes a vigorous effort to see that persons both within and without the military are educated on these questions. The Department of Defense (DoD) is, perforce, limited in what it can do to counter transnational threats by constitutional parameters. The kinds of proactive measures outlined here, however, minimize the impact of these restraints. They permit DoD to make the most of its capabilities and seize the opportunities for action available to it, while still working within these legal constraints.

A Proactive, Forward-Looking Process.

These, then, are the challenges imposed by the transnational threat environment. What has DoD done and what does it plan to do to meet these challenges? The U.S. military is not taking an ad hoc approach. Military planners in DoD and JCS are systematically studying and analyzing the future. Assessment and evaluation are accomplished through annual and biannual updates of the NSS and NMS. A thorough analysis of these challenges has produced some results. DoD (with the assistance of the JCS) has drawn up a list of what it calls derived imperatives. These are the crucial steps which must be taken in order to deal with the threats we face in this new environment. It has also identified three corresponding areas on which the CJCS should focus: information operations, homeland defense and support to civil authority, and joint force training and exercises. A number of external studies, including the Quadrennial Defense Review, the National Defense Panel, the Rumsfeld Commission, and several Presidential Decision Directives, have validated the conclusions of the

DoD/JCS analysis. Recent Joint Strategy Reviews have focused their attention on addressing asymmetric challenges. They have noted that this emerging strategic dimension impacts national security and has many legal ramifications. Military planners have, in short, determined important priorities.

How does the military codify the actions and processes which must be taken in support of these priorities? Two of the most significant mechanisms are the Joint Strategic Planning System (JSPS) and the Unified Command Plan (UCP). They are proactive, forward-looking processes. They enable U.S. armed forces to shape, respond, and prepare as required by the NMS. The JSPS links the many strategy-related documents together, thereby consolidating military advice and giving it a clear and disciplined format. This advice can then be given to our civilian superiors who are ultimately responsible for making strategic decisions. The NMS, which we have mentioned earlier, plays a central role in this process. It provides, in summary form, guidance to the president and Secretary of Defense, considers results of ongoing strategic assessments, and provides broad military advice. This advice permeates all of our other key documents.

Unified Command Plan—A Conceptual Framework for Future Strategy and Policy.

The UCP offers an adaptable conceptual framework designed to meet rapidly changing challenges on the world scene. The plan is evolutionary in nature, thereby making it possible for the U.S. military to fulfil its global engagement responsibilities in the face of constant change. It lays out a flexible plan for moving forward in the direction where strategic imperatives are headed. It plans for a joint forces organization, a space and information command organization, and a joint task force concerned with the provision of military support to civilian authority for the purpose of homeland protection. As CJSC General Henry

Shelton testified to the House Armed Service Committee on March 3, 1999,

> Joint Vision 2010 (the conceptual template for how America's Armed Forces will achieve new levels of effectiveness in joint warfighting) . . . must also have an accompanying vision for how to best organize. . . . That conceptual framework . . . Unified Command Plan (UCP) 21 . . . will be included as an annex to the 1999 Unified Command Plan recommendation. UCP 21 will lay out a flexible plan to establish a Joint Forces Command, a Space and Information Command, and a joint task force to deal with the complex issues of homeland defense.

Military Support to Civil Authority.

The U.S. military is often viewed as the agency best equipped to deal with certain transnational threats. It does not, however, have the constitutional authority to play more than a supporting role domestically. It can offer its support to civil authority in the areas of logistics, training, information and intelligence, communications, and planning. The National Guard also provides leadership and has developed Regional Response Centers. In accordance with DoD Directive 3025.15, *Military Assistance to Civil Authorities*, all requests by civil authorities for DoD military assistance are evaluated for legality, lethality, risk, cost, appropriateness, and impact on readiness.

Challenges.

Over the past decade increased demands have been placed upon DoD to bring resources to bear in support of civil authorities. At the same time, increasing diplomatic, environmental, legal, commercial, and moral constraints have been placed on the actions of the military. Legal constraints are especially confining. Before military resources can be employed in support of civil authorities, various laws must be taken into account. These include Posse Comitatus, the Stafford Act, the Economy Act, and Intelligence Oversight legislation. These constraints have

the potential to limit or degrade the ability of the U.S. military to execute the NMS. The U.S. military also faces a challenge in that it needs access to critical skill sets, especially when it has to deal with threats that emerge on the scene without warning. For the most part, these are to be found in the reserve components. This simultaneous increase in both demands and constraints poses a complicated challenge to U.S. armed forces and the nation they support and protect.

Military Obligation.

The most recent UCP (October 1, 1999) established a civil support role for Joint Forces Command. This role is evolving. According to this plan, Joint Forces Command becomes involved in civil support when civil (federal) authorities ask for our assistance. At all times, this document stresses, the military must remain subordinate to the civil authorities. At no time is the support offered by the Joint Forces Command to become a military operation in the classic sense. This plan, to be sure, does not garner universal support. Some would prefer that the U.S. military play no domestic role whatsoever. This is, however, a minority view. We cannot let it prevent us from fulfilling our obligation to the nation and its civilian leaders. As Deputy Secretary of Defense John Hamre said in December 1999,

> We may never completely assuage the fears of that 10 percent of Americans who fundamentally mistrust their government no matter what the issue. . . . But we owe it to the rest—without causing undue alarm—to explain why it is better to have basic military structures and planning processes in place to support the first-line civil responder to a major domestic destructive incident.

Imperatives.

It is widely recognized that better interagency and civil-military cooperation is needed. This will call for a great deal of effort, as we know from studying the experience of

the U.S. military itself as it attempted to integrate the capabilities of the various armed services. Nonetheless, if the effort is great, the payoff is even greater. To ensure increased cooperation several requirements must be met. First, some general criteria are needed for evaluating proposed interagency responses to transnational threats. Second, the diplomatic, informational, military, and economic elements of national power (known as D-I-M-E) need to be synchronized. The doctrinal principles of the U.S. military—Objective, Unity of Effort, Security, Restraint, Perseverance, and Legitimacy—would prove valuable here. These principles are enumerated in Joint Publication 3-07, *Joint Doctrine for Military Operations Other Than War*.

Summary.

The fact that non-military issues have become so deeply entangled with the question of military legitimacy presents a complex challenge to both the U.S. military and the society it serves. It is clear that factors other than security as it has been traditionally defined are becoming relatively more important in the calculus of national policy. This chapter has outlined the NSS and NMS and what they tell us about the transnational environment in which we operate. It has reviewed the Chairman of the Joint Chiefs of Staff's derived imperatives and the conceptual framework used by the U.S. military to address these imperatives. Finally, it has discussed what support DoD can provide to civil authorities. This discussion made reference to challenges and constraints, support criteria, and imperatives for all departments and agencies. Now that the groundwork has been laid for understanding the problems, we may turn to the search for solutions.

ENDNOTE - CHAPTER 3

1. The Global Division of the Joint Staff focuses much of its attention on these issues, which appear to be non-Title 10 and yet may have unforeseen collateral or second-order Title 10 effects.

CHAPTER 4

INFORMATION AND TERRORISTIC USE OF MASS WEAPONS: THE LARGER CONTEXT

Kenneth A. Minihan

Introduction.

For the foreseeable future into the 21st century, the United States will be the preeminent military power of the world. This means that if we do face a radical physical threat to national security, it will likely arrive not in the form of a traditional military attack by a peer competitor state, but rather in the form of a terrorist attack by a sub-state entity, based upon the covert deployment of such weapons of mass slaughter and destruction as chemical, biological, or nuclear agents. In such a case, certainly we would want to identify and punish the attacker, but, far more important, we would want to deter or prevent the attack in the first place.

To have any hope for successful preemption of such an attack, we shall require prior knowledge of its mobilization, meaning we must possess a highly efficient system for gathering and interpreting the necessary information, that is, operational intelligence. Fortunately, the United States is also the preeminent information power of the world, a fact that should give us some optimism in our quest to acquire the necessary intelligence capability. Unfortunately, however, as we learn at length in reading the other chapters in the present book, the total national security environment in the United States today is not coherently and efficiently adapted to the task of ferreting out and responding to transnational threats. And almost certainly, of course, a serious weapons of mass destruction (WMD) attack upon this country would be transnational in character.

In this chapter, rather than discussing intelligence per se, I shall discuss certain aspects of the total national security environment that tend to militate against an adequate intelligence capability for preempting a WMD attack on U.S. territory. In passing, I shall also comment upon impediments to national security in general, as well as steps for their resolution.

Our generation is faced by some urgent tasks and presented with some vital opportunities. We are living at a moment of fundamental and revolutionary change. The industrial era has given way to the era of information. Given that the United States is, at the moment, one of the leaders in the technological revolution, it ought to be able to forge an operating environment that will help assure its national security. However, it has not performed some vital and necessary tasks. It has not, in particular, come to terms with what conflict is today. It lacks a clear sense of the law of conflict in the information age. Until it develops an understanding of the principles of war, defines key terms, and lays down clear areas of responsibility, the military will not be able to act with decisiveness in response to threats. If the United States fails to grasp the opportunities available, it runs the danger of relinquishing what could be a dominant role within the new operating environment of the information age. The technological playing field will be leveled, to the detriment of our national interest.

A Revolutionary Change in Conflict.

Any discussion of current threats must factor in the changing nature of conflict at the start of the new millennium. The strategic coin of the 21st century is no longer just the industrial base, but now includes our knowledge assets. This fundamental shift in what counts in war has profound implications for how we conduct our national defense. What are some of the key changes of which we should be aware?

Key Changes in the Nature of Conflict.

We have and will continue to have enormous power and technological capabilities. Even the technological difficulties that still beset us will likely be solved eventually. It does not appear as if the shortage of bandwidth, for example, will long remain a problem. But we now have to contend with a profoundly different operating environment.

The new environment is far more complex than anything we have experienced to date. It is a global environment built by the commercial sector rather than by the national security apparatus. It is also characterized by a pace of change quite unmatched in earlier eras. All of these changes are, in turn, radically transforming the nature of conflict and affecting how we must respond to future threats.

The ramifications of the new environment are many. Future conflicts will be played out not on a conventional battlefield but on a turf comprised of technologies and infrastructures. In the new operating environment, government, citizens, adversaries, and resourcess all exist within the same operating space. We no longer live in a world in which the soldier fights on the battlefield, while the innocent citizens remain elsewhere. Threats, too, are changing; whether we are looking at hackers or at terrorists, we find that power tends to be more diffused and attacks more random. Traditional means of identifying our opponents are disappearing. The new global environment leaves no smoking gun, making anyone who can operate within our space a potential threat. At the same time we find that existing paradigms for war and conflict are no longer appropriate. Take for example a concept pivotal to the laws of conflict, that of the nation-state. Such a concept becomes obsolete in the new global environment, which recognizes no boundaries. The new environment also poses challenges to existing legal norms, forcing us to reevaluate many of our rules and priorities.

As the nature of conflict changes, so too do the demands placed upon us. Who defends us and how are subject to change. Among other things, some defense initiatives that once belonged to DoD must now fall to others. Even the responsibilities of command shift; leadership needs will change. We must now find people who are knowledgeable when it comes to operating within the technology environment. And DoD must prove able to change at a far more rapid rate than ever before. Whereas in the past DoD made annual plans, it now must emulate the many modern businesses which plan continually and expect to reengineer their companies every 2 or 3 years.

Responding to the Changes.

In short, we are now dealing with a whole battlespace of physical and virtual, lethal and nonlethal, and dispersed operations. In order to deal with future WMD threats, we must seize the opportunities presented us and also meet the new challenges. In many ways, we are in a fortunate position. After all, in the past the United States invested heavily in information technologies. It contributed more than any other nation to their research and development and also was heavily involved in the planned technology expansion. As a result, we have largely shaped the current operating environment. As long as we continue to invest in information technology and infrastructure, we should be able to hold our lead. The Cold War, we should remember, was won with steady investments, not as a result of a wrenching somersault in force structure. We must approach the new challenges in a similarly patient and persistent manner.

Need for a New Analytical Model.

Among those things we need to do in order to ensure a relevant defense is to develop a new analytical model. The industrial age model, built around organizational boxes and analogues, is not appropriate. A more useful model might

take the shape of a rich technology grid. Such a grid would enable us to do the following:

1. Understand the physical network and transportation layer.

2. Decide on the investments that should be made in global technologies. (These should be those that help us shape the operating environment in such a way as to enable us to achieve our national security goals.)

3. Determine the legal ramifications.

We must also revise our understanding of conflict and the laws that govern it. As mentioned earlier, conflict in the information age transcends geographic boundaries, but we have not changed doctrine to meet the changed circumstances. We have not reallocated authorities; Commanders-in-Chief (CINCs), for example, continue to be geographically defined.

We must develop clear guidelines permitting us to react to threats. One of the most vital issues is to determine the difference between a crime and an attack. Only when we have decided what an attack is can we discuss what might be the appropriate responses to an attack. The United States misguidedly spends more time on identifying those who have damaged us than on deterring them in the first place. We might rather borrow concepts drawn from Cold War deterrent theories to develop a strategy of active defense. We might, for example, defend certain parts of our strategic sanctuary within the global infrastructure asynchronously. That is, we would give warning that certain types of virtual and physical attacks might not be met in kind. But obviously, so long as the distinctions between crime and attack remain hazy, this kind of discussion cannot even begin.

The United States must also make a more concerted effort to retain its technological advantage. At the moment it is hindered in two ways. First, DoD has failed to take adequate steps to ensure that its leadership has the

necessary technological knowledge. Second, it still follows an annual planning cycle. It must learn to think in terms of "web years," i.e., exponentially accelerated timelines, and reorganize with the same alacrity as in the business world. Only then can it avoid the danger of falling behind. If it does not seize the day and keep up with the changing environment, it may find its advantages whittled away. It is possible that in the future our enemies will achieve a level playing field. This will deprive our children of the kind of trust in their future enjoyed by the children of the World War II generation during the growth of the industrial age.

Conclusion.

For an instructive perspective, let us think back to the early years of World War II, long before the disaster at Pearl Harbor in 1941 drew the United States into war. Previous generations had prepared, at least conceptually, for the national defense. The keels of most of the battleships that fought in the war had already been laid. Elaborate plans had been written. Responsibilities were clearly delineated. The generation that went to war understood its responsibilities and the law of armed conflict. Are we now in a similar position? Were we to experience an electronic Pearl Harbor today, could we meet it with the same degee of justified confidence as displayed by our fathers and grandfathers on the eve of our entry into World War II? I fear that we could not. We must begin to repair that deficiency. We must begin now to lay down the security keels for the 21st century.

CHAPTER 5

INTELLIGENCE PROBLEMS AS THEY RELATE TO INTERNATIONAL CRIME ORGANIZATIONS AND DRUG TRAFFICKING

William J. Olson

This chapter will address the issue of international organized crime. Attention will be paid to the nature of the threat in general, and to the challenges faced by intelligence in particular. Mark Twain once described himself as an optimist who never arrived. In evaluating the problems we face and our ability to handle them, this author must confess that he finds himself in a similarly pessimistic frame of mind.

The Threat.

Why this pessimism? To understand why international organized crime poses a serious national security threat, it is important to recognize how such institutions operate and how they are changing. Until recently, major criminal organizations were largely confined to individual countries or regions. They were not viewed as transnational threats, nor did they pose any perceptible national security threats to us or anyone else. But what we are seeing, increasingly, is an internationalization of the activities of criminal organizations. This goes hand-in-hand with the internationalization of legitimate commerce because organized criminals are nestled inside of it, performing illegal acts under cover of legal operations. This is true of both business and banking. Unfortunately, as communication and commercial barriers break down, the environment becomes more favorable for international criminal organizations. It is both easier for them to operate and harder for authorities to pursue them and curb their

activities. Thus, ironically, one of the most positive developments of modern times brings with it a seriously increased threat to our national security.

International organized crime exacts an immense human toll. It undermines our financial institutions and compromises our trade processes. It is immensely costly. In the past 5 years, in the United States alone, the costs of paying out of pocket for illicit drugs and for their health care and other social consequences are somewhere in the area of one and two trillion dollars. That is not counting the cost in human misery and life. In the last 10 years, international terrorists have killed a small number of Americans and, overall, about 11,000 people. But we lose at least this number every year to the drug trafficking carried on by criminal organizations. In the United States today we find drugs on virtually every street corner, in many of our schools, and in thousands of our homes. Most of these drugs originated as a product (usually an agricultural product) somewhere overseas, and were smuggled into the United States by a variety of different means.

Those in the drug trade do not merely wreak havoc by destroying lives and wasting resources. In the process of introducing the drugs to the United States and other nations, these criminals also undermine local governments, either through threat and intimidation or through corruption. There are many governments around the world today that are wholly owned subsidiaries of criminal organizations. Other governments find their ability to deal with criminal organizations seriously compromised because their police institutions are either inadequate or are too corrupt to act. This, in turn, leads to a growing lack of faith in government. Eventually resorting to crime comes to be seen as the only way an individual can get ahead. And so the problem continues to escalate. This is not a distant concern or a remote problem.[1]

At this time, Colombia is very much on the mind of Congress, which is trying to introduce some major

legislation that will help deal with the problem. Colombia shows signs of approaching social and political collapse. Its problems are largely caused by drug trafficking fed by an American appetite for drugs. What makes the situation so dangerous is that drug trafficking is no longer exclusively in the hands of drug trafficking organizations. A number of other groups have become involved. These include insurgents, paramilitary organizations, and others. They use the proceeds of the drug traffic to fund their own activities. A variety of threats have thus become linked. Even though international organized criminals are themselves mainly just interested in money, their activities have profoundly serious repercussions and do indeed pose a major threat to our security.[2]

International organized crime poses further problems for us inasmuch as the criminals are both organized and cunning. It is important to bear in mind that one of the principal characteristics of international organized crime, as opposed to opportunistic crime or criminal conspiracies, is precisely that it *is* organized. Such organizations have some kind of hierarchical structure, even if loosely defined. It still offers significant advantages such as durability and staying power. A comparison with the business community will help explain this. If, for example, the head of General Motors were to be removed, a replacement would almost certainly be found somewhere in the corporate structure. In the case of criminal organizations, the same thing happens, which means that it is impossible to get rid of the body by chopping off the head, so to speak.

Organizations have another advantage. They have institutional memory, which makes possible growth and learning. The former leader of a Colombian drug cartel operating in Mexico was recently interviewed. We learned from him that every time there was a drug bust, the cartel sent a team to Mexico to find out what had gone wrong. Once the cartel had found out how an operation was compromised, it made sure never to make that mistake again. Other cartels have learned how to manipulate the

judicial discovery process used in American courts. When one of their members is brought up on trial, these cartels legitimately use discovery to find out everything the prosecution knows. This includes the techniques used by the law enforcement authorities to penetrate the organization and arrest the perpetrators. Cartel representatives then take that information back and apply it. The next time around, authorities will not be able to use the same techniques again successfully.

International criminal organizations also show considerable business acumen, which makes them formidable opponents. They are fundamentally business enterprises. They are organized to make money. And they do it extremely well. As a business organization, they share many characteristics with other business organizations. They are product-oriented. The Colombian cartels provide an excellent example here. They have proved themselves to be quite versatile in the way they market different kinds of products. The cocaine cartels learned from those engaged in the marijuana trade. These, in turn, had learned (and in some instances also got their seed money) from emerald smugglers.

The Colombian cartels also show a sophisticated understanding of how markets evolve. For example, they quickly recognized that there would be a market for heroin because (1) it was a depressant whereas cocaine was a stimulant; and (2) most drug consumers are drawn to multiple addictive substances. They therefore got the Colombians into the business of heroin production (making and selling it). The criminal organizations of Mexico show a similar aptitude. They are now the major suppliers of methamphetamine in the United States. They have achieved this prominence as a result of careful study of market trends. They keep the supplies of methamphetamine as plentiful and as cheap as possible. If necessary, they even hand drugs out for free in order to develop a market. They also try to diversify; they seek to dominate a market and seek alliances.

International criminal organizations have found ways to minimize their risks. This they do in part by cooperating among themselves. For example, the Italian Mafia today works with the Colombians. The Colombian cartels wanted to penetrate European markets, but it was hard to establish networks since Colombians are so few in Europe, making them conspicuous. They decided it would be better to let the Italians or Albanians market their goods for them. They provided the Mafia with cocaine; in return, they accepted either heroin or money. The international criminal organizations also look for the most suitable venue for their activities. In other words, they select the environment, particularly a law enforcement environment, that is least likely to cause problems for them, one where local laws are lax, corruption rampant, or enforcement incompetent.

The threat posed by these organizations is magnified because of their enormous wealth. Their business is growing. Drug traffickers earn more every year than the United States spends on all of its counterdrug efforts. The annual income of these and other criminal organizations is frequently greater than that of many governments around the world, and it is more dependable. So far, there is very little we have been able to do internationally that has made a dent in their ability to generate large sums of money. Moreover, they are expanding their capabilities. They are rich, powerful, and ruthless; and they threaten the sovereignty of many of the countries we call allies or with which we have to deal.

Response to the Threat.

In short, international organized crime and drug trafficking clearly pose a serious threat to our interests. The threat is one that we cannot afford to ignore, but it is also one that we are not in particularly good shape to deal with. Why not? First, we are only now beginning to take the problem seriously. It was not until the mid 1960s that we awoke to the existence of a criminal threat to the United

States. The Lyndon B. Johnson administration then admitted that there were crime families and operations in the United States and promised to pursue them, particularly the Mafia. Thirty-five years later we are in a position to say that we more or less have the Mafia under control. But we have not succeeded in eliminating it. It still exists; it still operates.

But today we are faced by a threat of a more serious nature. International organized crime poses far more significant threats than the Mafia and similar organizations of the past. If we, as a superpower with all the enormous resources at our disposal, have not been able to eliminate the operations of a criminal organization within our own borders, how much harder will it be for us to deal with criminals operating both within and beyond our borders? We are, in fact, only just beginning to develop the kinds of institutions we need to take effective action. And we cannot look for relief in this regard to other nations across the world. In most instances, they are more out-manned, out-gunned, and out-dollared by international criminal organizations than we are.

There are many factors that make it difficult for the United States to meet the challenge of international organized crime. In the balance of this chapter, however, we will focus for the most part on the problems related to intelligence-gathering, analysis, and dissemination.

First, there are major structural, organizational, and institutional obstacles that handicap us as we attempt to deal with the threat of international organized crime. This is particularly true in the area of intelligence. "Intelligence" in this context means both law enforcement information and information collected by the intelligence community. Because international organized crime is international, we have to work with the international community when we attempt to deal with the threat. We cannot enforce our own laws internationally, thus we have to work through other countries. Yet they have different legal and administrative

structures and different ways of doing business. To compound the problem, many of the institutions with which we have to deal are corrupt or compromised—when they are not incompetent, incapable, or both. Another organizational weakness is a lack of clarity when it comes to the allocation of responsibility. Who collects the information? Who analyses it? Who acts on it? Law enforcement operates by a very different set of motives and authorities than does the intelligence community. This leads, on one hand, to the wasting of what are already limited resources. On the other hand, it means that, at times, important issues fall through the cracks in the system.

Second, international criminal organizations are very adept at camouflaging their activities. As noted earlier, criminal organizations have taken advantage of the growth in banks without borders. They are taking advantage of these markets in order to to disguise their activity. It is extremely difficult to uncover criminal activity once the associated money has fled to in the international financial system.

Third, our ability to deal effectively with the current threat is handicapped by the fact that international organized criminals belong to what are, in effect, business communities. Those tasked with pursuing them and thwarting their activities are not trained and organized to operate against this kind of institution. They are used to dealing with other countries and with organizations like themselves. They are not businessmen and do not think like businessmen. Yet, unless they can think like businessmen, they will find it very difficult to anticipate the moves of these criminals and get the better of them.

Fourth, the best way to penetrate such organizations is by human intelligence (HUMINT). The United States has tended to rely too much on technical means instead. As a result, it has neglected to find better ways to collect intelligence by HUMINT. And it is clear that this will be no easy task. Criminal organizations are largely ethnically

based and use family networks to protect their empires. This means that they are very adept at avoiding penetration by outsiders.

Conclusion.

Clearly, then, international organized crime poses a threat both in terms of the damage it can inflict and in terms of our relative incapacity to defend against it. The picture looks rather bleak. However, at least there is a dawning awareness that there is a problem. A philosopher once observed that, in dreaming, we all inhabit our separate worlds, but on waking we all share the same world. And it is in waking from our separate dreams that we learn that we have a common problem or set of problems. We have awoken to an appreciation of the threat and are perhaps at the point where we will be able to work together with other nations across the world to reduce it. It is to be hoped that we will. To quote an observation by Winston Churchill, "Americans will always do the right thing—after they have tried everything else."

ENDNOTES - CHAPTER 5

1. See U.S. Department of State, *Patterns of Global Terorism*, Publication 10687, annually. In 1999, international terrorist acts accounted for 233 deaths and 706 wounded worldwide. Only five U.S. Citizens lost their lives in such incidents in 1999. Between 1994 and 1999, 68 Americans died in terrorist attacks internationally, and 613 were injured.

2. The most comprehensive source on international narcotics-related issues is the U.S. Department of State's *International Narcotics Control Strategy Report*. This is an annual report on drug production, trends, government activities, and the threat from criminal organizations.

CHAPTER 6

TRANSNATIONAL THREATS VIS-À-VIS LAW ENFORCEMENT AND MILITARY INTELLIGENCE: LESSONS ON THE EMERGING RELATIONSHIP

Elizabeth Rindskopf-Parker

Introduction.[1]

If we are ever to successfully contain transnational threats, whether chemical, biological, nuclear, cyber, or criminal, it is vital that we find some way to improve coordination between law enforcement and intelligence services. This, in turn, will require us to understand the differences in mission, legal authority, and institutional cultures that separate those responsible for national security and those who tend to domestic security. For it is these as much as anything which give rise to the tensions between the services. The role of law enforcement has traditionally been confined to domestic matters, and its mission has been to engage in criminal prosecution. By contrast, the role of military intelligence has traditionally been confined to dealing with strategic threats to the nation's security. Because their activities do not normally involve citizens nor entail prosecutions, the normal protections of the Bill of Rights do not apply. Both are committed in their own way to protecting U.S. security, yet the differences are often profound. Our challenge is to use the tension created by their differences in a creative and constructive, rather than limiting, manner.

The need for coordination between law enforcement and defense intelligence capabilities has reached a crisis point in the last decade. Geographic boundaries and jurisdictions are becoming less relevant, especially where transnational

threats are concerned. As a result, law enforcement and military intelligence find their roles overlapping in untraditional ways. Yet a crisis can be an opportunity. If both law enforcement and intelligence are needed to confront transnational threats, new ways to surmount the problem of coordination are needed; we must "think out of the box" to discover new paradigms for cooperation and new responses to the national security threats of the new millennium. Yet while bold solutions are called for, all changes in the relationship of law enforcement and defense intelligence must observe constitutional limits with care.

Entrenched ideas can and do change. In my own case, over the course of my long career in service to U.S. national security organizations, my understanding of the relationship between intelligence and law enforcement gradually evolved, and my views often took surprising turns. It took time, to be sure, but many of my basic assumptions did change. The facts I observed gradually forced me to challenge many of the fundamental legal precepts that I had first learned in law school in the 1960s and which were, as a result, deeply ingrained. It takes time for an individual to change his or her basic assumptions. It takes still longer when large agencies and whole nations are involved. But it does happen.

Moreover, I have observed others considering whether we should change the way we handle law enforcement and military intelligence. Progress in understanding the complicated issues involved has clearly been made. In 1992, for example, the understanding of intelligence within the Department of Justice was minimal.[2] Today, however, there is considerable understanding of both law enforcement and intelligence capabilities among the affected agencies.[3]

So we certainly are capable of change. But should we? My belief as to the importance of coordination does not, I must say, go unchallenged. Some analysts, in fact, doubt the seriousness of transnational security threats. Many others worry about what might happen to citizen rights and

protections if military intelligence and law enforcement work together too closely. Thus we should not seek to change the way things are before we have evaluated the threats and determined our priorities.

How can we do this? History can provide us with some guidance here. R. James Woolsey, former Director of Central Intelligence, for example, has commented that our deceptively peaceful and prosperous time is correctly understood only when compared to the 1920s—an era which, in hindsight, appears to be "the calm before the storm." Such historical reference is useful in determining where we are now, where we should go, and how to arrive safely. This is just as true for grand strategic questions as it is for tactical legal considerations. So in this chapter, I will resort to history of a very personal kind to try to shed light on these important questions. I will share with you the lessons that I learned through my own personal experiences. I will take you on a journey through my past, dwelling on those key moments when my consciousness was shaped by events. Along the way, I will broach some of the solutions that have suggested themselves to me.

Lessons.

Experience has helped me identify several problems that need to be dealt with if we are to create better coordination between law enforcement and intelligence agencies. To begin with, each of these two communities occupies a different part of the constitutional landscape, and neither knows the other's territory well. At the beginning of my tenure as General Counsel of the National Security Agency (NSA), I thought I understood the best way to protect the constitutional rights of citizens. My confidence was based on 16 years in civil rights, civil liberties, and anti-trust litigation. I thought I understood the Bill of Rights and the protection of the civil rights of citizens. With the arrogance that sometimes characterizes lawyers, I was sure there was little I could learn about protecting the rights of U.S.

persons from my new NSA colleagues. I was equally convinced, having represented draft resisters during the Vietnam War, that the military—one in five of my new NSA colleagues—could not help me. I erred on both counts.

I learned that while my NSA colleagues might learn something from my experience, the reverse was more often true. And the most important thing I learned from my NSA colleagues was that there had been effective responses to problems uncovered in the Watergate period—responses not only unknown to me but to most other informed Americans. Two new rules, in particular, had been developed in response to the Watergate scandal. These rules, I found out, were simple and comprehensive. First, U.S. intelligence may "not collect on U.S. persons." Second, U.S. intelligence "does not do law enforcement work." The entire NSA work force was indoctrinated with these two rules. As a result, the legal decisions being made by the NSA Office of General Counsel were far more careful than mine would have been. Both predecessors and successors as NSA General Counsel have told me that they experienced a similar change of heart.

In later years, this early impression—that few lawyers understood the rudiments of intelligence operations law—was repeatedly reinforced as I talked to different groups about the law of intelligence. It was inescapably confirmed as a result of the financial crisis involving the Atlantic branch of the Banca Nazionale de Lavoro (BNL)—the so-called "Pizza Connection Case."[4]

Early on, I was asked by a senior federal official why U.S. intelligence had failed to note a fraudulent wire transfer scheme involving movement of millions of dollars among accounts in American branches of an Italian bank. His question revealed ignorance of a significant Watergate reform: it is unlawful for U.S. intelligence to collect law enforcement information about U.S. persons or to investigate law enforcement concerns in the United States. Here was a major gap in understanding about U.S.

intelligence. I was stunned. If senior federal officials did not understand NSA's governing principles, how could wise decisions about the relationship between law enforcement and intelligence be made?

My surprise was colored by the fact that I had been greatly influenced by the opinions of Justice Lewis Powell in cases considering the legal role of intelligence under the U.S. Constitution. I had assumed that Justice Powell's understanding of the constitutional role of intelligence was widely shared throughout all branches of government—Congress, the executive branch, and the judiciary. In fact, I now saw that Justice Powell's sensibility was something of an anomaly. It was produced by his own unique experiences during World War II as an Army officer responsible for handling sensitive intelligence information garnered from coded German communications.

It was this experience that had enabled Justice Powell so readily to balance the demands of national security with the Constitutional requirements of the Bill of Rights and to design approaches to protect at one and the same time classified information, individual rights, and national security.

Of course there are others who, with Justice Powell, have recognized that our Constitution has two distinct halves. A domestic internal half, focused on the relationship of the government to its citizens, is embodied in the Bill of Rights. An external half, focused on the relationship of the government to its citizens protects the nation from its external enemies. Judge William H. Webster was once questioned about how he, a former federal circuit court judge, could comfortably lead first the Federal Bureau of Investigation (FBI) and later the Central Intelligence Agency (CIA). He showed a clear recognition of this division when he said in response, "Domestically, I follow all of the law; abroad, I support the Constitution."

In its external role, our government is responsible only for the protection of its citizens, not for the preservation of

their rights. I had not considered this role and so had given little thought to constitutional authorities outside of the Bill of Rights. I had had cause to reflect on the authorities enjoyed by the president in his capacity as commander in chief. When he fulfills this function and is entrusted with the duty of protecting American citizens, he enjoys his greatest power. And for the intelligence services, it is precisely these considerable authorities that are of the greatest significance. For they derive their own responsibilities and functions from the needs and demands placed on them by the president in his national security capacity.

Like the majority of lawyers, I did not appreciate the entire set of rights and obligations that our constitution imposes upon the president and upon those who "stand in the shoes" of his national security authority—like the intelligence community. Not understanding these authorities or being unaware of them, I assumed they did not exist. "Intelligence law" was an oxymoron because I only understood one half of the constitutional picture.

This gap in understanding continues to grow. Today, too many of those under 30 know about intelligence only from movies or TV—questionable sources for accurate information. For many years, a shared World War II experience gave our national leadership a common understanding about the importance of intelligence and its proper, but limited role in a democratic governmental structure. Now that consensus has been lost.

We must bridge this gap. We must relearn how—and why—our two national responsibilities (national and domestic security) are organized as they are. From such a shared understanding, we can rebuild an understanding of the requirements of our national security. We can determine what are the legal requirements of national security, whether domestic or foreign. We can decide what the balance should be between individual liberty and national security under our constitution in this new

century. If we do not do so, we will be, I am afraid, a house divided between national security and personal liberty, between intelligence and law enforcement. Transnational threats will surely endanger this balance and may require us to consider new ways of doing business. But we will not be well-prepared to make these changes unless we first understand the current structure and the reasons for it.

At a slightly later stage in my career, my sense of the gaping divide between the various communities deepened. In particular I was alerted to the fact that, if few lawyers understood the rudiments of intelligence operations law, there was equally much that intelligence did not understand about law enforcement. The painful debate on encryption export policy that has raged for over 10 years did much to crystallize this consciousness.[5]

The encryption debate revolves around the question of whether the government should intervene in order to limit the strength of encryption products. Some of these are now so powerful that law enforcement officials cannot decipher them, and this deprives them of the traditional ability to eavesdrop electronically. U.S. firms have been prohibited from exporting their best products. These measures are strongly supported by law enforcement officers, who are worried about the protection encryption offers to criminals. But privacy advocates and U.S. software makers want to keep government out of the way. I myself participated in several rounds of the struggle to formulate policy on this issue while I was at NSA.

During the second round of policy discussions, I suggested to a new NSA director that the encryption debate was less about foreign intelligence-gathering than law enforcement. The problem of unreadable encryption would be most serious for law enforcement. In contrast, NSA would find the free export of encryption more manageable. Therefore, the law enforcement community, particularly the FBI, should take the lead in designing a balanced

encryption export policy. The director encouraged me to bring this idea to the attention of the FBI.

The FBI representatives were surprised on learning that NSA could not immediately decode and read all encrypted communications—that some encryption might be too powerful even for NSA to handle in real time. This news did not inspire grave concern, however, because those attending the meeting were locally focused and did not consider wiretaps to be the critical law enforcement technique for the post-Cold War world.

This view changed dramatically with the arrival of a new FBI Director, Judge Louis Freeh, whose own personal experience with wire tap information in the so-called "Pizza Connection Case" seemed to have convinced him that the future of law enforcement would be both global and technology-driven. This new FBI Director intuitively grasped the significance of the need to control U.S. encryption exports.[6] He needed no explanation of why national security and even more so, domestic security, needed protection against the proliferation of unreadable encryption then beginning to flood the commercial marketplace. Here again, personal experience was the key to his understanding.

Yet despite Judge Freeh's deeply held personal concern, influencing a major national security policy involving the need to coordinate several large bureaucracies proved exceedingly difficult. Neither he nor the FBI were sufficiently knowledgeable about encryption technology to fashion an effective policy for many years. Instead, motivated by fear of the unknown, they prevented any change in policy. In so doing, they quite possibly damaged for years to come any productive relationships with the technology community. In contrast, while NSA understood encryption technology and was prepared to accommodate a changing world, it did not understand the needs of law enforcement or the process of policy formulation. In consequence, its actions further confused and enraged the

"high-tech" community and made it still harder to bring about constructive change.

Later, when the Department of Commerce was assigned the role of implementing a succession of new encryption policies, matters became even more confused. The Department of Commerce did not understand the underlying technology of encryption. It had to design and implement regulations which would be flexible and fair and at the same time distinguish among highly technical products whose national security characteristics could not always be predicted prior to government review. This proved to be a very difficult policy dilemma.

As the evolution of a new encryption policy progressed from 1984 to 1999, various approaches were considered. The early Clipper Chip initiative offered the public high-quality cryptographic protection embedded in hardware in exchange for the government's ability to read the underlying text, but presumably only under appropriate, legally authorized circumstances.[7] The idea was so severely criticized that it was eventually discarded. As a policy the Clipper Chip failed.[8] Although the Clipper Chip was technically innovative, those supporting it had not considered the public's mistrust of intelligence. How could so fundamental a mistake have been made? Those whose professional life is spent working on intelligence gain little understanding of policy formulation. They may not always see themselves as others do. Experience again was the deciding factor. It explains why the Clipper Chip seemed a good idea to some within the intelligence community, particularly those from a military background, accustomed as they were to positive public relations, but a very bad one to the rest of the world.

Interestingly, not everyone in the intelligence community reacted positively when the Clipper Chip program was first proposed. Some career NSA cryptographers recalled the price that NSA had earlier paid for its involvement with the communications of U.S.

citizens. One senior official reacted with great concern to the proposal. It was his view that NSA should not create a readable encryption system for public use because it would enable NSA technically to read the mail of U.S. citizens. It was, in some ways, encouraging to find this intense concern from so senior a member of NSA. At the same time, it was less comforting in that it revealed a lack of understanding about how the law controls government capabilities when citizens' rights are involved. We bar government from misusing its technical capabilities, not by preventing or eliminating these capabilities but by regulating their use under a rule of law. It is this distinction that separates a domestic wire tap from foreign signals intelligence. Lacking experience in the world of domestic law enforcement where the only protection a citizen has against intrusive governmental conduct is the law, this NSA official found the idea underlying the Clipper Chip very disturbing. Many private citizens agreed with him.

As the encryption policy debate progressed, confusion among the affected agencies and their personnel grew. Coordination became problematic because agencies seemed not to understand their own role in encryption policy development and implementation, much less that of others. An interdependent policy addressing simultaneously the needs of national security, law enforcement, and commercial regulation proved exceedingly difficult when no one player understood all parts of this policy puzzle.

Such confusion can be expected to reoccur in the future as effective yet constitutional responses to transnational threats are explored, unless all agencies involved in dealing with transnational threats understand one another. Studies and commissions on this topic have been increasing in number since the early 1990s, when several failures of coordination produced mini-scandals sensationalized by the press to prod Congress. Eventually the earlier-noted BNL matter became public, convincing many that the CIA "lied" in denying that it had information about the banks' alleged criminal wrongdoing. In fact, closer examination shows

something quite different. The CIA Office of the General Counsel was asked by the Department of Justice whether there were any reports showing "criminal conduct" by the Bank. The General Counsel's Office responded that there was no such information. It failed to mention, however, that other reports existed which were relevant to the Bank, but which in the view of the General Counsel's Office did not suggest criminal wrongdoing. When these other reports came to light, the reaction, as is almost always true when the CIA allegedly missteps, was that the Agency had been engaged in an effort to mislead the Department of Justice. This exchange had the misfortune of occurring in the midst of a presidential election; it quickly became impossible to engage in any sensible analysis as charges and countercharges of increasing intensity reverberated between the three branches of government.

In the aftermath of both the presidential election and the BNL scandal, an effort was launched to learn what had gone wrong in this matter and what could be done to avoid such failures in coordination between law enforcement and intelligence in the future when once again they needed to work together. As co-chair of this effort, I spent great amounts of time considering the issues that were preventing law enforcement and intelligence from working together. My understanding of the issues deepened. It again became clear that even the most sophisticated members of the Department of Justice, who had for years worked with legal issues relevant to intelligence, still did not really understand the process of gathering and disseminating intelligence. Nor were there formally established procedures or other points of contact to guide the relationship of these two large bureaucracies where intelligence reporting was concerned.[9] This was because the Department of Justice was not seen as an important "consumer" by the intelligence community.

Thus, when the Department of Justice posed a question to the CIA General Counsel's Office about available intelligence, the question did not fit well with the office's

legal mission. Indeed, as it turns out, the question could not properly have been answered either by that office or by the CIA as a whole.

Intelligence reporting has highly structured "channels" for its analysis, reporting, and dissemination, understood by personnel on both the consumer and collection side who have been trained in the proper handling of intelligence reporting. Intelligence is often fragmentary and inconclusive, very different from the investigative reports created by law enforcement investigators. The CIA General Counsel's Office manages the Agency's legal issues but does not perform an intelligence collection or dissemination function. It was thus not an appropriate entity to ask to provide intelligence.

For its part, no part of the intelligence collection community is trained to make judgments on what is "criminal" and what is not. Its job, instead, is to collect information relevant to topics required, not to characterize what has been collected. Thus Department of Justice had asked the wrong part of the agency for intelligence information and placed a characterization on that intelligence which collectors were not competent to provide. It did so because it was comfortable dealing with the General Counsel's Office and did not have an established relationship with the intelligence collection and analysis portions in the CIA.

Under normal circumstances the Agency's lawyers should have recognized this problem, recast the request for information to exclude legal conclusions, and referred it to the proper part of the Agency for direct handling with the Department of Justice. However, this exchange happened in a highly charged situation, amidst intense public pressure, on the eve of a holiday week-end, making thoughtful analysis of a novel situation difficult. No one took the time to analyze the situation.

In retrospect, we also learned that the Department of Justice was poorly equipped to work with even that

intelligence information which it had been receiving. Reports on apparent topics of general interest to law enforcement went unread for want of staff trained to understand its potential value.

As a result of this debacle, at the beginning of the Clinton administration, a new CIA Director and Attorney General pledged to coordinate more effectively. To do so, they initiated studies on the working relationship of law enforcement to intelligence. I was assigned to this effort, along with a Department of Justice colleague, and had the opportunity to analyze the relationship, identify problems, and recommend changes. We were mutually astounded at what we did not understand about one another's responsibilities, although we had worked together closely over many years. Importantly, our relationship had been focused on law enforcement prosecutions and other litigation, where the intelligence agencies were the governmental client of the Department of Justice. In BNL the roles were reversed. The Department of Justice became the client of the intelligence community, seeking information relevant to its mission. This had not arisen before, and structures and trained personnel were not in place to work effectively with one another.

At the conclusion of this study in 1994, a report was issued touching on many of the issues in the present book. Still we did not anticipate that the world of law enforcement would so alter that today, not only senior officials at the Department of Justice but even local law enforcement would need to understand how to work with intelligence. The study required 2 years to complete. The issues were conceptually difficult. Often we lacked a common language to explore our concerns. The same words had different meanings depending on which community was involved. For example, the two communities had very different reactions to the concept and rules for handling a "source" of information. For intelligence, a source's identity (whether a person or technical means) is something to be permanently protected. Not to do so would subject the source, whether a

person in a foreign environment or a valuable technology, to permanent compromise. In contrast, a law enforcement source typically is designed for a specific, short-term use and is expected to become public when used in prosecution and trial. These differences produced legendary misunderstandings.

Complicating this was misunderstanding about the authorities of each and the lack of a shared understanding of the constitutional conceptual framework into which each fitted. So, too, the authorities governing collection on various topics differed. Finally, for want of understanding, the two communities were intensely suspicious of one another. In sum, what members of the two communities did not know about one another vastly outdistanced what they did know.

If the intelligence and law enforcement agencies are to coordinate with maximum effectiveness while observing constitutional limits, and if the relevant agencies within these communities are to work together, common experience and a better exchange of ideas are needed. (This coordination problem also characterizes many of the historical relationships within each of these two communities. Until recently, the CIA's problems with the FBI were mild compared to those with NSA.) In our effort to protect citizens against governmental abuse of power, we have segregated power into pieces, hoping to contain that power by compartmentalizing it. The negative aspect to this approach is that it creates different systems and different cultures which are unfamiliar and often suspicious of one another. There is more than a separation of rules and authorities. In the end an "anthropological divide" and an inability to communicate separate these two communities, preventing their cooperation.

This legal, functional, and cultural separation requires forceful corrective action, not wishful thinking. From my perspective, Congress would be wise to explore legislating a personnel system where rotational assignments for anyone

seeking a mid-level management position in these agencies are mandatory. Specific—and positive—career incentives are needed to overcome the natural disinclination to leave one's "mother agency" for a rotational tour at a sister agency when such a move may prove harmful to career advancement. Without such incentives, it will be difficult to overcome the disinclination that all people have for change.

Another point is relevant here. Law enforcement and intelligence organizations are consciously structured on the model of a "fighting force." The creation of esprit de corps by building cohesion, discipline, and the ability to work effectively together is widely regarded as important. Yet this very esprit de corps can lead to an "us against the world" psychology which can be both a strength and a weakness. Where coordination is concerned, it can be particularly problematic. The isolation it promotes and the associated provincial lack of world experience also make difficult such efforts as understanding others, setting a strategic agenda, and problem-solving that is "out of the box."

Thus, besides improving coordination, mandated rotational assignments promise to offer a second benefit. The shared experiences and enhanced mutual goodwill would perhaps foster more creative thinking. Current personnel systems do not make this easy. To be sure, such a change in personnel structure would generate concerns. The fact that the various agencies have different legal structures would cause some complications. Problems would likely arise also over the sharing of classified information with those not cleared for access to all levels of classified information through different agency processes. For many years, insistence by the intelligence community that no one be provided full access to the community without meeting the community's comprehensive background checks, including a polygraph examination, was a major barrier to the type of personnel exchange I am recommending here. Gradually that has begun to change, particularly in certain "joint" activities such as the CIA centers designed to confront terrorism and

nonproliferation. Consistent pressure is needed to guarantee that this progress continues. These issues are numerous and difficult. They require a concerted and continuous effort to ensure that both the intelligence and the law enforcement communities actively engage in practices that will loosen their respective bureaucratic structures and make possible greater exchange. We can coordinate activities as appropriate, even with people of different clearance levels.

Nonetheless, personal experience teaches me that increased personnel exchanges can foster more creative thinking about the problems of transnational threats among even the most knowledgeable leaders in our military intelligence and law enforcement communities. In 1992 I chanced to meet two of the most senior and respected leaders of the national security community at a seminar on the future of post-Cold War intelligence. A paper circulated for review had said nothing about the emerging relationship between law enforcement and intelligence. Surprised, I questioned this omission and for my trouble received blank looks. In 1996, the experience was repeated with yet a third highly regarded senior expert in the field of military intelligence. These same views, when offered to law professors at several highly ranked national law schools in 1994 and 1995, were no more warmly received.

These experiences are offered not to highlight my own insight, but rather to suggest that I had enjoyed the advantage of coming from one culture into another and, with that, had been stimulated to ask fundamental questions. My point here is that even very experienced and knowledgeable people cannot understand what they have not experienced. It is their very expertise in one discipline or area, gained from a lifetime of intense and circumscribed focus, that makes coming up with new paradigms and out-of-the-box solutions difficult. The cross fertilization of two cultures as similar, yet different, as law enforcement and intelligence can be profoundly enriching. It can inspire new ways of attacking common problems, even as these two

communities continue to perform their tasks according to different constitutional and legal requirements. Nothing short of this type of mind-expanding experience is required if we want to identify the most creative responses to our problems. I think of this as stepping outside ourselves so that we can see ourselves and our problems "in the round." This is the only perspective that will be good enough as we confront transnational threats in the post-Cold War world.

The private sector is another area we might explore in our search for creative new ideas. One of the most important changes in the recent past is the realization that the private sector is now a crucial part of our national security. Government will be able to realize national security objectives such as protecting the nation's infrastructure only if it talks with private industry. Yet industry no longer is comfortable talking to the government. Why? Among other reasons, they fear that threat information shared with the government will become embarrassingly public or competitively valuable information, or that trademarks will be lost. Combined with this is a mistrust of government motives in the national security arena. Once again, this mistrust is born of a lack of understanding.

Correspondingly, the government cannot now share its classified information with the private sector. Sensitive information, whether produced in the public or private sector, cannot go back and forth readily without carefully devised regulations and procedures to protect important interests on both sides. But solutions are being explored. One of the results of President Clinton's critical infrastructure protection initiative is the notion of mixed public and private centers where both sides can exchange information with the other in a protected environment. Perhaps this approach—creating mixed-use entities—could work in other areas as well. At a minimum, as the Clipper Chip story shows, the private sector increasingly must be a part of the discussion.

Such exchanges promise do more than just facilitate coordination. The opportunity to change places and see the world from different perspectives provides us with the means to challenge our existing assumptions and think in new ways. This is vital. If we ever hope to find effective approaches to transnational threats, it is necessary that we become more creative in our thinking.

ENDNOTES - CHAPTER 6

1. The substance of these comments was originally presented during a banquet speech at the Conference on Transnational Threats: Blending Law Enforcement and Military Strategies, February 2-3, 2000. The editor chose to retain the informal style because of the personal nature of the approach.

2. At the time, even establishing points of contact for our intelligence agencies at selected U.S. attorneys' offices was problematic, if only because of the different standards imposed on access to intelligence information by both communities. The understanding of intelligence within the Department of Justice was minimal. In contrast, questions asked today even by local law enforcement representatives are quite sophisticated.

3. One law enforcement representative noted that he had found it difficult to use military intelligence to assist him in drug trafficking investigations. He asked how he could use this information in a public trial if it had to remain classified. The answer, of course, is that it is possible for law enforcement to use military intelligence while still observing the important legal and practical requirements unique to each. With careful coordination, military intelligence can point out areas of concern. Law enforcement can then follow these leads, using its own investigative techniques. This solves the problem, as only the latter becomes evidence for courtroom use.

4. This episode, in fact, eventually led to a public examination of the problem. The Pizza Connection case was an international drug trafficking case that was broken through the effective use of wiretapping.

5. For background on the encryption debate, see Dan Froomkin, *www.washingtonpost.com (Staff)*; and Amy Branson, LEGI-SLATE News Service, "Deciphering Encryption," updated May 8, 1998, at *http://www.washingtonpost.com/wp-srv/politics/special/encryption/encryption.htm*. Encryption is data-scrambling technology. The debate

centered on whether or not the government should step in and limit the strength of encryption products to maintain law enforcement's historical ability to eavesdrop electronically on anyone it wants. Current policy has totally relaxed controls.

6. FBI Director Louis Freeh is an outspoken advocate of encryption restrictions. He argues that the ability to conduct court-authorized electronic surveillance should be built into any technology, including powerful encryption software. He fears, for example, that were the FBI and local police to lose the ability to tap telephones because of the widespread use of strong cryptography, the "country [would] be unable to protect itself against terrorism, violent crime, foreign threats, drug trafficking, espionage, kidnapping, and other crimes."

7. For a thorough discussion of the Clipper Chip, see Michael Froomkin, "The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution," 1995. The article, which is posted on the internet at *http://www.law.miami.edu/~froomkin/articles/clipper.htm*, addresses three issues. First, it outlines some of the promises and dangers of encryption. Second, it analyzes the constitutional implications of a major government proposal premised on the theory that it is reasonable for the government to request (and perhaps someday to require) private persons to communicate in a manner that makes governmental interception practical and preferably easy. Third, it speculates on how the legal vacuum regarding encryption in cyberspace shortly will be, or should be, filled.

8. Regarding the Clipper Chip and related products, the government proposes that, in exchange for providing the private sector with an encryption technology certified as unbreakable for years to come by NSA, the government would keep a copy of the keys—the codes belonging to each chip. The government hopes that this would allow it to retain the ability to intercept messages sent by the chip's user. *Ibid*.

9. In contrast, clear procedures had existed for some time to guide the relationship where the Department of Justice was acting as the CIA's lawyer.

CHAPTER 7

TERRORISM BY WEAPONS OF MASS DESTRUCTION: A REASSESSMENT OF THE THREAT

Bruce Hoffman

Terrorism today reflects both enormous change and remarkable continuity. New adversaries with new motivations and new rationales have indeed appeared in recent years to challenge some of our most basic assumptions about terrorists and terrorism. Their emergence, however, has not produced the anticipated changes in either terrorist weaponry or tactics that were predicted to follow in the wake of the Aum Shinri Kyo's 1995 nerve gas attack on the Tokyo subway. Instead, as has been the case for more than a century, the gun and the bomb remain the terrorist's main weapons of choice. Thus, as fanatical or irrational as even this new breed of terrorists may seem, like their more traditional counterparts they have also remained operationally conservative: adhering to the same familiar and narrow tactical repertoire they have mastered and believe maximizes their likelihood of success. For this reason, future terrorist use of chemical, biological, radiological, or nuclear (CBRN) weapons may be far less certain than is now commonly assumed.

The New Terrorism and Its Putative Implications.

In the past, terrorism was practiced by a group of individuals belonging to an identifiable organization with a clear command and control apparatus who had a defined set of political, social, or economic objectives. Radical leftist organizations such as the Japanese Red Army, Germany's Red Army Faction, Italy's Red Brigades, as well as ethno-nationalist terrorist movements like the Abu Nidal organization, the Irish Republican Army (IRA), and the

Basque separatist group, Basque Fatherland and Liberty (ETA), reflected this stereotype of the traditional terrorist group. They issued communiqués taking credit for—and explaining—their actions. However disagreeable or distasteful their aims and motivations were, their ideology and intentions were at least comprehensible.

Most significantly, however, these familiar terrorist groups engaged in highly selective acts of violence. They bombed various "symbolic" targets representing the source of their animus—embassies, banks, or national airline carriers—or they kidnapped and assassinated specific persons whom they blamed for economic exploitation or political repression. Their purpose was generally to attract attention to themselves and their causes.

Finally, these groups were often numerically constrained. They mostly comprised relatively small numbers of persons. Neither the Japanese Red Army nor the Red Army Faction, for example, ever numbered more than 20 to 30 hard-core members. The Red Brigades were hardly larger, with a total of fewer when 50 to 75 dedicated terrorists. Even the IRA and ETA could call on the violent services of only some 200-400 activists, while the feared Abu Nidal organization was limited to some 500 men-at-arms at any given time.

In contrast to the stereotypical terrorist group of the past, the new generation of terrorists shows signs of having undergone several important organizational changes. These, in turn, have affected their operations, decisionmaking, and targeting. Rather than belonging to the pyramidal, hierarchical organizational structures that were dominant among terrorist organizations during the 1970s and 1980s, terrorists are now increasingly part of far more amorphous, indistinct, and broader movements. These movements also tend to operate on a linear rather than hierarchical basis. Hence, instead of the classic cellular structure that was common to previous generations of terrorist organizations, some contemporary groups are

more loosely connected or indirectly linked through networks. These networks are comprised of both professional members (for example, full-time terrorists) and amateurs (hangers-on, supporters, sympathizers, and would-be terrorists who may lack the expertise or experience of their more established counterparts).

The absence of any existing, publicly identified central command authority is significant. First, it means that a state that has fallen victim to a terrorist attack may not be able to find a useful target to hit in retaliation. This could serve to remove any inhibitions on the terrorists' part against inflicting widespread, indiscriminate casualties. Individual networks thus could have greater freedom and independence in tactical decisions than traditional terrorist cells. Accordingly, this particular type of loosely structured terrorist group may pose a very different and potentially far more lethal threat than that posed by more familiar, traditional, terrorist adversaries. Second, the anonymity intrinsic to this type of operation, coupled with the lack of a discernible organizational structure with a distinguishable command chain behind the attackers, is deliberately designed to prevent easy identification and also facilitate the perpetrators' escape and evasion.

Finally, many terrorist movements today have less easily defined aims or identified objectives. Some appear to be motivated by unswerving hostility towards the West in general, and the United States in particular, or a desire for revenge and retaliation that is frequently fuelled by compelling religious imperatives and justifications rather than abstract political ideologies. In the past, the familiar, predominantly secular terrorist groups mostly claimed credit for and explained their violent acts. In contrast, the most heinous and lethal attacks perpetrated by terrorists over the past decade—which have usually been directed against civilians—have gone unclaimed.[1] By maintaining their anonymity, terrorists may believe that they are able to capitalize further on the fear and alarm intrinsically generated by their violence.

This array of changes has, in turn, raised serious concerns about the continued relevance of much of the conventional wisdom on terrorism—particularly as it pertains to potential future terrorist use of CBRN weapons. In the past, most analyses of the possibility of mass indiscriminate killing involving CBRN terrorism tended to discount it. Few terrorists, it was argued, know anything about the technical intricacies of either developing or deploying such weapons. Political, moral, and practical considerations were also perceived as important restraints on terrorist use of such weapons of mass destruction (WMD). Finally, and most significantly, we assured ourselves that terrorists wanted mass spectators rather than mass casualties. We believed, therefore, that terrorists had little interest in and little to gain from killing wantonly and indiscriminately.

A number of terrorist incidents in the 1990s forced a reevaluation of the terrorist threat. We may point in particular to the 1993 bombing of New York City's World Trade Center by Islamic extremists, the 1995 nerve gas attack on the Tokyo subway by an apocalyptic Japanese religious sect mentioned earier, and the bombing of a government office building in Oklahoma City by an American white supremacist just a month after the Tokyo incident. These events, coupled with other attacks perpetrated by religious-inspired terrorists throughout the world during the 1990s, appeared to have rendered traditional analysis dangerously anachronistic.[2] Upon closer examination, however, this has not proven to be so—despite fears, arguments and spending to the contrary.

First, this new era of terrorism has yet to materialize. Terrorism, as reported by such authoritative sources as the U.S. State Department's annual *Global Patterns of Terrorism* publications, has indeed become increasingly lethal.[3] Yet only a total of 84 Americans were killed in 40 attacks perpetrated against U.S. targets overseas during the 1990s. Approximately six times as many Americans (571), however, were killed by terrorists in the 69 attacks

that occurred the previous decade.[4] These figures do not seem to reflect an upward trend. It is, of course, incontestably tragic that any Americans should lose their lives to violence or be wantonly harmed and injured simply because of the nationality of the passport they carry, the uniform they wear, or the job they perform. And terrorism remains a threat to Americans travelling or working abroad. Nonetheless, the fact remains that despite the appearance of the "new face terrorism," the streets of the world hardly run red with American blood.

Nor is the situation terribly different in the United States itself. Admittedly, a total of 176 persons were killed by terrorists in this country during the 1990s—more than twice the international figure. We must be careful, however, how we interpret these figures. According to the Federal Bureau of Investigation (FBI), only 25 terrorist incidents occurred in the United States between 1990 and 1997 (the last year for which figures have been published). The tragic death toll is the result of only three incidents. And of the three incidents, it was one especially heinous act—the 1995 bombing of the Alfred P. Murrah Federal office building in Oklahoma City—that accounts for the overwhelming majority of fatalities (168 deaths).[5] Again, there is no doubt that terrorism remains a threat to the lives and well-being of Americans in our own country. The actual number of terrorist incidents (as opposed to the hundreds of CBRN hoaxes that the FBI and other law enforcement and public safety agencies now routinely respond to), remains, however, remarkably low, and those that cause fatalities still lower.[6]

None of the above considerations, it should be emphasized, is meant to suggest that the United States should become complacent about the threat of terrorism (domestic or international) or in any way relax our vigilance either at home or abroad. Terrorism poses, and will likely continue to pose, a serious threat to Americans and American interests both in this country and overseas. Nonetheless, it is equally clear that there has been a

tendency to exaggerate the dimensions of the threat and the strategic impact that terrorist violence has actually wrought. And by overreacting and falling prey to a sense of acute fear and intimidation, we inflate the terrorists' power in ways that are both counterproductive and often divorced from reality.[7]

Terrorism is fundamentally a form of psychological warfare, and fomenting widespread fear and intimidation is essential to terrorists' purposes. Accordingly, by succumbing to their threats and braggadocio, and by failing to distinguish their inflated rhetoric from genuine intentions and actual capabilities, we play into their hands. We risk making hard policy choices and budgetary allocations based mostly on misperception and misunderstanding rather than on hard analysis built on empirical evidence. Indeed, the incorrect lessons derived from the Aum Shinri Kyo experience in general and the 1995 nerve gas attack in particular illustrate the dangers of responding emotionally and viscerally rather than soberly and calmly to such terrorist threats.[8]

The Misunderstood Lessons of Aum Shinri Kyo.

Let us grant, for the sake of argument, the possibility that the motives of terrorists are changing, and that they may come to contemplate ever more bloody and heinous acts including the use of CBRN weapons. Even if we suppose this is an accurate reading of events (although the empirical evidence cited above seems to belie this), these trends do not necessarily imply that terrorists currently possess (as it is frequently portrayed) either the requisite scientific knowledge or technical capabilities to implement their violent ambitions. In this respect, even if it is as easy, as some say, for terrorists to culture anthrax spores or brew up a concoction of deadly nerve gas, there are other difficulties that stand in their way. The effective dissemination of these viruses and poisons still presents serious technical hurdles that greatly inhibit their effective use. Indeed, the same

Japanese religious sect that is most directly responsible for precipitating our current obsession with terrorism and CBRN weapons is precisely a case in point.

The Aum Shinri Kyo, it must be said, was by no means a typical terrorist group. The archetypal terrorist organization is composed of a handful of men and women, with limited training, technical capabilities, and resources. Aum defies this pattern. It was a religious movement with upwards of 50,000 members and offices in New York, Germany, Australia, Russia, and Sri Lanka, in addition to Japan. Aum had assets estimated to be in the neighborhood of $1 billion—and at least certainly in the hundreds of millions. It specifically recruited graduates with scientific and engineering degrees from Japan's leading universities and provided them with state-of-the-art laboratories and lavish budgets with which to fund the group's variegated weapons research and development (R&D) programs. While its biological weapons research was comparatively modest—its research never employed more than perhaps 20 persons at most[9]—as many as 80 scientific personnel were specifically detailed to work on the group's chemical weapons programs.

When police raided the sect's laboratories following the nerve gas attack, for example, they found enough sarin to kill an estimated 4.2 million persons.[10] In addition, Aum had either already produced or planned to develop other powerful nerve agents such as VX, tabun, and soman; chemical weapons such as mustard gas and sodium cyanide; and deadly biological warfare pathogens that included anthrax, the highly contagious disease known as Q-fever,[11] and possibly the deadly Ebola virus as well.[12] Aum's most ambitious project, however, was doubtless its efforts to develop a nuclear capability. To this end, the group had purchased a 500,000-acre sheep station in a remote part of Western Australia. There, they hoped to mine uranium that was to be shipped back to Aum's laboratories in Japan where scientists using laser enrichment technology would convert it into weapons-grade nuclear material.[13]

The group had also assembled an impressive panoply of conventional weaponry. Aum is believed to have purchased large quantities of small arms from Russian sources and to have been in the market for advanced weaponry such as tanks, jet fighters, surface-to-surface rocket launchers, and even a tactical nuclear weapon. Aum succeeded in obtaining a surplus twin-turbine Mi-117 helicopter—complete with chemical spray dispersal devices. The group also planned—and had gone as far as to acquire sophisticated robotic manufacturing devices—to produce at least a thousand knock-off versions of Russia's world-famous AK-47 assault rifle along with one million cartridges. Finally, the sect had determined how to manufacture TNT and the central component of plastic explosives, RDX.[14]

However, despite Aum's considerable financial wealth, the technical expertise that it could call upon from its well-educated members and the vast resources and state-of-the-art equipment at their disposal, the group could not effect even a single truly successful chemical or biological attack. On at least nine occasions, the group attempted to disseminate botulinum toxin (Clostridium botulinum) or anthrax (Bacillus anthracis) using aerosol means. Each time they failed, either because the botulinum agents they grew and enriched were not toxic or the mechanical sprayers used to disseminate the anthrax spores became clogged and hence inoperative.[15]

Even the comparatively more successful sarin attack on the Tokyo subway would be laughable if not for the tragic deaths of 12 persons and the physical and psychological harm caused to many more victims. For all its sophisticated research and development, the best means the group could find to disseminate the nerve gas was in plastic trash bags that had to be poked open with sharpened umbrella tips in order to release the noxious mixture.[16] And for all the fear generated by this attack, it was far from achieving mass destruction or inflicting mass casualties. New research has revealed that the number of persons physically injured or affected by the attack is much lower than previously

reported.[17] Of the 5,000 persons who received medical treatment in the aftermath of the subway attack, the vast majority (73.9 percent) were suffering from shock, emotional upset, or some psychosomatic symptom.[18] That the Aum, with all its unique advantages, could do no more harm than this speaks volumes about the challenges facing any less well endowed terrorist organization.

In sum, upon further examination and analysis, Aum's experience suggests—however counterintuitively or contrary to popular belief—the immense technological difficulties faced by any nonstate entity in attempting to weaponize and effectively disseminate chemical and biological weapons.[19] It also provides striking refutation of the argument voiced with increasing frequency in recent years of the ease with which such weapons can be fabricated and made operational. Public officials, journalists, and analysts, for example, have repeatedly alleged that biological attacks in particular are relatively easy for terrorists to undertake. According to one state emergency management official, biological weapons

> are available—and easy to make . . . . One does not need a degree in microbiology to make this work, being able to read is enough . . . . It's not like enriching uranium.[20]

Similarly, both the White House and senior FBI officials have argued that the information needed to develop chemical and biological weapons can be readily obtained from the Internet and other open sources.[21] Such claims do not square with the facts. Both the Aum experience and a considerable body of subsequent research and analysis make it clear that fabrication and dissemination of such weapons is not easy.[22] John Lauder, the national intelligence officer responsible for non-proliferation, elaborates:

> While popular culture can explore the potential BW threat, actually developing and using an effective biological weapon poses certain technological challenges.[23]

Policy Implications Regarding Future Possible CBRN Terrorism.

The analysis above is not to suggest, however, either that there is no threat of terrorist use of CBRN or that such a threat should be dismissed or discounted. Indeed, the difficulties now facing a terrorist who seeks to use a CBRN weapon to achieve mass effects could diminish dramatically because of new discoveries, further advances in technology, or other material factors.

What this chapter has argued is that by exaggerating the ability of terrorists to wreak genuine mass destruction or inflict widespread casualties, we are in danger of missing sight of where the real threats lie. A limited terrorist attack might, for example, involve not a WMD per se, but an unconventional chemical, biological, or radiological weapon built on a deliberately small scale. It might be used either alone or as part of a series of smaller incidents, which might occur either simultaneously or sequentially, in a given location. Such an attack could have disproportionately serious consequences, generating unprecedented fear and alarm, and thus serving the terrorists' purpose just as well as a larger weapon or more ambitious attack with massive casualties. The most salient terrorist threat involving an unconventional weapon will likely not involve (or even attempt) the destruction of an entire city (as often proclaimed by fictional thriller writers and some government officials). Rather it will involve the far more deliberate and delicately planned use of a chemical, biological, or radiological agent for more discrete purposes.

Yet despite the empirical evidence regarding terrorism trends and patterns of activity (both domestic and international), including the correct lessons that should be drawn from the case of Aum, the United States remains singularly preoccupied with the threat of mass-casualty terrorism. It continues to plan for worst case scenarios. This is largely a result of a mindset that took root in the immediate aftermath of the near simultaneous Tokyo nerve

gas attack and the Oklahoma City bombing in 1995. Our thinking and perceptions of the terrorist threat have remained fundamentally unchanged since this episode. New evidence regarding Aum and the overall pattern of terrorist activity in the 5 years since the 1995 subway attack suggest that many of our current assumptions may be wrong.

Nonetheless, no significant reassessment, reconsideration, or revision of the CBRN terrorism threat profile established during the 1995-96 time frame has yet been undertaken.[24] Thus, a critical first step in assessing the threat as it exists today and is likely to evolve in the future should be to undertake a broad new net assessment of the terrorist threat not only internationally but domestically as well. Such an assessment—addressing conditions, circumstances, and vulnerabilities of today rather than those of 5 years ago—will permit us to determine whether the worst-case scenario assessment approach that has dominated current domestic planning and preparedness for potential acts of CBRN terrorism is still appropriate, much less relevant.[25]

The current narrow policy focus on lower-probability/higher-consequence threats, which in turn posits virtually limitless vulnerabilities, does not reflect the realities of contemporary terrorist behavior and operations. “This kind of analysis,” Brian Jenkins recently warned in testimony before Congress, “can degenerate into a fact-free scaffold of anxieties and arguments—dramatic, emotionally powerful, but analytically feeble.”[26] At the same congressional hearing, another expert, John Parachini, had similar advice to give. The “apparent over-reliance," he noted,

> on worst-case scenarios shaped primarily by vulnerability assessment rather than an assessment that factors in the technical complexities, motivations of terrorists, and their patterns of behavior seems to be precisely the sort of approach we should avoid.[27]

The main weakness in such an approach is in the axiomatic assumption that any less serious incident can be addressed equally well by planning for the most catastrophic threat. This ignores the fact that the higher-probability/lower-consequence attacks might present unique challenges of their own.[28]

Finally, this approach may lead to less efficacious means of setting budgetary priorities and allocating resources, thus leading to less rather than more security for our country. This was precisely the point made by Henry L. Hinton, Jr., the Assistant Comptroller General, National Security and International Affairs Division, U.S. General Accounting Office, when he testified before Congress in March 1999. "The [most] daunting task before the nation," he argued,

> is to assess—to the best of its ability—the emerging threat with the best available knowledge and expertise across the many disciplines involved. The United States cannot fund all the possibilities that have dire consequences. By focusing investments on worst-case possibilities, the government may be missing the more likely threats the country will face. With the right threat and risk assessment process, participants, inputs, and methodology, the nation can have greater confidence that it is investing in the right items in the right amounts. Even within the lower end of the threat spectrum—where the biological and chemical terrorist threat currently lies—the threats can still be ranked and prioritized in terms of their likelihood and severity of consequences. A sound threat and risk assessment could provide a cohesive roadmap to justify and target spending.[29]

Moreover, at a time when the United States is especially preoccupied with these "high-end" terrorist threats involving mass-destruction CBRN weapons, the series of apartment building bombings that occurred in Russia and Dagestan during August and September 1999 is a salutary reminder of how terrorists can still achieve their dual aim of fear and intimidation through entirely conventional means and traditional methods: using bombs to blow things up.

This fact has important implications for America's—and indeed also other countries'—counterterrorism preparedness. Given the limited resources and constrained capabilities typical of most terrorists, they perhaps reflexively shun weapons and tactics either that cannot be relied upon completely or that pose such enormous complexities in terms of their employment (e.g., achieving effective dissemination) as to border on the unappealing, if not useless. For this reason, it can be said that terrorists remain essentially content with the limited killing potential of their handguns and machine-guns and the slightly higher rates that their bombs can achieve. In other words, they seem to prefer the assurance of the modest success provided by their more conventional weapons and traditional tactics to the risk of failure inherent in more complex and complicated operations involving CBNR weapons.

Indeed, of the more than 9,000 incidents recorded in The RAND Chronology of International Terrorism since 1968, fewer than 100 evidence any indication of terrorists plotting to use chemical, biological, or radiological weapons or to obtain nuclear devices—much less actually to carry out such attacks. As one critic has observed in connection with the current concern over terrorist use of biological agents: "Nasty people and the ingredients for bioterrorism were all in place over a decade ago. Why now the drumbeating?" [30] Indeed, since the beginning of the century, little more than a dozen terrorist incidents in fact have occurred that resulted in the deaths of more than a 100 persons at one time. This is an arguably infinitesimal number given the total volume of terrorism that has occurred worldwide within past quarter century, much less 100 years.[31]

There is another relevant paradox affecting terrorist behavior. Terrorists have long been seen as far more imitative than they are innovative. However, to date, no similar or copycat act of terrorism, which at the time was thought might likely follow in the wake of the sarin nerve gas attack on the Tokyo subway in 1995, has materialized. In this respect, the Tokyo incident has been the exception

rather than the rule in terms of terrorist behavior. "This fact gains significance," Brian Jenkins observed,

> when we note that past terrorist and criminal innovations—airline hijackings, political kidnappings, malicious product tampering—were promptly imitated. And terrorist attacks involving chemical and biological agents, if they do occur, are likely to remain rare events—they will not become the truck bomb of the next decade.[32]

Finally, as serious and potentially catastrophic as a terrorist CBRN attack might prove, it is highly unlikely that it could ever completely undermine the national security, much less threaten the survival of a nation like the United States or indeed most other Western countries. This point should be self-evident, but given the rhetoric and hyperbole with which the threat of CBRN terrorism is frequently couched, it requires reiteration. Even Israel, a comparatively small country in terms of population and landmass, who throughout its existence has often been isolated and surrounded by enemy states and subjected to unrelenting terrorist attack and provocation, has never regarded terrorism as a paramount threat to its national security and longevity. Israel has never construed terrorism as worthy of profligate budgets or the diversion of disproportionate resources and attention.

Moreover, we should recall that even in the wake of the intense fear and concern following the 1995 Tokyo nerve gas attack, the Japanese government did not fall, widespread disorder did not ensue throughout the country, nor did society collapse. There is no reason to assume that the outcome would be any different in the United States or in any other Western democratic state in the event of a similar terrorist attack involving a chemical or biological weapon. To take any other position risks surrendering to the fear and intimidation that are precisely the terrorists' timeless stock-in-trade. There is a thin line between prudence and panic. The challenge, therefore, in responding to the threat of potential terrorist use of CBRN weapons is to craft a

defense that is not only both cost-effective and appropriate, but also sober and practical.

ENDNOTES - CHAPTER 7

1. These include, among other incidents, the series of car bombings that convulsed Bombay in 1993, killing 317 persons; the huge truck bomb that destroyed a Jewish community center in Buenos Aires in 1994, killing 96; the 1995 bomb that demolished the Alfred P. Murrah Federal Building in Oklahoma City, leaving 168 dead; the 1998 bombings of the American embassies in Kenya and Tanzania; and the series of bombings of apartment buildings in Dagestan and Moscow in August and September 1999. Indeed, the 1988 in-flight bombing of Pan Am Flight 103 is an especially notorious example. Although we know—as a result of what has been described as the "most extensive criminal investigation in history"—that the two Libyan government airline employees, who are currently being tried in The Hague, were identified and accused of placing the suitcase containing the bomb that eventually found its way onto the flight, no believable claim of responsibility has ever been issued. Hence, we still *do not* know why the aircraft was targeted or who ordered or commissioned the attack. For a more detailed study of this issue, see Bruce Hoffman, "Why Terrorists Don't Claim Credit," *Terrorism and Political Violence*, Vol. 9, No. 1, Spring 1997, pp. 1-6.

2. Several such incidents may be noted here. In February 1993 a series of 13 near-simultaneous car and truck bombings shook Bombay, India, killing 400 persons and injuring more than 1,000 others, all in reprisal for the destruction of an Islamic shrine in that country. In December 1994 an Air France passenger jet was hijacked by Islamic terrorists belonging to the Algerian Armed Islamic Group (GIA). The terrorists' plot (mercifully foiled) was to blow up themselves, the aircraft, and the 283 passengers on board precisely when the plane was over Paris, thus causing the flaming wreckage to plunge into the crowded city below. Between July and October 1995, a wave of bombings was unleashed in France by the GIA. The attacks targeted metro trains, outdoor markets, cafes, schools, and popular tourist spots, killing eight persons and wounding more than 180 others. Note also the following episodes: the assassination in November 1995 of Israeli Prime Minister Itzhak Rabin by a Jewish religious extremist, the assassination to be the first step in a campaign of mass murder designed to disrupt the peace process; the Hamas suicide bombers who turned the tide of Israel's national elections with a string of bloody attacks that killed 60 persons between February and March 1996; the Egyptian Islamic militants who carried out a brutal machine-gun and hand grenade

attack on a group of Western tourists outside their Cairo hotel in April 1996 that killed 18; the June 1996 truck bombing of a U.S. Air Force barracks in Dhahran, Saudi Arabia, where 19 persons perished, by religious militants opposed to the reigning al-Saud regime; the massacre in November 1997 of 58 foreign tourists and four Egyptians by terrorists belonging to the Gamat al-Islamiya (Islamic Group) at the Temple of Queen Hatsheput in Luxor, Egypt; and the bombings of the U.S. Embassies in Kenya and Tanzania in August 1998 that killed 257 and injured some 5,000 others.

3. Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 1997*, Washington, DC: U.S. Department of State Publication 10535, April 1998, pp. iii, 1.

4. Statistics compiled by the Bureau of Diplomatic Security, U.S. State Department. See also Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 1999*, Washington, DC: U.S. Department of State Publication 10687, April 2000, p. 1.

5. Counterterrorism Threat Assessment and Warning Unit, National Security Division, *Terrorism in the United States 1997*, Washington, DC: U.S. Department of Justice, Federal Bureau of Investigation, 1998, pp. 22-23.

6. See Statement for the Record before the Senate Select Committee on Intelligence, January 28, 1998, *http://www.fbi.gov/congress/98archives/threats.htm, of FBI Director Louis J. Freeh, p. 6; Statement of Robert J. Burnham, Chief, Domestic Terrorism Section before the U.S. House of Representatives Subcommittee on Oversight and Investigations, May 19, 1999, p. 1, at http://www.fbi.gov/pressrm/congress/bioleg3.htm*; Statement for the Record of Mrs. Barbara J. Martinez, Deputy Director, National Domestic Preparedness Office before the U.S. House of Representatives Transportation and Infrastructure Committee, Subcommittee on Oversight, Investigations, and Emergency Management, June 9, 1999, p. 1, at *http//:www.fbi.gov/pressrm/congress/counterr.htm*.

7. Our preoccupation with Osama bin Laden and attendant—however inadvertent—lionization of his stature and power is perhaps such a case in point. Despite his vast wealth and alleged legions of minions, it is hardly likely that bin Laden could ever hope to vanquish the U.S. military, overthrow our government, or achieve any fundamental political changes in American foreign or domestic policy. Yet, this single individual arguably is held in fear and accorded a stature far in excess of what logic would seem to dictate.

8. Among the first and most important works to incisively analyze the true implications of Aum and the 1995 nerve gas attack are David Rapoport, "Terrorism and Weapons of the Apocalypse," *Georgetown National Security Studies Quarterly*, Summer 1999, pp. 49-67; Ehud Sprinzak, "The Great Superterrorism Scare," *Foreign Policy*, No. 112, Fall 1998, pp. 110-125; Milton Leitenberg, "Aum Shinrikyo's Efforts to Produce Biological Weapons: A Case Study in the Serial Propagation of Misinformation," *Terrorism and Political Violence*, Vol. 11, No. 4, Winter 1999, forthcoming.

9. Telephone interview of RAND research staff member Professor Anthony Tu, July 21, 1999; and of Milton Leitenberg, July 16, 1999.

10. Richard Lloyd Parry, "Sect's poisons 'could kill 4.2m,'" *The Independent on Sunday* (London), March 26, 1995; Andrew Pollack, "Japanese Police Say They Found Germ-War Material at Cult Site," *New York Times*, March 29, 1995.

11. Reuters, "Aum Cult Gas Cache," *International Herald Tribune* (Paris), December 13, 1996. See also National (Japanese) Police Agency, "Aum Shinrikyo: An Alarming Report on the Terrorist Group's Organization and Activities," *Shoten* (Tokyo), No. 252 (1195), pp. 10-12; and David E. Kaplan and Andrew Marshall, *The Cult at the End of the World*, London: Hutchinson, 1996, pp. 10, 95-97, 121-125, 151, 211-221, 232.

12. Following an outbreak of Ebola in Zaire in 1992, Asahara and 40 followers traveled to that country ostensibly on a humanitarian aid mission. Associated Press and Agence France-Presse, "Cult 'studied deadly Ebola virus,'" *New York Times*, April 25, 1995. See also Kaplan and Marshall, pp. 96-97.

13. Kaplan and Marshall, pp. 85, 126-133; 190-192, 208; Sopko, "The Changing Proliferation Threat," p. 13.

14. See Kaplan and Marshall, pp. 76, 88, 107-112, 151, 190-193; James K. Campbell, "Excerpts From Research Study 'Weapons of Mass Destruction and Terrorism: Proliferation by Non-State Actors,'" *Terrorism and Political Violence*, Vol. 9, No. 2, Summer 1997, pp. 35-37; Ron Purver, "Chemical Terrorism In Japan," unpublished paper by the Canadian Security Intelligence Service, Ottawa, Canada, June 1995, p. 15; National Police Agency, *Shoten* (252), "Aum Shinrikyo: An Alarming Report on the Terrorist Group's Organization and Activities," 1995, p. 10.

15. Two attempts were made with anthrax and seven with botulinum toxin. W. Seth Carus, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century*, Washington, DC: Center for Counterproliferation Research, National Defense University, March 1999, p. 62.

16. D. W. Brackett, *Holy Terror: Armageddon in Tokyo*, New York: Weatherhill, 1996, pp. 126, 129.

17. Leitenberg, "The Experience of the Japanese Aum Shinrikyo Group and Biological Agents," forthcoming.

18. Anthony G. Macintyre, *et al*., "Weapons of Mass Destruction: Events with Contaminated Casualties—Planning For Health Care Facilities," *Journal of the American Medical Association*, No. 263, January 2000, pp. 242-249.

19. Indeed, this same point can also be made regarding the formidable hurdles faced by many established states in developing their own effective weapons programs in the same areas of chemical, biological, and nuclear warfare.

20. Quoted in Grant Sasek, "Officials in State Warn of Biological Terrorism,"*Helena Independent Record*, *http://billinsgazette.com/region.990125_reg009.html*.

21. See, for example, the White House, "Fact Sheet on Combating Terrorism: Presidential Decision Directive 62," May 22, 1968, accessed at *http://cns.miis.edu/research/cbw/pdd-62.htm*, which states that

> easier access to sophisticated technology means that the destructive power available to terrorists is greater than ever. Adversaries may thus be tempted to use unconventional tools, such as weapons of mass destruction, to target our cities and disrupt the operations of our government.

Statement for the record before the Senate Select Committee on Intelligence, January 28, 1998, *http://www.fbi.gov/congress/98archives/threats.htm*, of FBI Director Louis J. Freeh:

> The ease of manufacturing or obtaining biological and chemical agents is disturbing. Available public source material makes our law enforcement mission a continuous challenge.

Statement of Robert J. Burnham, Chief, Domestic Terrorism Section before the U.S. House of Representatives Subcommittee on Oversight

and Investigations, May 19, 1999. *Http://www.fbi.gov/pressrm/congress/bioleg3.htm*;: "Literature containing recipes and modes of dissemination are available through 'how to' literature and over the Internet."

22. See, for example, the more detailed analysis summarized in *First Annual Report to The President and The Congress of the Advisory Panel To Assess Domestic Response Capabilities For Terrorism Involving Weapons of Mass Destruction: I. Assessing the Threat*, December 15, 1999, at *http://www.rand.org/organization/nsrd/terrpanel*, pp. 20-34.

23. In this capacity, he is the nation's senior intelligence analyst concerned with this issue. U.S. Congress, "Statement by Special Assistant to the DCI for Nonproliferation John A. Lauder on the Worldwide Biological Warfare Threat," House Permanent Select Committee on Intelligence, March 3, 1999, *http://www.cia.gov/cia/public_affairs/speeches/lauder_speech_030399.html*.

24. Discussion with a senior national intelligence officer responsible for this issue, Washington, DC, January 10, 2000.

25. This same argument has been made repeatedly by Henry L. Hinton, Jr., Assistant Comptroller General, National Security and International Affairs Division, U.S. General Accounting Office, before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, U.S. House of Representatives in (1) "Combating Terrorism: Observation on Federal Spending to Combat Terrorism," March 11, 1999; and (2) "Combating Terrorism: Observation on the Threat of Chemical and Biological Terrorism," October 20, 1999; as well as by John Parachini in "Combating Terrorism: Assessing the Threat," and Brian Michael Jenkins in their respective testimony before the same House subcommittee on 20 October 1999; the Hinton testimony "Combating Terrorism: Observation on Biological Terrorism and Public Health Initiatives," before the Senate Committee on Veterans' Affairs and Labor, Health and Human Services, Education, and Related Agencies Subcommittee, Senate Committee on Appropriations, *GAO/T-NSIAD*-99-12, U.S. General Accounting Office Washington, DC, March 16, 1999.

26. Jenkins, "Testimony," October 20, 1999, p. 4.

27. Parachini, "Combating Terrorism: Assessing the Threat," October 20, 1999, p. 17.

28. A higher-probability/lower-consequence event is considered to involve the limited, rather than massive, use of a chemical, biological, radiological, or conventional weapon whose effects would be geographically confined in both scope and actual physical destructiveness and that would most likely be aimed at inflicting fatalities numbering in the tens or twenties rather than the thousands (even though the number of injured requiring medical treatment could number in the thousands).

29. Hinton, "Combating Terrorism: Observations on Biological Terrorism and Public Health Initiatives," *GAO/T-NSIAD*-99-112, March 16, 1999, pp. 4–5.

30. Daniel S. Greenberg. "The Bioterrorism Panic," *Washington Post*, March 16, 1999.

31. These include a bombing in Bessarabia in 1921; a 1925 bombing of a crowded cathedral in Sofia, Bulgaria; a largely unrecorded attempt to poison imprisoned German SS concentration camp guards shortly after World War II; the crash of a hijacked Malaysian passenger plane in 1977; the arson attack at a Teheran movie theater in 1979 that killed more than 400; the 1983 bombing of the U.S. Marine barracks in Lebanon that killed 241; the 1985 in-flight bombing of an Air India passenger jet that killed all 328 persons on board; the simultaneous explosions that rocked an ammunition dump in Islamabad, Pakistan in 1988; the bombing of Pan Am Flight 103 in 1988 that killed 278 persons; the 1989 in-flight bombing of a French UTA flight that killed 171; the 1989 in-flight bombing of a Colombian Avianca aircraft on which 107 persons perished; and the aforementioned 1993 series of bombings in Bombay, the 1995 explosion at the Murrah Building in Oklahoma City, and the two American embassy bombings in East Africa in 1998. As Brian Jenkins noted concerning such episodes:

> Lowering the criterion to 50 deaths produces a dozen or more additional incidents. To get even a meaningful sample, the criterion has to be lowered to 25. This in itself suggests that it is either very hard to kill large numbers of persons or very rarely tried.

See Brian M. Jenkins, *The Likelihood of Nuclear Terrorism*, Santa Monica, CA: RAND, P-7119, July 1985, p. 7.

32. Jenkins, "Testimony," October 20, 1999, pp. 2-3.

CHAPTER 8

TERRORISM AND WEAPONS OF MASS DESTRUCTION: A REVIEW AND NEW PARADIGM

Jeffrey F. Addicott

Introduction.

A fundamental obligation of any state is to protect its citizens from external as well as internal threats to person and property. Nowhere is this obligation more difficult to perform than in the realm of terrorism, particularly when one considers the apocalyptic horrors that might be unleashed through the terrorist use of weapons of mass destruction (WMD). In the case of the government of the United States, it is concerned not only with those renegade states that might commit or sponsor various WMD terrorist activities against U.S. citizens, but also with international or domestic terrorist groups, and even individuals. When one considers that terrorists have targeted the United States more often than any other country in the world, the specter of WMD terrorism demands top priority in our thinking and planning.[1]

Many solutions have been suggested. Among them are the institution of new security and intelligence-gathering methodologies to help prevent a WMD terrorist act; the development of streamlined plans for a rapid federal, state, and local response to the aftermath of a WMD event; and an increase in the role of the Department of Defense in counterterrorism. These solutions are focused, as it were, on the pressure points of the problem. However, the threat of WMD makes it critical for our national strategy to appreciate as well that since democracies do not engage in terrorism, we must do more to promote democratic institutions throughout the community of nations. This

democracy-building initiative must be the basis for a new and dynamic paradigm whose application might point a more effective way to WMD terrorist avoidance, especially in regard to state-sponsored terrorism.

Terrorism.

There is no universally accepted definition of terrorism, either in the international community or in the United States. As the root word *terror* implies, terrorism involves the use of fear to attain certain goals. Notwithstanding that terrorism is the antithesis of the rule of law, the postmodernist adage that "one man's terrorist is another man's freedom fighter" further contributes to the inability to carve out a clear definition. Certainly, however, civilized nations have come to associate certain specific acts as terrorism per se. Hostage-taking, public bombings, and acts directed against civilians are easily defined as terrorist in nature, regardless of the ideological, religious, or social goals of the perpetrators.

For those who follow the trends, the lethality of terrorism continues to grow, particularly against U.S. interests. Although the number of terrorist attacks has fallen from 484 in 1991 to 250 in 1996, both the State Department and the RAND-St. Andrews Chronology of International Terrorism agree that 1996 (the last year records have been updated) was one of the bloodiest years on record. A RAND study found that a "total of 510 persons were killed, 223 more than in 1995, and 91 more than in 1994."[2] These studies are, of course, rather inconsequential when one considers the aftermath of a terrorist directed nuclear, biological, chemical, or radiological attack in an urban area of the United States. To the mass casualties and devastating economic disruption, one must add the troubling impact this event might have on future civil liberties and freedoms that Americans now enjoy.

Sources of WMD Terrorism.

Apart from the normal modus operandi of terrorism, one must now add WMD as a special definitional subset. In Section 1403 of the National Defense Authorization Act for fiscal year 1997, a WMD is defined as

> any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release of toxic or poisonous chemicals or their precursors, a disease organism, or radiation or radioactivity.[3]

Thus WMD includes the full range of biological, chemical, and radioactive agents.

There are three general sources from which a WMD terrorist attack can emanate—state, sub-state, or individual. Tragically, all three categories have flirted with the use of WMD in the past decade.

State-Sponsored Terrorism.

Perhaps the most easily identifiable category of terrorism is the state-sponsored terrorist attack. In recent times, the international community has been shocked to learn that certain renegade states such as Iraq have shown an unabashed willingness to use deadly nerve gas to kill thousands of men, women, and children (the Kurds). Indeed, it can be argued that all totalitarian states pose an ever-present threat for the use of WMD at any given time—both against their own people and against other nations. The U.S. State Department now designates seven countries as sponsors of terrorism against other nations: Cuba, Iran, Iraq, Libya,North Korea, Sudan, and Syria.[4] In fact, the number is larger. John A. Lauder, director of the Central Intelligence Agency's Nonproliferation Center, has testified before Congress that a dozen countries

now either possess or are actively pursuing offensive biological weapons capabilities for use against their perceived enemies, whether internal or external.[5]

In the context of a state use of WMD in a terrorist attack, several commentators seek to distinguish a state-sponsored terrorist act from a state-supported terrorist act. State-sponsored terrorism exists when a state directly but secretly uses its own government apparatus and resources to perform acts of terrorism against another country. Since accountability for such acts is always denied, the aggressor state seeks to avoid responsibility. On the other hand, state-supported terrorism refers to the practice of a state providing resources to a terrorist group for training, logistics, or financing as is currently the case in Afghanistan, where the Islamic terrorist group headed by Osama bin Laden (the inner core group is known as Al-Qaeda) takes refuge. Under the state-supported scenario, the terrorist group generally operates independently from the state.[6]

In the final analysis, it is difficult to make a practical distinction between state-sponsored and state-supported terrorism. The terms really speak only to the degree of culpability. If the rule of law has any force, states who allow terrorist groups to operate with impunity on their soil should never be able to escape the attendant lawful consequences.[7]

The early days of concern regarding terrorism and the use of WMD saw most of the emphasis focused on the actions of the totalitarian state. Because many believed that ready access to WMD material was limited, sub-state terrorist groups or individual terrorists were generally given less attention. For these latter categories of terrorism, the international community generally concentrated on making specific overt acts international crimes, e.g., airline hijacking or hostage-taking. For renegade states, however, the major issue turned on the proper application of

appropriate sanctions against the state that sponsored or supported a terrorist incident.

A considerable debate rages regarding how to deal with a WMD terrorist event vis-à-vis international legal sanctions. A particularly interesting concern centers on the use of the diplomatic pouch to import and export, with impunity, assorted prohibited and illegal items into receiving and transit states.[8] (The diplomatic pouch issue continues to cause great consternation.) Modern international practice has witnessed the use or attempted use of the diplomatic pouch to transport illegal foreign currency, illegal drugs, weapons, and even people. While all manifestly evil acts committed under the cover of this diplomatic shield are sorely objectionable, the most insidious and disconcerting activities are those in which the diplomatic pouch might be used as a vehicle to commit clearly defined acts of terrorism, especially those related to WMD.

Currently, the diplomatic privileges and immunities accorded to the diplomatic pouch under treaty and customary international law are set out in Article 27 of the Vienna Convention on Diplomatic Relations.[9] In short, the diplomatic pouch is deemed by international law to be inviolable and not subject to detention or search. The central thrust of those who periodically argue for a change to the Vienna Convention is that the protected status given to the diplomatic pouch must be significantly revised to account for the legitimate security interests of the receiving state. Again, the major concern is that the diplomatic pouch could be used to commit a WMD terrorist act. For example, responding to public fears that diplomatic privileges could be used as a vehicle to commit state-sponsored terrorism related to WMD,[10] then Secretary of Defense Caspar Weinberger publicly indicated in 1986 that the entire doctrine of diplomatic immunity should be greatly limited.[11] Arguing that state-sponsored terrorists were abusing the doctrine, Weinberger called upon “diplomats with the assistance of the legal profession” to define new limits that would help solve the problem of diplomatic privileges being

extended to those states that were connected with terrorists.[12]

True, in the context of the large-scale destruction that would result from even a single WMD event, the demands for security safeguards would apparently far outweigh the advantages of maintaining the present international rules intact. Otherwise, if ordinary weapons can be neatly and easily sent into the receiving state via the diplomatic pouch, why not WMD? A hostile country, for instance, could smuggle in a vial of lethal biological material for contaminating a city water supply. Fortunately, although these emotion-driven arguments come to the forefront from time to time, the privileged status of the diplomatic pouch has never been successfully curtailed. This is true for three reasons.

First, most people understand that if the diplomatic pouch privilege is limited, then the determined terrorist will find yet another way to smuggle WMD materials into the United States. In an open society such as the United States, the state-sponsored terrorist can obtain much, if not most, of the needed materials on the domestic open market and, more importantly, do so without leaving a signature.[13] Second, since nations have an inherent right of self-defense to search out and otherwise protect themselves against viable threats to their national security, the state which sponsored such blatant aggressive behavior takes an inordinate risk by using the diplomatic pouch in such a manner.

Third, the Vienna Convention can never hope to maintain any form of functional integrity unless it is strictly adhered to. Nations who demand inspection of even the most suspicious diplomatic pouches must do so only at the risk of having their own bags subjected to the same process by the sending state.[14] And that practice would quickly undermine the entire process of free diplomatic intercourse. The only real guarantee that other nations, friendly or otherwise, will generally follow international rules rests in

this reciprocity analysis—the *red thread* of international law.

The way to deal with a state-sponsored terrorist attack, if linkage is established, is to seek redress under the rule of law—financially, judicially, or militarily.[15] Historically, if a state sponsors a terrorist act, the United States has generally demonstrated that it has the capability and willingness to retaliate under the well-recognized justification of self-defense. Unlike other international disputes between nations, terrorist attacks should never be handled by some third party in the context of a dispute resolution. The renegade state is punished in a legitimate manner and forum. Ultimately, the aggrieved state can turn to the classical forms of self-defense, depending on the severity of the terrorist incident. Realistically, if the United States had hard evidence that a state was behind a terrorist attack, it would likely respond under the traditional notions of self-defense and forcible self-help. The United States would certainly do what was necessary to protect itself from acts of violence.[16] In this context, the classical right to engage in self-defense under Article 51 of the United Nations' Charter would be entirely appropriate.[17]

Finally, reflecting the seriousness of WMD, there are a number of scholars who believe that the threat of WMD to national survival is so great that a new international legal regime should allow for a threatened nation to engage in "preventive or preemptive use of force to either deter acquisition plans, eliminate acquisition programs, or destroy illicit WMD sites at any stage in the proliferator's acquisition efforts."[18] The 1981 Israeli attack on the Iraqi nuclear reactor at Osiraq, is certainly an example of a nation exercising preemptive self-help in the face of a rogue nation engaged in the production of WMD materials.[19]

Sub-state Terrorism.

In early 2000, U.S. and Israeli intelligence sources reported that Hamas, the militant Islamic terrorist group,

was experimenting with chemical weapons in their rocket attacks against Israeli targets.[20] With the increasing availability of high-tech weapons and nuclear materials from former Communist countries and the ease with which some chemical and biological agents can now be manufactured, there is growing concern that sub-state groups will now actively cross over into the WMD domain. Sub-state terrorist groups can be either domestic or international terrorist organizations and are generally categorized by either religious or political ideologies. In 1995, for example, "25 of 58, or 42 percent of known, active, international terrorist groups, had a predominately religious component or motivation."[21]

The first use of a WMD by a sub-state group occurred on March 20, 1995, when members of the Aum Shinri Kyo cult in Japan released a lethal nerve agent, sarin, in the Tokyo underground subway. This WMD attack killed 12 people and reportedly injured 3,000 others.

While attacks by sub-state groups against U.S. interests have not yet used WMD (as of this writing), many groups have shown a viciousness and disregard for human life that clearly points to a willingness to use such weapons in the future. For instance, Osama bin Laden's Islamic fundamentalist terrorist group conducted bombings of the U.S. embassies in Kenya and Tanzania in August 1998 that killed 257 people and injured almost 5,000.[22] Another Islamic radical group headed by Ramzi Ahmad Yousef conducted the 1993 bombing of New York City's World Trade Center in an attempt to topple one of the twin towers onto the other to kill thousands, an act clearly in the spirit of a WMD event.[23]

The United States has taken unilateral steps to ensure that the individual perpetrators of international terrorism are brought to justice in a court of law. In the United States, the Omnibus Terrorism Act of 1986 made terrorist attacks on U.S. citizens overseas a Federal crime and authorized the extraterritorial arrest and trial in U.S. courts of the

suspected perpetrators. The most famous case in this regard was the arrest and prosecution by U.S. authorities of Fawaz Yunis, an Arab terrorist involved in the hijacking of an aircraft aboard which were two U.S. citizens.[24]

Individual Terrorism.

Perhaps the most troubling aspect of WMD terrorism is the prospect of an individual setting off a WMD in a major urban area. Because they operate on their own, without affiliation to any known group or state, individuals who engage in terrorism are far harder to track or predict. They are a new breed of terrorist.

To demonstrate our vulnerability to individual terrorism, on March 3, 1999, William C. Patrick III, a leading U.S. expert on biological warfare, walked through the security check system at the Rayburn House Office Building in downtown Washington, DC, carrying 7 1/2 grams of powdered anthrax (enough to kill everyone in the building) in a small plastic bottle.[25] This action dramatically illustrated the ease with which a single determined terrorist could breach security systems and target, in this case, a major federal government installation. It also provided a wake-up call to U.S. government officials and the public at large.[26]

Patrick told a Congressional committee that he was trying to show how a hostile or aggressor state could smuggle powdered anthrax into the United States in a secure diplomatic pouch.[27] What Patrick was really demonstrating, however, was the ease with which any individual terrorist—domestic or international—could unleash untold WMD horror, almost at will. In his testimony, Patrick related that he had also carried other similar deadly materials through all the major airports, and the security systems of the State Department, the Pentagon, and even the CIA, without anyone stopping him.[28]

The most notorious example of an individual terrorist attack in the United states occurred in April 1995 with the bombing of the Murrah Federal building in Oklahoma City by Timothy McVeigh (an accomplice, Terry Nichols was also convicted). Although McVeigh did not employ WMD, his actions clearly raised the issue of individual domestic terrorism in the context of WMD.[29] While one can ponder the far-fetched "anti-government" sentiments that motivated McVeigh, the greater issue really revolves around individual access to WMD materials.

Finally, not all individual terrorism can be associated with hard-core political or religious ideologues. Individual terrorism can be committed by persons seeking personal rather than political gain, or even by individuals who are mentally ill. Indeed, considering the number of "Timothy McVeighs" in any given society, the prospect of individuals having easy access to WMD is chilling. The threat will only grow with time.

Current Methodology for Dealing with a WMD Terrorist Event.

By definition, the traditional approach to combating terrorism is encompassed in two terms—antiterrorism and counterterrorism.[30] Antiterrorism involves all those steps and actions taken by authorities to decrease the probability of a terrorist act occurring. It is the proactive, preventative stage to stopping terrorism. It includes techniques designed to harden potential high profile targets, e.g., government buildings or military installations, as well as actions taken to detect a planned terrorist attack before it occurs.[31] For example, the Pentagon is currently looking at new image-recognition technology through the Defense Advanced Research Projects Agency (DARPA) to assist in the battle against future terrorist attacks.[32] DARPA is experimenting with video surveillance, modeling techniques, and commercial technologies such as those used

to identify automatic teller machine customers by scanning their faces.

One of the most innovative antiterrorism technological projects is found in Britain. In the East London Borough of Newham, more than 200 outdoor cameras keep watch on

> pedestrians and passersby, employing a facial-recognition system that can automatically pick out known criminals and alert local authorities to their presence.[33]

Another innovative antiterrorism program is designed to ease tensions between the Federal Bureau of Investigation (FBI) and anti-government militias. This approach has FBI agents talking directly with militia leaders. From Montana to Indiana, federal agents have opened dialogues with leaders of several militia organizations to provide a forum for discussion in the hope that these channels of communication will help prevent violence.[34]

Counterterrorism measures are those tactical actions taken by authorities in response to a terrorist incident. Proper prior planning and training will obviously have a great impact on the success or failure of real world counterterrorist actions. In most areas of management, reorganizations are the product of some form of crisis. Counterterrorism initiatives are no exception. Since the 1980s there have been numerous legislative initiatives that address terrorist activities, most enacted on the heels of some terrorist attack. The central existing legislation dealing with WMD terrorism is the "Defense Against Weapons of Mass Destruction Act,"[35] commonly referred to as the NLD Act after its sponsors' names—Senators Nunn, Lugar, and Domenici.

The 1996 NLD Act envisions the creation of a domestic preparedness program which is intended to enhance federal, state, and local emergency response capabilities to better deal with a domestic terrorist incident involving WMD. The central thrust of this umbrella security program

involves the coordinated efforts of key U.S. departments and agencies focused on protecting U.S. personnel and property.[36]

While the Department of Justice, through the FBI, is still the lead agency in the event of a WMD terrorist attack, the expected mass casualties, physical damage, and potential for civil disorder resulting from a WMD incident have necessitated a gradual shift to DoD as the de facto lead Federal agency for many counterterrorism issues. However, on April 1, 2000, President William J. Clinton directed that neither the Under Secretary of Defense for Policy nor the Secretary of the Army, under executive agency powers regarding military support to civil authorities, has responsibility for "incidents involving chemical, biological, radiological, nuclear, and explosive consequence management."[37] Instead, should a large-scale WMD event occur in the United States, the Assistant to the Secretary of Defense for Civil Support will coordinate all domestic actions, although the Secretary of the Army would still provide the actual domestic civil assistance through the Army's Director of Military Assistance. Thus, while the individual state and local authorities still have the primary responsibility to respond to any emergency within their jurisdiction, when requested, DoD can provide extensive assistance should a WMD detonation overwhelm the state and local authorities.

The use of DoD personnel to help local metropolitan authorities quickly respond to a WMD event is the central vision of the NLD legislation. Accordingly, under NLD the Secretary of Defense works in close cooperation with the FBI, the Department of Energy, the Environmental Protection Agency, the Department of Health and Human Services, and the Federal Emergency Management Agency (FEMA) to provide direct support response to major cities in order to help local providers better deal with WMD terrorism.

A primary initiative of NLD includes the establishment of a nationwide training support plan with an initial focus on 27 cities in the United States, to be expanded to the 120 largest cities over the next several years.[38] In this program, DoD stands as the interagency lead for a new "first responder" training program, i.e., training the local resources of the affected urban area.

With a stated goal of providing WMD training support to U.S. major cities, the training is conducted primarily by the U.S. Army Chemical-Biological Defense Command and consists of 8-to-12-person training teams dispatched to each individual city. The team trainers are both active and reserve military personnel, DoD civilians, and contractors with extensive experience in emergency procedures associated with WMD. Actual training focuses on integrating metropolitan actions—by firefighters, police, and emergency medical technicians—to be taken after a WMD terrorist incident occurs. Specifically tailored to the needs of each city, six separate courses are taught: Nuclear, Biological, and Chemical Awareness; Operations During an Incident; Technician Hazardous Material (HAZMAT); Technician Emergency Medical Service; Hospital Provider; and Actions for the On-the-Scene Commanders. In this fashion, local first responders are provided with the expertise to deal with decontamination, crowd control, and search and rescue. With $300,000 set aside for each city, the program is scheduled for completion and final evaluation by 2002. By the end of 1999, over 84 cities had received NLD training from the military.

Initial evaluations of the NLD training program have been mixed. Richard Davis, a senior analyst with the U.S. General Accounting Office, reported that the program was fragmented and wasteful, adding little to a real world solution for responding in a unified way to a terrorist attack using WMD.[39] Others, however, continue to support the initiative, but recognize that the military role must be balanced against the reality of available resources. In this light, Secretary of Defense William Cohen announced in

April 1999 the creation of a 3-year advisory panel, headed by Virginia's Governor James Gilmore, to "assess domestic response capabilities for terrorism involving weapons of mass destruction."[40] The panel will report to Congress and the President on the challenge of WMD and the federal, state, and local response mechanisms which could handle the ensuing crisis.

Furthermore, in a July 1999 speech, Secretary Cohen listed five cautionary aspects of the NLD legislation regarding military support in the wake of a WMD event:[41]

• Any military assistance must be in support of the appropriate authorities.

• A clear chain of command and responsibility must be established for any type of support rendered by the military.

• Military assistance should not come at the expense of the primary mission of the U.S. military—to fight and win the nation's wars.

• The military response efforts will be grounded primarily in the National Guard and Reserve. The Guard and Reserve forces are the "forward-deployed forces here at home."

• The U.S. Government must not "trample on American lives and liberties in the name of preserving them." The military will not exceed legal authorities when performing a counterterrorism mission.

The U.S. Military—Active, Reserve, and National Guard.

Presidential Decision Directive (PDD)-39, "United states Policy on Counterterrorism," signed in June 1995, directed a number of measures to reduce the country's vulnerability to terrorism and to better manage the consequence of terrorist use of WMD. This PDD was revalidated in May 1998 by PDD-62, "Protection Against Unconventional Threats to the Homeland and Americans

Overseas." Both PDDs affirm that the FBI is the lead agency for crisis management and operations. Public Law 93-288, "The Federal Response Plan," provides the authority for the federal government to respond to disasters and emergencies as defined in the Stafford Disaster Relief and Emergence Act.[42] The plan describes the government's role in providing immediate action to save lives and mitigate property damage. FEMA is the lead agency for consequence management, i.e., care of casualties, decontamination, and clean up, and DoD is one of the supporting agencies for the FBI and FEMA, with the Army serving as the lead agency within the DoD.

Notwithstanding the chain of command which designates the Army as supporting other Federal agencies, the prevailing understanding is that the military will be called on to lead the "on the ground" emergency response in the aftermath of a significant WMD terrorist attack. However, those familiar with the facts know that because today's U.S. armed forces face serious problems meeting even the basic national defense requirements, they will inevitably encounter serious difficulties responding to requests for adequate and responsible support following a WMD event. In short, the stark reality of a scaled-down military suggests that the U.S. active duty military is simply not prepared to meet the demands associated with a major WMD terrorist event.

This state of affairs exists for two basic reasons. First, the continued downsizing of active duty Army personnel from 770,000 soldiers 10 years ago (total active duty personnel from all forces in 1990 was 2,043,705) to about 470,000 today has hollowed the military strength of the United States.[43] This reduction in the Army has forced a decrease from 18 to 10 divisions. Similarly, the Navy has had to cut by nearly half its number of ships, and the Air Force has cut its fighter wings from 36 to 20. Second, coupled with the downsizing of the active duty Army, the last decade has witnessed an increase in a wide variety of nontraditional missions which have siphoned off forces to

such places as Bosnia-Herzegovina, Iraq, Kosovo, Kuwait, Macedonia, Somalia, and Haiti.

Recognizing the overtaxed condition of the active duty military, Secretary Cohen has tagged the National Guard and Army Reserve forces as the primary response force to a WMD episode.[44] Accordingly, the Army Reserve's Regional Support Commands have realigned themselves along FEMA boundaries for ease of command and control during an actual WMD incident. An Army Reserve emergency operations center is available in each FEMA region that can support a WMD response. In addition, the Reserves have also provided several hundred emergency preparedness liaison officers to the 1st and 5th Armies (Reserve).

The announced rationale for having the National Guard and Army Reserve out front hinges on several factors. First, the National Guard and Army Reserves are supposed to be fully trained in how to function in a nuclear, biological, and chemical environment. Second, the Army Reserve has nearly 60 percent of the total Army's chemical defense and medical assets. Third, the National Guard and Army Reserve units can respond quickly because they are a community-based force.

Unfortunately, the picture of the National Guard and Army Reserve forces serving effectively in the context of a WMD event is not as rosy as painted by Secretary Cohen and others. First, the overall record of performance of today's National Guard and Army Reserve in traditional support roles has been troubled, particularly in regards to large-scale deployments. And this mixed performance makes problematic expectation that they will do much better in handling a full-blown WMD terrorist event.

Although the active Army has increasingly relied on the Army Reserve (208,000 personnel) and National Guard (357,000 personnel) to fulfill its critical missions in overseas operations, it has not come to grips with the problem of improving Guard and Reserve readiness. The Pentagon's so-called Total Force policy, which envisions a seamless

bond between the active and nonactive military forces, is still yet to be developed or fulfilled.[45] For example, in preparing for Operation DESERT STORM against Iraq in 1991, a tank brigade from the Georgia National Guard was slated for combat duty in the Gulf. However, even after the Guard spent more than 2 months of intensive training at the National Training Center in Fort Irwin, California, the Army believed the brigade was still not ready and refused to send it into combat. This is but one of numerous examples of problems associated with large-scale, stand-alone deployments of National Guard and Army Reserve personnel. While they are effective when used in small numbers and folded in with active duty soldiers, their job performance in independent military actions remains unproven.

The problem of readiness rests in part with the very nature of the force structure of these dedicated citizen soldiers. National Guard soldiers spend most of their lives in their civilian jobs, officially training in military skills only 39 days a year, usually a weekend a month plus a 2-week annual training exercise. While they are activated for duty in times of crisis, they rarely, if ever, are afforded the opportunities to rehearse large-unit operations, let alone train for a massive response to a WMD terrorist event.

Although Secretary of Defense Cohen's 1999 Annual Report to the President and the Congress recognizes the threat from WMD, there exists little sense of urgency to do anything other than have the National Guard *study* what services it might provide in the future:

> The National Guard will also complete its work in examining the roles, missions, and responsibilities that the National Guard may appropriately fulfill in responding to terrorist attacks involving WMD.[46]

It is not enough that the public be told that the National Guard and Army Reserve will coordinate with FEMA if WMD terrorism strikes. If the leadership in the United

States is serious about the issue of WMD terrorism, drastic and immediate steps need to be taken. At a minimum, this means creating a dedicated, trained, and effective WMD Rapid Response Force (RRF) in each of the 50 states.

Creating a WMD Rapid Response Force (RRF).

Studies have shown that hardening potential high profile targets such as federal buildings or military installations reduces the frequency of terrorist attacks on those types of facilities.[47] As an effective antiterrorist measure these types of preventive activities can and must be continued at key civilian and military facilities across the nation. In fact, a special emergency funding source now exists for the U.S. military to "react to unanticipated requirements from changes in terrorist threat level or force protection doctrine/standards."[48] This flexible funding source was created in 1997, providing a powerful tool for each commander-in-chief of a unified command to finance emergency high-priority antiterrorism requirements. These funds have been used to construct concrete barriers, clear vegetation, purchase equipment, hire personnel, set up security checkpoints, etc.

Tragically, despite such limited preventative moves the federal government has done almost next to nothing to better prepare for the catastrophic aftermath of a WMD event in an urban area. The paltry sum authorized by the NLD legislation to provide one-shot training courses to local first responders is a far cry from what needs to be done. In short, a frightened municipality will require a large and capable WMD RRF to provide order, treat casualties, and restore confidence. To be sure, the logical choice for developing this force should be the U.S. military.

Ever since the end of Reconstruction in the southern states, there has been a distinct aversion to expanding the role of the armed forces in the domestic arena. This is clearly reflected in the Posse Comitatus Act, which prohibits the active duty military from performing police duties in the

United States.[49] Accordingly, the idea of creating a centralized homeland defense force under a single command to handle the issues associated with a WMD terrorist attack has met with strong opposition from civil libertarian groups.[50] Paradoxically, the very organization that is most capable of responding to a WMD event is not given the task.

Nevertheless, in December 1999, the Secretary of Defense established a separate command called the Joint Task Force Civil Support (JTF-CS). The command is headed by Major General Bruce Lawlor (United States National Guard), with a budget of four million dollars and a staff of 36 personnel. The purpose of JTF-CS is to coordinate civilian and military responses to a WMD event in the United States. Once the President issues a federal emergency declaration and approves the use of the JTF-CS, it will support the designated lead federal agency with DoD's consequence management instruments in response to civilian and military WMD events.

Pending the real world use of the JTF-CS, Lawlor is tasked to work on integrated contingency plans for quick access to appropriate military assets that are otherwise unavailable to the civilian first-line responders. In the longer run, his role will expand, with the Task Force to be given direct oversight of the 15 Reserve/National Guard Regional Response Centers that will be activated by 2006. In commenting on the mission of his new command, Lawlor said,

> We don't do law enforcement or arrests. We will save lives, prevent human suffering, and restore as fast as possible critical life support systems in the community.[51]

The only alternative to the use of a centralized active duty military force would be the use of the National Guard and Army Reserve to create a WMD RRF for each state with the attendant funding to develop and train the necessary personnel. Following the 1991 war with Iraq, this idea was

quickly put into full force in Israel, where a Home Defense Command was set up. Building the command with 97 percent reservists, Israel set up 67 stations throughout the nation in order to better deal with the aftermath of a WMD event. In contrast, this same idea has not taken hold with policymakers in the United states.

The biggest obstacle to a WMD RRF in each state is the massive amount of funding and training required. Indeed, as the three most important considerations in buying a house are location, location, location, the three most important factors in building a WMD RRF would be training, training, training. And training requires money.

One way to help reduce costs for developing a WMD RRF is provided by the state defense forces model. USC, Title 32, Section 109, provides:

> In addition to its National Guard, if any, a state or territory . . . may, as provided by its laws, organize and maintain defense forces.[52]

State legislatures in 24 states and Puerto Rico have created state Defense Forces to perform a wide variety of functions, ranging from light infantry duties (the Virginia Defense Force) to military police functions (Ohio Military Reserve).

Of particular interest in looking at the mechanics of creating a WMD RRF is the example set by the Texas state Guard. During 1998, units of the Texas state Guard "participated in 122 events, which involved 1,865 members who contributed 24,663 man-hours and saved the state's cities $490,860."[53] These events included crowd control, traffic control, and search and rescue operations, entailing just the type of capabilities sorely needed in the aftermath of a WMD terrorist attack.

Unfortunately, until policymakers and the public come to understand that the number one civil defense issue confronting the United States is the threat of a WMD event, it is unlikely that steps will be taken to create separate

WMD-specific forces from the National Guard, the Reserves, or state Defense Forces. On the brighter side, if and when a WMD RRF is created, this force could receive valuable collateral training by assisting local law enforcement authorities during "normal" emergencies, as is the case with the Texas state Guard.

"Democracies Don't Engage in Terrorism."

Apart from all that can be said for the state of preparedness in the United States itself for responding to a WMD terrorist attack, there is comfort in the fact that a window of opportunity exists for the United States to create a new paradigm for reducing the likelihood of terrorism, at least on the international level. With the collapse of the Soviet Union, the addition of new democracies to the community of nations makes us more secure because, in the words of Anthony Lake,

> democracies tend not to wage war on each other and they tend not to support terrorism—in fact, they don't. They are more trustworthy in diplomacy and they do a better job of respecting the environment and human rights of their people.[54]

Recognizing a nexus between the nation that mistreats its own citizens and the nation that fosters aggression against its neighbors, both the preamble and Article 1 of the U.N. Charter make crystal clear that the framers believed that the unleashing of aggressive war occurred at the hands of those states in which the denial of the value of the individual human being was most evident.[55] Furthermore, with the research of former University of Hawaii Professor R. J. Rummel, it is now possible to demonstrate numerically the validity of the proposition that totalitarian regimes are the chief abusers of internationally recognized human rights and the most likely candidates for state-sponsored terrorism:

> War is not the most deadly form of violence. Indeed, I have found that while about 37,000,000 people have been killed in

> battle by all foreign and domestic wars in our century, government *democide* [genocide and mass murder] have killed over 148,074,000 million more. Plus, I am still counting. Over 85 percent of these people were killed by totalitarian governments.[56]

Thus, the new paradigm is a very simple model. If democracies make better neighbors, then it is certainly in the best interests of the United States to do all it can to foster these emerging nations and to thereby enlarge respect for the rule of law in international relations. In the words of Professor B. Russett,

> Democracies have almost never fought each other. . . . By this reasoning, the more democracies there are in the world, the fewer potential adversaries we and other democracies will have and the wider the zone of peace.[57]

The simplicity of Russett's argument should be clear to all. In fact, as Professor John Norton Moore of the University of Virginia School of Law explains, this simple fact represents a "new and more accurate paradigm about war, peace, and democide."[58] It replaces the old thinking and highlights the fact that democratic growth alone can hope to reduce the threat of WMD terrorism in the long run. A recent RAND study seals the point:

> The failure of regimes to provide for peaceful political change and the phenomenon of economies unable to keep pace with population growth and demands for more evenly distributed benefits can provide fertile ground for extremism and political violence affecting U.S. interests. For this reason, the United states has a stake in promoting political and economic reform as a means of reducing the potential for terrorism, some of which, as in Latin America, the Middle East, and the Gulf, may be directed at us.[59]

Conclusion.

Dealing with a WMD terrorist event requires two avenues of consideration, one short term, the other long term. In the short term, the United states must formulate

contingency plans that include the immediate establishment of a large and trained WMD RRF located in each of the 50 states. This cannot be a crisis-driven action. As pointed out earlier, the WMD RRF force would need to be trained from the ground up and dedicated to dealing with every aspect of a WMD event. In tandem with the establishment of this force, antiterrorism efforts must also be expanded. At a minimum, likely civilian and military targets need to be hardened as much as practicable.

In the long term, the United states needs to intensify efforts to assist the full development of fledgling democracies on the principle that democracies do not wage war or terror on each other. If the RAND study quoted above is correct, this strategy will go far in reducing the root causes of terrorism.

If necessary and appropriate actions are not taken now, it is certain that the effects of a WMD terrorist event will be far more devastating than necessary. The question is not whether there will be a WMD terrorist attack in the future, it is simply a matter of where.

ENDNOTES - CHAPTER 8

1. The RAND-St. Andrews Chronology of International Terrorism is a database of international terrorist incidents from 1968.

2. Ian O. Lesser *et al.*, *Countering the New Terrorism*, Santa Monica, CA: RAND, 1999, p. 12.

3. "Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments," Report to Congressional Requesters, Washington, DC: U.S. Government Accounting Office, April 1998.

4. Libya has not hesitated to finance, support, and even direct several acts of terrorism against various Western powers, to include the in-flight bombing of Pan Am Flight 103 over Scotland which killed 278 persons.

5. Vernon Loeb, "Anthrax Vial Smuggled In To Make A Point At A Hill Hearing," *Washington Post*, March 4, 1999, p. 1. Lauder's dozen includes Iran, Iraq, Libya, North Korea, and Syria.

6. Under international law, a receiving state is one that receives diplomatic materials from a sending state. A transit state can be any state through which diplomatic materials might pass. See Vienna Convention on Diplomatic Relations, opened for signature April l8, 1961, 23 UST. 3227, T.I A.S. No. 7502, 500 U.N.T.S. 95.

7. Jeffrey F. Addicott, "The United States of America: Champion of the Rule of Law or the New World Order?" *Florida Journal of International Law*, Vol. 6, No. 63, 1990.

8. See Report of the International Law Commission on the Work of its Thirty-Eighth Session, U.N. Doc. A/41/10, 1986.

9. The Vienna Convention on Diplomatic Relations was entered into force for the United States on December 13, 1972. The U.S. ratification appears at 111 Cong. Rec. 23, 733, 1965.

10. Perhaps the most widely publicized abuse of the diplomatic pouch to date, and one which clearly illustrates the controversy over the status of the bag, was committed by the Libyan government of Colonel Qaddafi. In April 1984, two Libyans gunned down 11 demonstrators and one British constable as they stood outside of the Libyan Embassy in London. Despite substantial suspicions that the weapons and other evidence connected with this heinous act of terrorism were disposed of through outgoing Libyan diplomatic pouches, the British authorities allowed the Libyans to carry them out of the country without searching or scanning them.

11. Address by Secretary of Defense Caspar W. Weinberger, American Bar Association National Conference on Law in Relation to Terrorism, June 5, 1986.

12. *Ibid*.

13. See, e.g., FBI Director Louis J. Freeh, Statement before the Senate Select Committee on Intelligence, January 28, 1998:

> The ease of manufacturing or obtaining biological and chemical agents is disturbing. Available public source material makes our law enforcement mission a continuous challenge.

14. William Nelson, "Opening Pandora's Box: The Status of the Diplomatic pouch in International Relations," *Fordham Int. L. J.*, Vol. 12, 1989, p. 494.

15. An early pattern was set regarding the use of force to counter state-sponsored terrorism under the Reagan administration. On April 14, 1986, the United States conducted bombing strikes on various targets in Libya. This was in response to the Libyan-ordered bombing of a discotheque in West Berlin on April 5, l986. The Clinton administration has followed a similar pattern of U.S. air strikes on suspected terrorist camps.

16. The right of a country to engage in acts of self-defense is well known in international law. The famous Caroline Doctrine, which defines the circumstances that permit forcible self-help, grew out of an 1837 raid by Canadian troops into New York. In response, Secretary of State Daniel Webster set down the rules for such acts of self-defense. He indicated that a nation may resort to necessary and proportional acts of self-defense if such acts arise out of an instant and overwhelming necessity, leaving no choice of means and no moment of deliberation. *See* William McHugh, "Forcible Self-help In International Law," *Naval War College Review*, No. 25, 1972, p. 61.

17. Article 51, U.N. Charter.

18. See, e.g., Guy B. Roberts, "The Counterproliferation Self-Help Paradigm: A Legal Regime for Enforcing the Norm Prohibiting the Proliferation of Weapons of Mass Destruction," *Denver Journal of International Law & Policy*, Summer 1999, p. 485.

19. See Louis Rene´ Beres and Yoash Tsiddon-Chatto, "Reconsidering Israel's Destruction of Iraq's Osiraq Nuclear Reactor: Aggression or Self-Defense?" *Vanderbilt Journal of Transnational Law*, No. 75, 1982, p. 417.

20. Paul Bedard, "Danger Zone," *U.S. News & World Report*, March 6, 2000, p. 10.

21. Lesser *et al*., p. 17.

22. David B. Ottaway, "U.S. Considers Slugging it Out With International Terrorism," *Washington Post*, October 17, 1996, p. 25.

23. It has been reported that those behind the 1993 World Trade Center bombing were also gathering the ingredients for a chemical weapon that could have killed thousands. Some reports indicated that the bomb might have been laced with cyanide, but the poison burned up

in the detonation. William S. Cohen, "Preparing for a Grave New World," *Washington Post*, July 26, 1999, p. A19.

24. *U.S. vs. Yunis*, 924 Fed 2nd 1086, D.C. Cir. 1991.

25. Loeb.

26. The most recent "real world" scare came in May 1995, when Larry Wayne Harris was arrested in his home for illegally obtained bubonic plague vials from a biological repository in Maryland.

27. *Ibid*.

28. *Ibid*.

29. Tim Kelsey, "The Oklahoma Suspect Awaits Day of Reckoning," *The Sunday Times* (London), April 21, 1996.

30. U.S. Army Training Circular 19-16, *Countering Terrorism on U.S. Army Installations*, April 1983, pp. 1-2.

31. Neil King, Jr., and David S. Cloud, "Casting a Global Net, U.S. Security Survived a Rash of Millennial Plots," *Wall Street Journal*, March 8, 2000.

32. "Seen Before," *Scientific American*, December 1999, p. 56.

33. *Ibid*.

34. Kevin Johnson, "FBI's Uneasy Alliance," *USA Today*, November 29, 1999, p. 1.

35. "Defense Against Weapons of Mass Destruction Act" contained in the National Authorization Act for Fiscal Year 1997, Title XIV of Public Law 104-201, September 23, 1996.

36. See Raymond E. Heddings, *U.S. Roles in Providing Humanitarian Assistance Following NBC Accidents/Incidents: The Legal Considerations*, Colorado Springs, CO: Institute for National Security Studies, 1999.

37. William J. Clinton, Memorandum for Secretaries of the Military Departments *et al.*, Subject: Consequence Management Responsibilities within the DoD for Incidents Involving Chemical, Biological, Radiological, Nuclear, and High Yield Explosives, April 1, 2000.

38. “Domestic Preparedness Program in the Defense Against Weapons of Mass Destruction, Department of Defense Report to Congress, May 1, 1997.

39. Bradley Graham, “Anti-Terrorism Plans Termed Inadequate,” *Washington Post*, October 3, 1998, p. 9.

40. “DoD Establishes A Weapons Of Mass Destruction Advisory Panel,” News Release No. 148-99, Office of Assistant Secretary of Defense for Public Affairs, Washington, DC, April 5, 1999.

41. Cohen, “Preparing For A Grave New World,” p. A19.

42. Stafford Disaster Relief and Emergency Act, 42 USC 5121.

43. See Annual Report to the President and Congress, William S. Cohen, Secretary of Defense, 1999.

44. *Ibid*.

45. *Ibid*.

46. *Ibid.*, p. 100.

47. Lesser *et al*., p. vii.

48. “Combating Terrorism Readiness Initiatives Fund,” Chairman of the Joint Chiefs of Staff Instruction 5261.01, March 1, 1997.

49. Posse Comitatus Act, 10 USC 375 and 18 USC 1385. The Posse Comitatus Act prohibits use of the military to execute the civil laws of the United States “except in cases under circumstances expressly authorized by the Constitution or act of Congress.” The primary prohibition of the Posse Comitatus Act is against direct military involvement in law enforcement activities. Generally, court interpretations have held that military support short of actual search, seizure, arrest, or similar confrontation with civilians is not a violation of the Act. Examples of permitted support include traffic direction and the provision of information, equipment, and facilities. The Posse Comitatus Act does not apply to a member of the Reserve component when not on active duty, nor to a member of the National Guard when not in federal service.

50. Elizabeth Becker, “Military Terrorism Operation Has Civilian Focus,” *New York Times*, January 9, 2000, p. 17.

51. *Ibid*.

52. 32 USC 109.

53. Captain Valentine J. Belfiglio, "State Defense Forces: Part of the Total Force," *Officer Review*, September 1999, p. 12.

54. Address by Anthony Lake, Special Assistant to the President for National Security Affairs, Johns Hopkins University, School of Advanced International Studies, October 21, 1993.

55. See Frank C. Newman and David Weissbrodt, *International Human Rights*, Cincinnati, OH: Anderson Publishing Co., 1990.

56. R. J. Rummel, *Death By Government: Genocide and Mass Murder in the Twentieth Century*, New Brunswick, NJ: Transaction, 1994, p. 12.

57. Bruce B. Russett, *Grasping the Democratic Peace: Principles for a Post-Cold War World*, Princeton: Princeton University Press, 1993, p. 4.

58. John Norton Moore, "Enhanced Effectiveness in United Nations Peacekeeping, Collective Security, and War Avoidance," Unpublished manuscript, 1997, p. 12.

59. Lesser *et al*., p. 128.

CHAPTER 9

BRUCE HOFFMAN'S VIEW OF TERRORISM BY WEAPONS OF MASS DESTRUCTION: ANOTHER PERSPECTIVE

Victor Utgoff

In his chapter titled "Terrorism by Weapons of Mass Destruction," Bruce Hoffman makes a number of valid points. His central thesis, in particular, is, in the view of this author, correct. The threat of terrorism by weapons of mass destruction (WMD) is clearly not as great as some of the sensationalized media presentations on the subject might suggest. Moreover, we can surely join Dr. Hoffman in taking comfort from the failure of the Aum Shinri Kyo to inflict mass destruction using chemical and biological weapons. This having been said, terrorism by WMD remains a serious threat. It is the purpose of this brief commentary to offer a slightly different perspective from Dr. Hoffman's and to suggest why we should continue to invest substantially in defense against an event of this sort.

There are three general points that need to be made. First, it is not logical to conclude that just because one large terrorist organization with deep pockets failed in its efforts to carry out large-scale chemical/biological (CB) attacks, others therefore will also fail. In fact, there is evidence to the contrary. Probably the best example of a successful attack is the one made on the population of Dalles, Oregon in 1984.[1] That attack was made by a local cult using cultures of S. Typhimurium, a bacterium that causes salmonellosis. These cultures were prepared in the cult's labs and clandestinely inserted in the salad bars of at least ten area restaurants. These attacks caused approximately 750 people to get seriously ill. Furthermore, had killing been its purpose, the cult could have used a lethal agent, and it could have attacked many more targets.

Second, Dr. Hoffman is undoubtedly correct in his claim that the difficulties of making and using CB weapons have been exaggerated. This is not, however, the same as to say that they are impossible to make and will never be used. He rightly observed that we have not, to date, accurately assessed how hard it is to make biological weapons suitable for large-scale terrorist attacks. The subject clearly calls for more investigation. What can we deduce at this point?

Some of my colleagues and I have undertaken preliminary analysis of this sort. Our research suggests that creating such a BW capability would take 1-2 years, require perhaps a half dozen people, and cost no more than a few million dollars. The project would require some careful cut-and-try engineering development and testing, not new science. The offensive BW programs once pursued by the United States, and apparently still continuing in Russia and elsewhere, have demonstrated that it is possible to make biological weapons capable of inflicting mass casualties. A great deal of information is available in the open literature on how to build such weapons. Legitimate industry employs machinery and processes that solve many of the problems involved in making practical biological weapons. And one cannot dismiss the possibility that terrorists might hire experts from foreign BW programs.

This suggests that a more careful and painstaking effort by the Aum Shinri Kyo or others should bear fruit and result in the production of effective biological weapons. It also, however, bears out Dr. Hoffman's contention that the effort might be more trouble than it is worth to most terrorist groups. The effort required to create a capability for large-scale BW attacks would be far greater than that required to blow tens or hundreds of people away with automatic weapons and truck bombs. Thus, Dr. Hoffman is right in arguing that nearly all of the terrorism we can expect to see in the foreseeable future will probably involve the use of conventional rather than CB weapons.

But nearly all is not the same as all. And the necessary components for successful CB attacks are already in existence. Certainly the necessary motives are present. Some terrorists are now driven not so much by the desire to use fear to bring about clearly definable objectives as by the desire to cause as much damage as possible. Then too the necessary means are there. Some private groups and individuals have already created and used biological agents to cause substantial numbers of casualties. Further, there are groups that have the money, engineering expertise, managerial capabilities, and patience for the kind of development and operational test activity that is needed.In my opinion, these necessary components should not be expected to come together often, but by the same token, can be expected to come together sometimes. And this is cold comfort.

My third general point is that the possibility of large-scale CB attacks on the United States is already real enough to deserve serious and well-funded attention by the government. Currently the federal government is attempting to create some initial capabilities specifically oriented toward reducing the consequences of CB attacks by terrorists against the public. To this end, it is spending something on the order of $100 million a year. By the standards of federal programs, this is not a great sum of money.

At the present time, the government does not appear ready to define what a full-blown defense against state or nonstate BW attacks might look like. However, my colleagues and I have done some preliminary analysis to assess the nature and costs of such a defense program. Our figures suggest that on the order of $5 billion per year could provide a respectable defense. The kind of defense we envision could drive down the losses from a very big CB attack to a 10th or less of what they could be without it. Clearly this level of expenditure is not prohibitively high. It also does not rule out taking serious measures against smaller-scale conventional terrorism.

To conclude, Bruce Hoffman is surely right to note that the threat from terrorists using WMD is probably not so great as the news media suggest. But the government is surely right to take the possibility of large-scale CB terrorism seriously and to begin preliminary steps toward defending the public against it. To fail to do so would be a dereliction of its duty.

ENDNOTE - CHAPTER 9

1. Thomas J. Torok *et al*., "A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars," in *Biological Weapons: Limiting the Threat*, Joshua Lederberg, ed., Cambridge, MA, and London, England: BCSIA Studies in International Security, MIT Press, 1999, pp. 167-184.

CHAPTER 10

THE NATIONAL INFORMATION INFRASTRUCTURE: THE ROLE OF THE DEPARTMENT OF DEFENSE IN DEFENDING IT[1]

Daniel T. Kuehl

Introduction.

Cyberspace is that place where electronic systems such as computer networks, telecommunications systems, and devices that exert their influence through or in the electromagnetic spectrum connect and interact in the telematic medium.[2] It is, from a military point of view, our newest operational environment. Threats, intrusions, and attacks are likely to be mounted against the United States in the future using this environment.

It is the thesis of this chapter that the Department of Defense (DoD) does have both a role and a responsibility in helping defend against this threat. To make the point, we will start by looking at an imaginary scenario in which a fictional state mounts an attack against this nation using cyberspace as its chief operating environment. This scenario will set the scene for a discussion of the security problems posed by the advent of the age of cyberspace. The chapter will (1) explain what we mean by cyberspace and why it must be understood as a new operational environment, (2) discuss the security implications of cyberspace, (3) discuss what "war" is in the context of the information age, and (4) conclude by considering the appropriate role of the DoD in combating cyberwar and cyber terrorism.

A Fictional Scenario.

The date: December, 200X; the place: the new operations complex for Triangle Telematics, the critical node for virtually all digital and electronic traffic in the entire eastern half of the United States; the problem: someone was inside the system, exploiting its connections to, and in many cases control of, computer and telecommunications systems that crisscrossed almost every key infrastructure.[3] The BIGGER problem: this "someone" was causing significant disruption to the efficient and effective functioning of many infrastructural elements. Because of the overall U.S. strategic situation, this caused a crisis. The disruption of Triangle Telematics coincided with one of the worst cold spells the Northeast had faced in recent memory. The sputtering of energy management systems thus caused acute hardship for millions. The attack also coincided with the height of the pre-Christmas shopping season, a period critical to the economic stability of thousands of businesses. Financial management and transfer systems were being adversely affected, raising the specters of both theft and lost revenue. Telematic networks—the marriage of telecommunications systems and computer networks—were behaving mysteriously; phone service to selected areas was collapsing for no apparent reason. Transportation systems, including air and rail networks, were unable to operate normally. Movement slowed, delaying everything from tangerines to tanks.

From a national security perspective, the transportation problem was especially crippling. The United States was also in the midst of a politico-military crisis in a particularly troublesome part of the world. It had just agreed to deploy a significant emergency force to Ruritania in order to aid that country in its resistance to aggression from its larger neighbor, Zenda. Now, as a result of the disruption of Triangle Telematic's networks, the machinery of deployment was grinding to a near standstill. The telecommunications network around Scott Air Force Base,

(headquarters for the U.S. Transportation Command, its Air Force element, the Air Mobility Command, and its Tanker-Airlift Coordination Center) was seemingly connecting to everyplace except where it was supposed to.

Thanks to the collapse of the civilian communications network, U.S. ability to direct the global flow of airpower and airmobile forces was "significantly degraded." The initial deployment of several fighter wings had failed because of inexplicable errors in arrangements made for their rendezvous with the aerial tankers. Now fighters and tankers were scattered all over the globe between the United States and Ruritania. The transportation network around East Coast ports had diverted tens of thousands of tons of military equipment urgently needed in Ruritania onto railroad sidings. When the Army brigade initially slated for rapid movement to the crisis area began preparations to move, the shocked commander received a report from his frantic chief medical officer that 77 percent of the troops were HIV positive. That, at least, is what their medical records indicated.

In short, the United States had been subjected to a successful cyber attack on its critical infrastructure. A high-level Presidential Commission was formed to study the causes of what could only be described as a strategic debacle and to suggest some solutions.

A year later, the Commission issued its long-awaited report. Even the sanitized version released to the press and public over the DoD's website could not minimize the degree of damage that had been done by what was now being dubbed the "Christmas Catastrophe." The national power of the United States had been dealt a serious blow via exploitation of its infrastructural vulnerabilities. The dollar losses to U.S. business were being measured in the billions. The death toll from mid-winter energy interruptions was tallied in the low hundreds. The shock to public confidence was severe, and the administration saw no way to recover in time for the pending national elections. As to the mission to

aid Ruritania, this failed. Ruritania rapidly accommodated—some would say capitulated—to its aggressive neighbor Zenda, a country intent on establishing itself as the anti-U.S. hegemon in the region.

The event was branded as this country's worst foreign policy disaster in a quarter century. Although the investigatory reports and nodal analysis of the incidents were not publicly released, there was no doubt that Triangle Telematics had been the key target of the attack. It offered massive connectivity to American businesses and those that depended on the businesses—including the U.S. armed forces. This connectivity proved to be both its greatest strength and its greatest weakness. It offered a gateway into America's infrastructures, a gateway that was strategically exploited, leading to a societal crisis and resounding strategic defeat.

A Revolution in Warfare: The Lessons of the Scenario.

The purpose of this brief glimpse into a possible future is to help us grasp some of the fundamental issues at stake about warfare in the information age. This, in turn, will help us answer the question lying at the heart of this chapter, "What role should the DoD play in defending our national information infrastructure?"

The scenario highlights a couple of major points. It makes clear that potential attacks on our infrastructure pose a serious threat to our national security, an issue that has been termed a "vital national interest" in the latest version of the President's National Security Strategy.[4] In our fictional scenario, Triangle Telematics constituted what Clausewitz would have called a "center of gravity," a strategic point critical to our military strength, societal well-being, and national will. By attacking Triangle Telematics, Zenda was able to penetrate a wide range of infrastructures. It degraded a diverse set of our national functions and capabilities, some purely societal, some

clearly military, but most serving both the society and the military. The attack on Triangle Telematics was, in short, responsible for the social crisis in the United States and for its strategic defeat.

At the same time, the scenario sheds light on why we are even bothering to ask the question of whether the DoD should be involved in protecting our information systems. In this scenario, Triangle Telematics was not attacked using force as it is normally understood, nor was it attacked via traditional environments—land, air, sea, or space. Had it been, there would have been little or no problem deciding who had the responsibility for defending Triangle Telematics; the role would have fallen to the Army, Air Force, Navy and Marines. But Zenda did not use any of these traditional warfighting environments when it attacked Triangle Telematics. It used cyberspace. Who, then, should defend cyberspace? Because it is a new environment, and because, as we will see, cyber attacks do not comfortably fit into our traditional constructs of war, the answer is not immediately obvious.

In short, we are experiencing an era of revolutionary change in warfare and we need to be aware of three key points: (1) cyberspace is a new operational environment; (2) it is of immense strategic importance to us, and it is at the same time a source of our vulnerability because we are increasingly dependent upon it and on the private sector which owns and controls much of it; and (3) traditional paradigms of warfare may not be applicable in this new environment. All these points must be taken into consideration as we seek to answer the question of the role and responsibility of the DoD in defending our information infrastructure. Let's discuss each in turn.

Cyberspace: DoD's Newest Operational Environment. Our starting point must be to define what we mean by cyberspace and explain why it must be understood as a new operational environment. To begin with, it is important to understand that information has exploded to the point

where it can no longer be encompassed by traditional concepts alone. Almost everyone understands information as a tool, a process, a target, even a weapon, to assist in the application of traditional force elements: blast, heat, and fragmentation.[5] While these concepts remain valid, they do not in isolation convey the import of what information has become in the world today. The synergistic interactions of electronic digital technology with an information-dependent society have, in fact, transmuted information into a virtual environment, with cyberspace as its physical manifestation.

It must also be recognized how very revolutionary this is. At first sight, this may not seem to be borne out by the evidence. Cyberspace was defined at the start of this chapter as that place where electronic systems such as computer networks, telecommunications systems, and devices that exert their influence through or in the electromagnetic spectrum connect and interact in the telematic medium. Understood in this way, it is clear that cyberspace has always existed. It must be realized, however, that it was not until very recent times that cyberspace became visible and usable.[6]

A useful analogy is outer space—it has always been there, but not until mankind developed technologies that enabled us to extend our affairs into it and use it to conduct terrestrial affairs did we fully comprehend that it forms another physical and operational environment beyond the land, sea, and air. Outer space does not have the same physical presence or properties of land or water—you cannot weigh or measure it in a useful sense—but it nonetheless exists because we can see the physical results of things that happen there.[7] The physical laws and principles that govern how systems function in these environments are the borders that fix the environmental boundaries.[8] Submarines function very well in an environment governed by the laws of hydrodynamics, but they cannot fly; the Space Shuttle works in an environment governed by the laws of orbital mechanics, but it cannot function submerged under

the water. All of these environments interact with each other and have synergistic effects, but they are distinct and unique.

The same holds true for cyberspace. Those devices and systems that operate in cyberspace function because they were designed to conform to and exploit the laws governing radiated and electronic energy. We can date our use of this environment to the mid-19th century and the invention of the telegraph, the first telecommunication system to operate in accordance with the laws of this medium.[9] The next 100 years saw steady and evermore technologically sophisticated advances in the ability to exploit and develop this medium—undersea telegraph cables, telephone, radio, television, microwave relay, even communications satellites—that extended the reach of communications to continental and eventually intercontinental distances.

We have enormously increased the volume of information that can be stored, manipulated, and transfered. But it has only been in the past 2 decades, the closing quarter of the 20th century, that the fortuitous marriage of these technologies with the microchip has led to attainment of "critical mass" and the emergence of cyberspace as a full-fledged environment. Cyberspace, therefore, is something very new, an environment in which military forces and society in general are only just beginning to learn how to operate.

Cyberspace: Strategic Importance and Strategic Vulnerability.

Cyberspace, then, is a new environment. But more than that, it is of immense strategic importance to us. Our imaginary scenario has already illustrated this. Let's look at another example. Every year, students from the different service war colleges meet in April at the Air Force War Gaming Center at Maxwell Air Force Base and engage in a week-long exercise called the Joint Land Air and Sea Simulation (JLASS). Blue team fights Red team. The

wargame is set in an Asian context. National Defense University (NDU) students specializing in information warfare are always the Red team, and every year they cause serious problems for the Blue team because of their mastery of information operations. In 1998 these NDU students developed a very interesting information operations war plan that targeted a whole series of information systems. On the very first day, the Blue team found, to its surprise and consternation, that certain of its system capabilities had been degraded by 25 percent. The Blue team students had not realized how much their military effectiveness depended on these systems. This anecdote vividly illustrates just how crucial information and information systems are to our military capability.

Cyberspace is also an environment in which the U.S. armed forces and the private sector are inextricably interconnected. The dependence, for example, of the DoD on civilian telecommunications networks is well known. The principle of dependency is not itself new. The military's need for reliable civilian communications dates back at least to World War I as demonstrated by the fact that the President exercised his legal power to take control of commercial radio and telephone systems. But the degree of dependency is new and growing rapidly.

DoD itself estimates that somewhere in excess of 90 percent of its daily communications are carried by commercially owned and operated communications systems.[10] The problem grew so acute that the National Security Telecommunications Advisory Council (NSTAC) was formed in the 1980s to provide a critical and very high-level interface between the telecommunications industry and the national security community.[11] During the Persian Gulf War of 1990-91, DoD drew upon commercial communications networks to assist in the deployment, support, and employment of American forces. This led to an ongoing debate about the legal restrictions on the use of some multinational communications systems such as Intelsat or Inmarsat.[12] As available bandwidth grows, the

demand for it seems to grow even more rapidly, as the recent air campaign in Kosovo clearly demonstrated.

Future warfare as conceived by American military planners in *Joint Vision (JV) 2010* (and its soon-to-be-published follow-on, *JV 2020*) will be highly information-dependent. Attaining and maintaining information superiority are increasingly regarded as indispensable parts of how Americans will fight. But this trend entails problems. Take, for example, the concept of focused logistics, which depends on the development of what is called a "reachback" capability. This connects globally deployed forces to critical nodes and bases far to the rear, as far back in some cases as the United States. Reachback capability reduces the size and scale of forces that need to be sent to any operational area. This improves the speed with which forces can be deployed and reduces the amount of support needed to sustain them.

But this speed comes at a price. The military's most recent instruction on Defensive Information Warfare noted that "use breeds dependence, and dependence breeds vulnerability."[13] While this might seem to be obvious, the implications for the future effectiveness of U.S. military operations are profound, because the increasing dependence of DoD on telematic systems that it neither owns nor controls confronts those forces with a potential vulnerability that may be difficult to counter. Since the linkage between commercial telematic networks and military capability is becoming ever more important to national security, the need for an effective partnership between those communities becomes increasingly important. This is a truth recognized in the latest National Security Strategy, which places great emphasis on the ability to attain information superiority.

The Role and the Responsibility of the DoD.

DoD clearly recognizes these realities. It is taking steps to ensure that it will, in fact, be able to operate in this new

environment. It is making efforts to reduce the vulnerability of which we have spoken, and recognizes the need for an adequate defense of that part of the national information infrastructure under the control of the private sector, even if the question of who conducts that defense is under debate. DoD is also working to develop new relevant technologies and keep apace of the rapid changes of the Information Age. Perhaps more importantly still, it is developing new concepts to suit the changing environment. The development of new technologies calls for new organizations and doctrines. It is these, not technological superiority alone, which lead to victory in war. History makes this abundantly clear; during World War II, for example, what enabled the German victory in France in May 1940 was not their technologies per se, which were not unique to them, but the way in which they were able to exploit them.[14] The American military does, in fact, recognize its need to make organizational and doctrinal change in the area of information warfare to bring about information superiority.[15] Cyberspace is indeed a new environment which is of great—and recognized—significance to the military.

Information War: A New Paradigm.

Ironically, however, despite the obvious importance of cyberspace to our military efforts and our national power, threats directed against us via cyberspace are not visible acts of war as traditionally understood. The problem is partly definitional. The Clausewitzian paradigm with which most of us are familiar is one where warfare is "an act of physical force, a pulsation of violence."[16] Its purpose is to "impose our will" on our opponents. It is waged by a special class of actors, called "warriors," who fight (using armed and violent means) on behalf of a special kind of political entity, called states. The information age is rendering this definition less relevant, and perhaps obsolete. This is because cyberspace may permit us to impose our political will without the use of physical force, without the pulsation

of violence. Under the circumstances, can cyberwar be classified as war? What *is* an attack in the information age? Who are the combatants? And what is an appropriate response to an attack that does not involve the pulsation of violence by a recognizable enemy?[17]

What is an attack? If we think back to the scenario with which we started, in no way, shape, or form is it clear that what happened via cyberspace amounted to an "attack." Certainly there were no kinetic actions like bomb explosions, nor were there any violations of national sovereign territory: no tanks or airfleets crossed any borders. Suppose, however, that in a slight variation of this scenario, the nation of Zenda were to target one of Ruritania's key communications networks. Suppose, furthermore, that it wreaked havoc on that country's military capability, degraded its key societal infrastructures, and created great disorder in political systems and economic affairs. Suppose it did all of this without the use of kinetic force and violence. Might not the Ruritanians argue that they had been "attacked"? Would they be wrong to claim that they were "at war" and entitled to exercise their "inherent right of self defense"? During the student exercise mentioned earlier in this paper the Red team developed a war plan against the Blue team that included information warfare attacks against such targets as the air traffic control system, financial centers, energy distribution network, and telecommunications infrastructure. The intent of these attacks was to degrade and disrupt the Blue team's political, social, and military cohesion.[18] Would these actions equate to "force," "armed attack," or "armed aggression," to use the terminology in the U.N. Charter? Does war between states, in short, require physical violence, kinetic energy, and human casualties for it to be termed war?[19]

There is a whole host of other questions that emerge. What is a combatant? According to the Clausewitzian paradigm, the warriors are the uniformed military—armies, navies, and, in more recent times, air

forces. In the student exercise just described, who is a "combatant"? What role is played by intent? How might the law itself change in response to the information age? How will long-established legal principles such as national sovereignty and the inviolability of national boundaries be affected by the ability of cyberspace to transcend such concepts? Will the technologies of the information age, by bringing atrocities and violations of the law of war into the intense and immediate glare of global public awareness, increase the observance of the legal norms of armed conflict?[20] These questions merely hint at the tremendous uncertainties that surround the evolving discipline of information warfare and the concepts of national and global information power.

We must search for a new and more satisfactory paradigm for warfare if we are to resolve such issues. This paradigm should remain true, as far as possible, to our traditional notions of war. If cyberwar, in other words, equates to warfare conducted via the environment called cyberspace, then it must meet constructively the criteria usually associated with warfare. It must be waged by a political entity that is an acknowledged actor in the international community, normally a nation-state. It must include military operations. It must involve overt hostility and the use of force, which normally entails physical destruction. This is where, however, cyberwar can be distinguished from other types of war. For, while most of the operations mounted by Zenda did not cause death or physical destruction, their intent *was* to compel the Ruritanians to do their will. Zenda, in other words, did use a form of force.

These definitional issues are of obvious relevance to the question at hand. It seems clear that *if* (and the verdict is not yet final) these activities can be called war, then the DoD must be in the forefront of our defense against them. It must lead any efforts to "protect and defend"—to use language from national policy on information assurance and the latest version of the National Security Strategy—our

"national cyberspace" and national infrastructures that are critical to military, economic, and societal security.[21]

Information War.

It must be clear by now that we are in need of a new paradigm that will permit us to deal with this new phenomenon of war in cyberspace. What *is* information warfare?

The earliest use of the term seems to have originated in the DoD's Office of Net Assessment, where Dr. Tom Rona was exploring the relationships among control systems, a field known as cybernetics. Dr. Rona described the competition between adversarial control systems as "information warfare," in the sense that control systems can be described as the means for gathering, processing, and disseminating information, processes which can be diagrammed and described with flow and feedback charts of mind-numbing dryness and complexity.[22] Later, with the publication of DoD Directive 3600.1 in 1993, we arrived at an official definition for the term. To add confusion, there were actually several definitions, at differing levels of classification.[23] Perhaps not surprisingly, this definition underwent frequent revision, with the current definition the longest-lived, in effect since promulgation of the current version of DoD Directive 3600.1 on December 9, 1996. Joint Publication 3-13, *Joint Doctrine for Information Operations*, published in 1998, incorporated the DoD language, probably ensuring that this definition will remain in effect for some time longer.[24] Let's glance at the current definition of information warfare (IW), along with the closely associated terms information assurance (IA) and information operations (IO), starting with the latter.

• Information Operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems.

• Information Warfare. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

• Information Assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

These definitions leave much to be desired in the areas of who, why, when, etc. Under the DoD definition, IW is an activity that only the military undertakes, and even then only under specific circumstances, while IO is a much broader and more inclusive field in which the entire government is engaged, in peacetime as well as wartime. An example of IO was the activity of Radio Free Europe, which operated during peacetime under governmental control. IA, on the other hand, is an activity that goes on constantly and engages all elements of national information power, including specific aspects of the private sector.[25]

Most U.S. service concepts of IW rest in part on the concept of the "information environment." Whether it is described as an environment, realm, domain, or whatever, there is a clear sense that information has become some kind of location where crucial operations are conducted. The Army's pathfinding doctrinal publication, Field Manual 100-6, *Information Operations*, even speaks of a "global information environment [and] battlespace" in which conflict is waged. The latest version of the U.S. Air Force's basic doctrinal publication explicitly addresses the need to dominate the information realm, describing information superiority as

> the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same. [It] includes gaining control over the information realm.[26]

IW/IO thus emerge as the struggle to control and exploit the information environment. Needless to say, this struggle extends across the conflict spectrum from "peace" to "war" and involves all the government's agencies and instruments of power. One advantage of this approach is that if one replaces "information" with "aerospace" or "maritime," you have defined air and naval warfare, or, more appropriate to our purposes, airpower and seapower. Thus information operations can be described as those activities that governments undertake to control and exploit the information environment via the use of the information component of national power.

DoD and Cyber Terrorism.

A strong case can be made that the DoD has a responsible role in the defense of our national cyberspace in the event of IW (cyberwar). There is far less consensus when it comes to how to deal with its lesser cousin, cyber terrorism. Cyber terrorism may be defined as the use of cyberspace by individuals or non-state/transnational groups to cause human injury or physical damage and induce fear for political purposes.

There is, first of all, quite a lively debate over whether it should be a civil law enforcement or a national security community responsibility. Cyber terrorism differs from cyberwar in the same way that the non-cyber variants differ: the political status of the actors. While most terrorism is conducted in order to achieve some type of political objective, the actor lacks the legitimacy of a nation-state or other recognized political entity. It is therefore usually viewed as a crime, and the task of dealing with criminals traditionally belongs to the U.S. law enforcement community rather than the military.[27]

Can the military do nothing? It is certainly constrained to a degree. The Posse Comitatus Act, for example, enacted in 1878 in response to the unrest of the Reconstruction era, essentially prohibits the uniformed military from acting in a

civilian law enforcement role. However, the prohibition is not absolute. The DoD *can* assist the civil law enforcement authorities under the proper conditions and safeguards.[28] Indeed, over the past several years the military has played an important role in assisting and cooperating with civil authorities in their war on drugs. According to some analysts, it could and should assist in the fight against terrorism and cyber terrorism.

There is also a debate over the role that should be played by the private sector. This added twist stems from the pervasive involvement of the private sector in cyberspace. The private sector owns and operates many of the information systems and networks that would be affected by the terrorists. It would thus seem to have a stake in the defense of our information infrastructures. But cooperation with the private sector is by no means easy to achieve or universally desired.

The effort to defend against cyber terrorism is complicated by the very different interests and perspectives brought to bear on the problem by the DoD, the law-enforcement community, and the private sector. The private sector sees the information revolution as a means for expanding business opportunities and exploiting organizational changes to create a global economy. Its concern quite naturally is whether a partnership with government would affect their business. Would it, for example, lower their profits? Undermine consumer confidence? Lead to restrictive regulation?[29] It tends to see government involvement as an unnecessary impediment to swift progress.

The law enforcement community, trying to fight the twin scourges of organized crime and political terrorism, sees the information revolution as a frightening collection of capabilities that their adversaries can exploit to operate inside of law enforcement's OODA Loop, the famous Boyd cycle of "observe-orient-decide-act." The growing reliance on cyberspace also makes it an objective in and of itself.[30]

As to the national security community, in particular the DoD, it faces a very real dilemma. Its ability to operate globally has become increasingly dependent on this new environment, yet, at the same time, its ability and authority to protect and defend cyberspace is limited.[31]

None of this would matter so much if it were not that cyber terrorism appears to be a serious and growing threat around the world. A number of political groups around the world have come to see cyberspace as an inviting new medium in which to commit terrorist acts. More than a decade ago, for example, the Italian Red Brigade's operational manifesto specified the destruction of Italian computer systems and facilities as a means of "striking at the head of the state." Similarly, the Sinn Fein arm of the Irish Republican Army attempted to bomb computer and telecommunications systems supporting the British financial network.[32] In the past few years, groups such as the Tamil Tigers from Sri Lanka, the East Timorese resistance movement, and the Maxican Zapitistas have all employed Internet-based efforts to exploit cyberspace for revolutionary purposes.

Cyberspace presents some obvious advantages to such groups. The entry costs are negligible. Often, no more is needed than a computer and Internet access. Yet the effects of an attack can be rapid and intercontinental. There is almost no physical risk to the attacker, while a direct forceful impact can be directed against large faceless entities such as corporations or government agencies. These, rather than innocent individuals, comprise the enemy. Attacks of this sort are less likely to result in a hostile popular reaction.[33] The use of cyberspace for these purposes is not likely to diminish.

International Strategies.

In this new environment, so vital to both business and national security, an effective defense against diverse threats in cyberspace can come only from a partnership

among all the interested parties, private sector as well as government. While the United States has been described as the most information-dependent nation in the world, it is by no means the only nation whose society and military forces rely heavily on the new technologies of the information age. Many, if not most, of the world's more technologically advanced countries have become aware that information and the infrastructures that depend on digital information are critical to societal stability and national security.

In 1998 the Australian Parliament received a report on the high-tech threat to that country's critical infrastructures. The collapse of the electric power grid in Auckland, New Zealand, the following year, although caused by a mechanical failure, not by terrorists, pointed out the economic and social costs of such infrastructural degradations.[34] The Norwegian government has established a commission to study the vulnerabilities of that country's infrastructures, and the Swedish government has undertaken a similar effort. Many of the NATO countries have had discussions with American authorities, at least at the level of protecting military systems and networks. But it is at a higher level that some very interesting developments are underway.

In the summer of 1998 the President of the Russian Federation sent a draft resolution to the United Nations Secretary General. The key portion of the resolution aimed at

> developing international legal regimes to provide security of global information and telecommunication systems and combat terrorism and criminality in the field of information.

Particularly interesting about this proposal was its organizational path of entry: it was introduced via the First Committee, which deals with issues of disarmament.[35] After consultations with other delegations, including the United States, the draft was rewritten. In its new form the resolution aimed to develop

> international principles [to] enhance the security of global information and telecommunication systems and help to combat information terrorism and criminality.

This resolution passed the General Assembly by consensus on December 4, 1998. While it does not, of course, have the force of international or domestic law, it established the basis for further work, which continues.

While the Russian proposal was primarily concerned with military information warfare, there are other efforts underway more tightly focused on the civil or criminal aspects of the issue. In March 1999, a committee of experts on crime in cyberspace, a subgroup of the Council of Europe's Committee on Crime Problems, issued a working draft of a position on cyber crime.[36] The draft focused on such issues as extradition, mutual legal assistance, and trans-border computer searches. These are thorny issues that will not easily be resolved. The draft did not appear to define cyberspace, although the draft was clearly focused on computer systems and the interactions between systems linked across national borders.

In October 1999, a G-8 Ministerial Conference on combating transnational organized crime met in Moscow and issued a communiqué. It made multiple references to computer crime, stressing the need to continue work on an action plan to deal with high-tech and computer crime. Six weeks later, Stanford University's Hoover Institution hosted a symposium to explore ways to develop international cooperation to combat cyber crime and terrorism. The symposium's closing session focused on a proposal for an international convention, drafted by the Center for International Security and Cooperation, or CISAC, to combat cyber crime and terrorism. The CISAC considered some of the same issues as those covered in the Council of Europe draft, also providing specific explanations of offenses. Members of CISAC are currently in the process of gathering comments and inputs before revising the draft.

In short, the seriousness of the threat is well recognized not only within the boundaries of the United States, but beyond.

Conclusion.

We return to the question with which we opened this discussion: "Does the DoD have both a role in and a responsibility for defending American cyberspace?" Clearly, the National Information Infrastructure is of critical and growing importance to American economic strength, political vitality, national will, and military power. A growing number of government publications, directives, and policies relating to information and its role in national security provide evidence that this issue will increase in importance. The newly issued government policy paper, "Defending America's Cyberspace: National Plan for Information Systems Protection," is a detailed and comprehensive approach to this issue. There seems to be little question that cyberspace is an operational environment crucial to military capability, but there is much less consensus that this is an environment in which the DoD has a role outside of the confines of purely military systems and infrastractures. But the mission of America's armed forces is quite clear: to provide for the common defense. The growth of cyberspace as an environment critical to America's security and well-being means that the DoD has both a role and a responsibility, albeit in conjunction and cooperation with law enforcement and the private sector, to protect this environment from "all enemies, foreign and domestic." To do less would be to endanger national security and abdicate the responsibility assigned it by the American Constitution.

ENDNOTES - CHAPTER 10

1.The views and opinions contained in this paper are those of the author and should not be construed as the official position of the U.S. Government, the Department of Defense, or the National Defense University.

2. The term "telematics" probably originated in the United Kingdom in the 1980s. It refers to an evolving disciplinary area that incorporates telecommunications and communication networks. In today's world, which is massively interconnected and becoming more so every day, those worlds are now inextricably bound together.

3. These infrastructures are described and the potential threat outlined in a 1999 publication issued by the White House's Office of Scientific and Technology Policy (OSTP), "Cybernation: The American Infrastructure in the Information Age," available online at *http://www.whitehouse.gov/WH/EOP/OSTP/html/cyber2.html*.

4. See *A National Security Strategy for a New Century*, published by the White House in December 1999 and available online at *http://www.whitehouse.gov/WH/EOP/NSC/html/documents/nssr-1299.pdf*.

5. I am indebted to the Director of the National Security Agency, Lieutenant General Mike Hayden, for the terminology used here.

6. While it's impossible to say when the term "cyberspace" was first used, several authors stand out as being among the leaders. William Gibson's classic work of science fiction, *Neuromancer* (New York: Ace, 1984), first broached the concept of humans seamlessly operating within a cybernetic, virtual reality environment, while Nicholas Negroponte's book, *Being Digital* (New York: Knopf, 1995), is an exploration of the impact of cyberspace on our daily lives. The 1999 movie hit, *The Matrix*, is yet another exanple. The term itself has only recently come into widespread use. A search of several automated databases, for example, covering the years 1986-89 and 1986-91 contained only 17 "hits" on the term; the same databases for 1996 contained 754!

7. Of course outer space can be measured in a scientific sense, but not in terms useful in a lay sense.

8. The question of where the borders of cyberspace lie is an intriguing one. Michael Benedikt has written perceptively on it in his book, *Cyberspace: First Steps* (Cambridge, MA: MIT, 1991), while Anne Wells Branscomb in a recent monograph *Cybercommunities and Cybercommerce: Can We Learn to Cope?* (Harvard University, Program on Information Resources Policy), suggests that the borders of cyberspace are discernible at the interconnection points between segments of the Internet, with network managers and systems administrators acting as the border guards, in a sense. A striking graphical representation of this is available at *www.peacockmaps.com*.

The technology of cyberspace makes "virtual" organizations ever more plausible and perhaps in some scenarios even desirable. Four people physically located on the Greenland icecap, in the Australian outback, in the Amazon rainforest, and halfway up Mount Everest will be able to meet in cyberspace, discuss a problem, develop a solution, and monitor the corrective actions via information technologies. Already, totally global voice communication is possible via satellite-based telephone systems such as Iridium (see their website at *www.iridium.com*) or Globalstar (at *www.globalstar.com*), and within a few years it is planned to have the same capability for heavy bandwidth data transmission. See, for example, the Teledesic plan at *www.teledesic.com*. Regardless of the financial difficulties which Iridium has encountered, the movement of telematic architectures into space is a trend which can only continue.

9. This construct omits communication methods such as signal flags, smoke signals, drums, or even heliograph because they did not require manipulation of the electronic environment. The interest of the national security community in cyberspace thus dates to the Civil War, in which the national, political, and military leadership of both the North and South depended on the telegraph for strategic direction of their respective war efforts.

10. See the "Report of the Defense Science Board (DSB) Task Force on Information Warfare-Defense," January 8, 1997, available online at *http://cryptome.org/iwd.htm*.

11. By "high-level," we mean interface between CEOs and the President of the United States. See *www.nstac.org* for details. Note that this was not the only reason for the formation of this institution, but it was certainly an influential factor.

12. Richard A. Morgan, "Military Use of Commercial Communication Satellites: A New Look at the Outer Space Treaty and 'Peaceful Purposes,'" in *Journal of Air Law and Commerce*, Vol. 60, No. 1, September-October 1994.

13. CJCSI 6510.1, *Defensive Information Warfare*, 1998.

14. The Germans were not superior in any one category. They had tanks, to be sure. But so did the French and British. They had the airpower. But so did the French and British. They had radios and effective command and control. So did their enemies. Then why were the Germans able to take their tanks through the French and British lines in May 1940 like a hot knife through butter? The answer is that the human element made all the difference. The Germans made

organizational changes (Panzer divisions and even Panzer corps) and developed an operational concept, a doctrine (we like to call it "lightning war") to employ the technology in a novel way.

15. We are evolving the necessary new concepts like "dominant battlespace knowledge" or "network centric warfare."

16. See *On War*, Book One, Chapter 1, for Clausewitz's complete analysis of these relationships.

17. In early 1999, then-Deputy Secretary of Defense John Hamre testified before Congress concerning recent intrusions into U.S. military computer systems, intrusions apparently originating in Russia. Hamre said that a "cyberwar" was underway. This mischaracterization of the incident is an example of the murkiness of the terminology, because while the incident could certainly have been called cyber-espionage, it was hardly war.

18. While this example could be dismissed as an American example of mirror-imaging, a recent book published in China by two colonels in the Chinese Liberation Army, *Unrestricted Warfare*, suggests that such concepts are gaining wider acceptance among other military forces.

19. See Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law*, Vol. 37, No. 3, 1999); Walter Gary Sharp, Sr., *Cyberspace and the Use of Force*, Falls Church, VA: AEGIS Research Corp, 1999; and Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, *Information Warfare and International Law*, Washington, DC: National Defense University Press, 1997, available online at *www.dodccrp.org*.

20. Information warfare also raises specific legal issues related to computer crime: what is a crime, who commits it, and what does the law say about it?

21. *A National Security Strategy for a New Century*, December 1999.

22. This author first heard Dr. Rona's ideas during a presentation on June 13, 1994, at the Information Resources Management College, National Defense University, in Washington, DC. He defined IW as

> the sequence of actions undertaken by all sides in a conflict to destroy, degrade, and exploit the information systems of their adversaries. Conversely, information warfare also comprises

all the actions aimed at protecting information systems against hostile attempts at destruction, degradation, and exploitation. Information warfare actions take place in all phases of conflict evolution: peace, crisis, escalation, war, de-escalation, and post-conflict periods.

23. During the initial classroom meeting of the School of Information Warfare and Strategy's first class in August 1994, the 16 students reacted with dismay to the plethora of official and unofficial definitions of IW. While some believe that any attempt to fix a definition of IW at the present time is premature and counterproductive, others believe that some degree of imposed consensus is essential, and that unless the different organizations involved in the issue have some common terminology, any attempt to plan is doomed to frustration and failure. While this author agrees that trying to fix terms for all time is futile because the discipline is still evolving, some kind of terminological commonality is vital.

24. One of the reasons for the creation of the term "information warfare" is the visceral dislike and mistrust of the word "war" by many of the agencies and people who are beginning to find that the information age envelops their activities and mission. Thus the creation of a term that points at the larger arena in which information "stuff" is conducted, but does not tie those operations so visibly to the military.

25. See the author's "Defining Information Power," published by the National Defense University Press as Strategic Forum #115, 1997, available online at *www.ndu.edu*.

26. See Field Manual 100-6, *Information Operations*, U.S. Army Training and Doctrine Command, August 1996; also see Air Force Doctrine Document–1, *Air Force Basic Doctrine*, USAF Doctrine Center, September 1997, pp. 31-32. FM 100-6 is currently under revision. Some would suggest that it is under attack rather than revision, by traditionalists who see IO solely in terms of an enabler or force multiplier rather than as something that could be the central or decisive element of a campaign. While not so pronounced, similar currents are detectable within the Air Force as well.

27. This oversimplifies. There is still a lively debate over the question of whether counterterrorism is primarily a civil law enforcement or national security community responsibility.

28. A detailed exploration of this issue can be found in Gregory D. Grove, *The U.S. Military and Civil Infrastructure Protection: Restrictions and Discretion Under the Posse Comitatus Act*, Palo Alto,

CA: Stanford University, Center for International Security and Cooperation, 1999.

29. A symposium was held at the Supreme Court in the Summer of 1998, after issuance of PDD-63. During one discussion a lawyer from a private sector firm asked quite pointedly of the government representatives, "What's in it for me?" This is, of course, an entirely valid question for the private sector to ask. Fearful of increased governmental regulation and bureaucracy, they view "help from Washington" with a jaundiced eye. If the government cannot effectively make the case that IA is a shared need, the partnership called for by both PDD-63 and the *Report of the President's Commission on Critical Infrastructure Protection* (PCCIP), published in 1997, will be difficult if not impossible to attain. The PCCIP Report is available online at *www.ciao.gov*.

30. This was one of the key issues addressed by the President's Commission on Critical Infrastructure Protection.

31. Efforts are underway in academia as well as government to study the problem. The Carnegie Endowment for International Peace, for example, has launched a study on the information revolution and world politics, with cyber terrorism as one of its key issues. See their website at *www.ceip.org*.

32. See Andrew Rathmell, "Assessing the IW Threat From Sub-State Groups," in *Cyberwar 2.0: Myths, Mysteries and Reality*, Alan Campen and Douglas Dearth, eds., Fairfax, VA: AFCEA International Press, 1998, pp. 295-312.

33. Devost, Pollard, and Houghton, "How Safe is Your Toaster?" in *Sun Tzu and Information Warfare*, Robert E. Neilson, ed., National Defense University Press, 1996.

34. See Adam Cobb, *Thinking About the Unthinkable: Australian Vulnerabilities to High-Tech Risks,* Parliamentary Research Service, June 29, 1998; available online at *www.aph.gov.au/library/pubs/rp/1997-98/98rp18.htm*.

35. Diplomatic historians and scholars familiar with the early history of the Law of War and other international agreements such as that at the Hague Conference of 1899 may recognize the motivations behind Russian sponsorship of that meeting a little more than century ago. Russian fears of advanced German and Austro-Hungarian military technology had led to an understandable effort to restrain the development and deployment of such technology.

36. This draft, issued on March 11, 1999, was the 14th attempt prepared by the Directorate of Legal Affairs.

CHAPTER 11

DANIEL T. KUEHL'S VIEW OF DOD'S ROLE IN DEFENDING THE NATIONAL INFORMATION INFRASTRUCTURE: ANOTHER PERSPECTIVE

Phillip E. Lacombe

The previous chapter by Dr. Daniel Kuehl has much to commend it. Broadly speaking, I share his understanding of the problem and his evaluation of what needs to be done. If I have any reservations, it is that Kuehl has not gone far enough in stressing the urgency of the problem and the need to deal with this important challenge.

This brief chapter will therefore not so much modify, as underline, the points made by Kuehl. It will draw on my experience as a member of President William J. Clinton's Commission on Critical Infrastructure Protection (1996)[1] as a member of the Transition Office that followed, and my work at a company whose business is closely linked to this very problem. The chief purpose of this discussion will be to argue for some profound changes in the way we think.

The Nature of the Threat.

The first point to make is that the cyber threat has developed with quite extraordinary rapidity. In 1996, when I was considering whether or not to join the President's Commission on Critical Infrastructure Protection (PCCIP), I was advised against the move by a very senior defense official. His words of caution were, "Don't go, there's no threat, it's a flash in the pan, and will be gone in a heartbeat. You won't be doing anything important." And at that early date there was reason to believe he might be right. Within the information warfare arena, there were people who were

seriously concerned with the issue. But they were largely alone. No one else seemed to be paying attention to the problem, not operational commanders, not the law enforcement agencies of the United States, not businesses, and not the press. Two and a half years later, after the commission issued its report, and in particular after February 1998 when the solar sunrise woke people to the danger, the level of concern is enormously higher. It is clear that our information infrastructure is at risk, and that attacks on it cannot be taken lightly.[2]

The suddenness with which the threat developed has considerable implications. The seriousness of any threat is related to the amount of damage it can inflict and to our ability to defend against it. Cyber threats pose some unique challenges to us in part because they are so very new. This means that not only must we find ways to deal with new complexities, but we must also draw upon our imaginative resources to come to terms with a phenomenon outside of our traditional experience. In doing so, we must overcome deeply rooted cultural assumptions. We must do some radical rethinking.

Critical Infrastructure Protection: A Neglected Effort.

One of the most strikingly obvious features about attacks on our information infrastructure is our failure to accept it as the threat it is. Clearly such attacks have the potential to do enormous damage to our nation. Kuehl illustrated this very effectively in his chapter. It is a fact that all of our infrastructures rely on communications and information systems. The water system in Los Angeles is controlled by a phone and computer system. It opens and closes gates in the water system using computer controls over the phone. All the electrical power in the United States is delivered by way of the computer systems that control it. In the near future, electrical power will be delivered using a new system called Oasis. Electrical power will be auctioned

in real time. This has clear advantages; the American people will get the best rate in their homes, businesses, and agencies. At the same time, however, this system will be controlled by computer and communication systems, enabling the systems to run without the intervention of individuals. This will create a new vulnerability. Weapons of mass disruption, as cyber attacks have been dubbed, are indeed a serious problem. Yet, as we have already said, recognition of the full scope of the problem has been very slow in coming. What explanations are there for our reluctance to accept reality? And what can be done about this?

First, we have had relatively little historical experience of attacks on our infrastructures; the last time America's information infrastructures were attacked was during the War of 1812. This means that we must call upon considerable powers of imagination to grasp what such an event would entail. We must ask ourselves basic questions. How would we be affected by an attack on our information infrastructure? What do we mean when we say that this or that institution is "at risk"? Let us consider here the example of a library. Many American children today visit the library by computer. Rather than going to the physical building, they access the data base using their home or school computers. If their internet service is cut off, so too will be their ability to access the library. When we start to think through some of these realities, we will begin to better understand the profound ways in which our daily lives would be affected in the event of a cyber attack.

Another explanation for the failure of many to grasp the serious nature of the threat to the information infrastructure lies in the complexity associated with the information system itself. We do not fully grasp the notion of cascading effects. We do not remember that the electrical power system affects water supply, that the lack of electrical power or the lack of telephone availability in turn affects a whole host of other vital services. Once again, we must

expand our powers of imagination and improve our thinking.

Cultural assumptions are also to blame for our myopia when it comes to the information threat. There is an old adage that runs, "Sticks and stones may break my bones but words will never hurt me." We have grown up with the notion (rightly or wrongly) that we cannot be hurt or do hurt by words (read "information"). We minimize and misunderstand the nature of the threat. This can also be illustrated by thinking about the reaction of typical American parents when they catch their children hacking into computer systems. Most parents do not seem to grasp the fact that this is not only a crime, but dangerous. In their minds, their children are merely gaining access to information.

We must rethink what we mean by information and come to recognize that, contrary to our comfortable assumptions, the state of communications can hurt you. Bits and bytes do now contain the ability to harm to the nation.[3] We must also recognize that information is no longer "just" information. It is property.[4] It has value independent of anything else, and we need to start to think about it in these terms. If and when parents begin to appreciate the act of hacking as a property crime, they will come to have a better appreciation of its seriousness.

New Paradigms for Dealing with Cyber Threats.

The newness of the cyber threat also increases the challenge by rendering obsolete many of our traditional paradigms. How, for example, should we defend our infrastructure? As a nation, we are accustomed to a particular way of defending against threats. In the past, we have followed a model whereby we sought to identify our enemies, understand their motives, and anticipate their potential targets.

This paradigm simply does not work in the case of a cyber attack. When something happens in the cyber dimension, when a computer system is broken into, when a telephone system goes down, when an internet service provider's capabilities are saturated or spammed[5] out, we do not necessarily know who is responsible for the problem, nor why that person is doing what he or she is doing. There are no explosions, gunfire, or blood in the streets to give us an indication or warning of a pending threat. A cyber attack can be perpetrated using nothing more than a 486 computer, a telephone line, and a modem. How is an intelligence agent to anticipate such a threat? Even after an attack, it is hard to identify the perpetrator, as Kuehl has clearly pointed out.

Given the extreme difficulty of actually determining the "who" or "why" of an attack, our conventional model becomes dysfunctional. But from the standpoint of how we are affected, the distinctions are in any event irrelevant. Consider a major retail company that finds itself unable to conduct business because its information network is down and it cannot process a transaction. It really does not matter whether the problem was caused by some 14-year-old in Stockholm playing around on the internet, or by a competitor or foreign country intending harm. The fact is that the business will suffer and is vulnerable, regardless of who the "actor" was or what his or her motives were.

This is why we must rethink how we deal with threats. The President's Commission concluded that we should think about the threat in terms of capability and vulnerability rather than in terms of actor and motivation. We must, in other words, start to think in terms of what our vulnerabilities are and whether or not the capabilities exist to exploit them. It is clear that our systems are vulnerable. It is also clear that the capability of disrupting our information infrastructure does exist. Those in doubt should read up on the modus operandi of well-publicized hackers. It will become clear in very short order that all their tools are extraordinarily modest.

Another important point to register about "targets" in this new environment is that public confidence itself is today a target. This is not in and of itself really new; Bruce Hoffman, for example, has drawn attention in his chapter to the crucial role played by public confidence in terrorism. But it is important to recognize the way in which cyber attacks can erode public confidence and thereby disrupt our nation. A hypothetical example here will illustrate the point. Suppose a hacker were to intrude into the computer systems of Citibank, causing some 100,000 people to lose $20 each in their bank accounts. Suppose the hacker quit after a day or two but also published an advertisement in the *New York Times* and told everyone what he had done. Suppose he also threatened to do the same thing again if his demands were not met. What do you suppose this would do to public confidence? It is not difficult to appreciate that it would not only erode trust in the banking system, but might also undermine public trust in the U.S. Government and its ability to defend its people.

Who Is Responsible For Defense?

I shall conclude by taking a brief look at the question of responsibility, a theme lying very much at the heart of this anthology and clearly addressed by Kuehl. Who is responsible for protecting those infrastructures that are at risk? Here again, it seems that we shall need to think about this issue in far from traditional ways. We must find new ways to approach defense, law enforcement, intelligence, and other activities as they relate to cyber threats.

Consider the question of the role of the military. Should the military be involved in the defense against cyber attacks? While the U.S. military has no problem understanding that its job might be to protect Joe's Corner Market from a missile strike, it has a harder time understanding that its job might be to protect Joe's Corner Market from a cyber attack. Either type of attack, nonetheless, is likely to cause Joe's Corner Market to go out

of business. Kuehl is no doubt correct when he says that the Department of Defense (DoD) should be involved in the protection of our information infrastructures. Yet, as long as we continue to think of attacks as confined to acts of physical violence, this function will seem to be unnatural. We thus must rethink our conventional notions of what constitutes an attack.

We must at the same time redraw the boundaries between public and private spheres. Where information is concerned, every improvement in defense capability in the private sector is tantamount to increasing our national security. We must do more to bring about an effective partnership between the government and business. Such a partnership would entail, among other things, the sharing of information among these groups. Both government and the private sector have shown themselves to be profoundly hesitant to do so, as this author, whose career has straddled both sides of the dividing line, is very much aware. And their hesitation is perhaps understandable.

From the perspective of a private company, entering into a partnership with government may entail some serious risks. The government clearly needs to know when AT&T, Citibank, or Joe's Corner Market is hacked into in order to defend the nation better. Private companies are not insensitive to this need. Yet if they were to share information about system vulnerabilities and successful penetrations, they fear that these would become public knowledge and adversely affect the competitiveness of their businesses. Given that it is so difficult to protect sensitive information in the era of the Freedom of Information Act—in the era of the public's right to know—these fears are not unfounded.[6]

But it is equally difficult, if not more so, to get the government to share information with the private sector. Consider, for example, just how difficult it is to get the Federal Bureau of Investigation to share the information to which it has access, even with those it trusts. Again, we can

understand the reluctance: the information is both sensitive and tied to criminal investigations. We must, however, find ways to reduce the present impediments to information-sharing among the parts of both the public and private sectors.

It is vital, in short, that we come of age in the cyber age and start thinking seriously about how to achieve a genuine public-private partnership. This may call for a complete redefinition of its meaning. It may also call for the creation of entirely new types of institutions. To deal with the cyber threat, we may need to rely on an institution that is not law enforcement, not intelligence, and not defense, but a little of each, that is not private sector nor public sector, but a little of both. Such a concept has been discussed. A group of analysts at the National War College is, in fact, investigating the possibility of developing an institution called a Triune, which would house an intersection among the private sector and federal, state, and local governments.[7] This idea is one which the President's Commission considered in 1996-1998, but rejected as too impractical. It is an indication of how much things are changed that this idea is now being taken far more seriously.[8] Four years ago we were just beginning to understand the cyber threat, and the idea of creating a triune was a pipe dream. Today, it is not. It may be that we really do need to start thinking about something unique, something, to quote Elizabeth Rindskopf-Parker, far "out of the box."

Conclusion.

Kuehl is right to stress the growth of cyber space as an environment critical to America's security. He is also right to stress that the DoD does have both a role and a responsibility, in cooperation with law enforcement and the private sector, to protect this environment. What I wish to emphasize still more, however, is the degree to which Americans need to rethink the meaning of such concepts as

"information," "threats," and "public/private" relations. Only if they do, can we hope to maintain an adequate defense of our information infrastructure in coming years.

ENDNOTES - CHAPTER 11

1. The members of the commission were asked by Clinton to look at eight critical infrastructures to determine whether or not they were vulnerable to both physical and cyber attack. They chose to concentrate on the cyber arena because the physical arena was already well documented.

2. This delay in recognition makes the problem all the more urgent because we have not adequately anticipated the problem and are therefore forced to play a game of catch-up.

3. This was one of the conclusions reached by the President's Commission.

4. As a matter of fact, we are beginning to think this way in the United States.

5. To spam is computer lingo for disrupting or clogging e-mail or computer traffic with commercial mesages.

6. As things stand at the moment, the tendency is for private companies to work against, rather than with, the public sector. This is illustrated rather strikingly by an episode which took place very recently at a meeting between this author and some of his marketing personnel at Veridian (a company which primarily contracts for the government but is starting to move into the private sector). We were discussing how best to market a new capability in the private sector. One of the marketing personnel suggested that the way to do this was to offer to protect potential commercial clients from the government! Clearly, the mistrust is huge.

7. Randy Larson, Bart O'Neal, and Ms. Andreazi. State and local governments have a huge responsibility because they regulate most of our infrastructure.

8. Jeff Smith (a former general counsel at the CIA) suggested we think about defining a new type of institution—something with a defense, law enforcement, and private sector intelligence responsibility.

CHAPTER 12

DANIEL KUEHL'S VIEW OF INFORMATION WARFARE AND THE DEFENSE OF U.S. INFORMATION SYSTEMS: ANOTHER PERSPECTIVE

Richard Marshall

Introduction.[1]

The purpose of this chapter is to comment on the chapter by Dr. Daniel Kuehl and raise some further questions concerning the role of information warfare and the defense of U.S. information systems. We are all captives of our environment, and the environment and training of this author are that of a lawyer. I am therefore going to take a lawyerly approach to this task. I shall commence by describing the problem and offering an analysis—a somewhat subjective one, to be sure. Then, I will offer some possible solutions for the readers' consideration.

Framing the Issue.

Kuehl has argued, in no uncertain terms, that the Department of Defense (DoD) does have a responsibility in this area. He is undoubtedly correct that DoD (and, for that matter, the National Security Agency [NSA], which in a somewhat schizophrenic fashion can be considered a part of DoD) has a mission to defend against all enemies, foreign and domestic. At first sight, it would appear as if the issue could be resolved with beautiful simplicity; let the Federal Bureau of Investigation (FBI) take care of cyber attacks when they are crimes, and let the DoD take care of them when they are acts of war, that is, when they are perpetrated by our enemies. Close inspection makes it clear, however, that this is less than easy to do. It is very hard to

determine who is behind a cyber attack. Action must normally be taken long before it is clear whether the attack is a crime or worse. So we must approach the question from a different standpoint. We need first answer some basic questions, specifically, (1) who can be trusted with the important business of defending our information highways, (2) who has the technological capability to do this, and (3) who has the constitutional responsibility to do this? With answers in hand, we shall conclude by arguing that the defense of cyber space is indeed important enough to involve the DoD, but that it needs to involve the business community as allies in the fight.

Preliminaries.

Before we proceed further, a couple of really basic points need to be clarified. The first relates to the fundamental seriousness of the threat, which should not be underestimated. The second relates to the nature of cyber space, which in the view of this author is often misrepresented, to ill effect.

As Kuehl indicated, the cyber threat has not loomed large on our threat horizons until fairly recently. It is unquestionably taken much more seriously now, since it has the potential to cause us serious military headaches. Let me illustrate this by drawing attention to a real life exercise that was played out in 1997.

Eligible Receiver is a periodic exercise sponsored by the Joint Chiefs of Staff (JCS). Its purpose is to test the responsiveness and effectiveness of our military forces. In 1997, for the first time ever, a cyber attack scenario was incorporated, and, again for the first time, the aggressors won. They a won in a matter of hours rather than a matter of days. So rapid was the victory that the exercise had to be halted. Afterward, the person who was acting as the JCS Chair reported to the National Security Council (NSC) that cyber warfare did indeed pose a military threat. He noted that in the scenario just played, U.S. forces in the Pacific

had found themselves facing a shooting war. They were, however, without any means of communicating with stateside headquarters except carrier pigeons and semaphore flags! These would quite clearly not be up to the task of sending messages between Washington and the Pacific! The lessons of this scenario were obvious. Indeed, the newly awakened consciousness of the seriousness of the problem led to the formation of the President's Commission on Critical Infrastructure Protection in 1996. It is a matter of crucial importance, in short, that we apply our keenest intellectual energies to this issue.

My other point relates to the popular understanding of cyber space. One of the obstacles we face in our attempt to deal rationally with questions of responsibility is our tendency to make it more abstract than it actually is. Charts depicting cyber space are generally depicted by clouds. Well, cyber space is not a bunch of clouds. Cyber space is basically the public switch network. It is a tangible, physical entity. Behind all the abstractions, fascinating though they may be, are physical things. There are switches, routers, and telecommunication hard devices. This is true even in a wireless society. When you incorporate a computer into a cellular telephone, the signals go through a public switch network. There is a choke point that can be accessed, that can be utilized to determine a number of things. The electrons go through an area which can be grabbed. Thinking of cyber space in this way will help reduce the confusion and perhaps make the business of defense of cyber space seem less remote and more manageable.

The Challenge of Cyber Warfare.

Let us revert at this point to the question of responsibility and the ambiguities we spoke of earlier. It bears some elaboration. First, let us imagine a fictional scenario. It takes place in what Kuehl would call the traditional dimensions of war. If an enemy aircraft flying somewhere in our airspace were to drop a nuclear bomb on

the White House, our initial reaction would be that the Air Force should respond to this threat. This reaction would be right, however, only if the aircraft were state-sponsored. Suppose that the aircraft was piloted by a slightly crazy member of a fringe group from within the United States, someone, for example, from Wyoming or Utah. In this case, the bombing would be better classified as a crime than as an act of war. And it would surely be the task of the FBI to deal with this threat. The point of this scenario is to elucidate a very important reality. It is extremely difficult in cyber space to determine the status of the perpetrator of an "attack."

A series of real life cyber attacks that took place in 1997 suggests more fully the extent of this problem and its many ramifications. At that time, some 3 months after the military exercise Eligible Receiver, attacks on Air Force logistics-related computers were reported at a number of installations. In and of themselves, these incidents were not terribly exciting. They seemed to be random, isolated events. Taken individually, they had all the appearance of criminal acts. However, seen in the broader strategic context, they provided indications of a more serious threat. For at the very time of these cyber attacks on government computers, U.S. forces were preparing for another Middle East test range exercise in Iraq. U.S. military forces were preparing for deployment, and a military buildup was in progress. This pointed to the possibility that it might be the enemy nation—Iraq—who was behind these attacks.

Suppose for a moment that this possibility had in fact been rapidly confirmed. This still does not make it altogether clear what the appropriate reaction should be. Ask yourself what you would you do if you were the President of the United States, or Secretary of Defense, or Chairman of the Joint Chiefs of Staff? Could one justify the launching of military forces against another nation in retaliation for the extraction of information from government computers?

The fact is, however, that it is rare indeed for any clear-cut blame to be assigned in short order. In the case in question, it took some time. Air Force computers have sensors that make it possible to detect whether any anomalous activity has taken place. This kind of activity is not detected at the time of an attack, but some hours after it occurs. The sensors point the way like Tonto for the Lone Ranger. The FBI, with the assistance of the NSA, determined that two adolescents in California were responsible for all of this activity. Everyone involved heaved a big sigh of relief. But was this premature? Were the young Americans really acting on their own? According to press reports, their mentor lived in Israel. Did he work for the Israeli government? Did he work on his own? Perhaps, after all, the attacks were state-sponsored.

There is a still more recent example. For some time now, Air Force computer systems have been afflicted by intrusions. The intrusions come in via educational sites and then go out via industrial sites. They extract unclassified data associated with advanced weapons technology. No one knows for sure who is behind these intrusions. According to press reports, they may be coming from countries in Europe. But there is no definitive way to tell whether the intrusions are sponsored by states, by non-states, or simply by a group of cyber-happy kids. If you are part of the decisionmaking authority in the United States, how do you react to a threat of such uncertain origin? Do you go to the State Department and have it issue a strongly-worded statement calling on the perpetrators to stop their illegal activities? Do you launch your Air Force bombers? Or your submarine-borne ballistic missiles? Whom do you call upon to help you deal with the threat? Do you call in the FBI? All of the above suggestions have been considered. But framing the appropriate reaction to an event is very difficult indeed.

Analysis: Who Should Defend Our Critical Infrastructures?

Dividing responsibility for the defense of cyberspace between law enforcement agents and the military, based on an evaluation of whether an act is a crime or an act of war, does not appear to be very practical. Rather than do this, we should approach the whole question from a different angle, simply asking ourselves who should be entrusted with the task of defending something so essential to our national well-being, and why. We will also extend our consideration to include the private sector. The reader is now invited to ask himself or herself, some fundamental questions.

• Whom ***do*** Americans trust? First of all, we must consider who it is that can be trusted to protect this vital resource. A brief survey was taken at the time of the conference presentation on which the present chapter is based. Members of the audience were asked whether they would permit NSA to examine their home computer and see what kind of programs they were using and with whom they were communicating. The same question was asked concerning the Central Intelligence Agency (CIA) and the FBI. Only a handful (some five or six people out of about 100 people) indicated that they would. When asked how many would permit Microsoft to come in and take a look at their computer system, rather more indicated that they would. Far more have given their tacit consent simply by owning computers and running Microsoft products like a Windows 95 or 98 or Microsoft Office 2000 product. In so doing, these people have in effect given Bill Gates permission to come in and see what type of programs they are using. The point is that someone *is* looking into our computers. Americans do not seem to mind if this someone is American business.

The question might be framed in a different way. Suppose we were to poll Americans to see if they would permit NSA or CIA or FBI to come into their computers and modify the functionality of their programs? The evidence suggests that most of them would be adamantly opposed to

such a notion. Yet, these same individuals permit AOL and other Internet service providers to do that very thing. Merely by using an Internet service provider to connect to the Internet, they have allowed these companies to come in and modify the functionality of their computer.[2]

• Whom ***should*** they trust? Americans trust business to do intrusive things even though they do not trust the federal government. Is this logical? Perhaps. It is certainly surprising in some ways. In the first place, American business is uncontrolled. The federal government is subject to federal law and the Fourth Amendment. In the second place, our trust is in large measure based on the (false) assumption that the businesses in question are American businesses. In fact, we are living in the age of international business, and much of the software that Microsoft and other companies sell is written outside of the United States. Why? Because it is much cheaper. It might surprise you to find out where a lot of the software is written—India, Pakistan, Israel, Russia, and China, for example. We should ask ourselves whether or not we should, under these circumstances, feel warm and trusting.

• Who is best equipped to defend us against cyber threats? Both government and the private sector have technological capabilities which they do not always share with one another. The private sector tends to be somewhat advantaged in that it is not quite as constrained as the government when it comes to invading privacy for the purposes of defense.

• Who bears the constitutional responsibility to defend us against cyber threats? What is the proper role of the government in dealing with these threats? Can DoD defend us against crime and still keep within its constitutional bounds? Do we let the military defend our cyber space, even if those they are defending it from are criminals rather than enemies of the state? One could argue that there is a historical analogy for this. The early modern period witnessed a commercial revolution in Great Britain.

Britain's budding prosperity was threatened by pirates and other miscreants who preyed upon British shipping. This led the commercial sector to ask for intervention by the government and to the foundation of the Royal Navy. Have we now reached a similar moment? Should we call upon the DoD to protect our information highways?

At the same time, the legal authority of anyone in the government to take appropriate action against threats to our critical information infrastructure is limited. With regard to NSA, Executive Order 12333 says that it is to provide signals intelligence and national security for the U.S. Government. That gives NSA the authority to deal with threats to federal systems but not with threats to the private sector. Another document, National Security Directive 42, refines the role of NSA to that of protecting national security systems. That affords some legal sanction for guarding DoD telecommunications systems. That is some small comfort. But even in this case, NSA is limited by the Electronic Systems Privacy Act, the Computer Fraud and Abuse Act, and also the Fourth Amendment. There is, in effect, rather little that NSA can do to help protect national systems.

One of the documents that came out of the President's Commission is Presidential Decision Directive (PDD)-63. It reached some interesting conclusions. It recognized that a threat to our information systems does indeed exist. It recommended that various areas in the government work individually and together to try to resolve it. A basic point to remember is that no one is in charge. No single authority has undivided responsibility to ensure that the systems are protected. A variety of groups such as National Institutes for Standards and Technology and the Office of Management and Budget is involved. They have a role to play and do have some responsibilities. But none of them has the authority or the technical capability to reach out and work with the private sector. And it is the private sector which is most vulnerable. A joint task force for civil support

was established, but this too was just a pathway to a fix, not a fix in itself.

Solutions.

Thus far, this chapter has sounded a note of almost unmitigated gloom. Some suggested solutions were promised, however. Let's consider a few ideas that might point the way to solutions.

In my opinion, the defense of U.S. information systems must, in the final analysis, rely in large part on private industry and businesses. I will attempt to explain the logic behind the conclusion.

In January 2000, I traveled to a conference attended by a group of professionals who, broadly speaking, were interested in communications and information security. The conference was also attended by Internet service providers, computer developers, and software manufacturers. Significantly, their main concern was to find ways to develop Internet security. In the past, what had guaranteed a good profit margin was to sell telecommunication and computer systems that worked. Now, Internet security was the dominating concern. All at the conference recognized that if e-commerce is to work, ordinary Americans have to have confidence that their communications are safe and secure from hackers, and hopefully from state-sponsored terrorist activity as well.[3] Recent events had contributed to the awareness of the conference participants. When, for example, a major bank was hit by hackers in January 2000, it lost money, and the American public promptly fled in large numbers to that bank's competitors.[4] The bank lost over 3,000 accounts in a 24-hour period. It is in the enlightened self-interest of businesses to improve their security. What is more, they know this.

This leaves room for some optimism. In the final analysis, for all the mutual suspicions, government and

private industry are all in the same boat together. Both face a considerable threat, and both stand to gain by increased cooperation.

The government is, as we have seen, handicapped in ways that business is not; the Fourth Amendment and Federal regulations, while serving a vital purpose, do put obstacles in the way of government's ability to handle threats to the private sector. The private sector would itself stand to gain if it could work more closely with the government. The government has some experience in identifying adverse activity coming into its communications systems. The Army, Air Force, and Navy, to a degree, have all had some success using the computer sensors we spoke of earlier in this chapter. The key to national security (the concern of government) and prosperity (the concern of business) hinges on the development of an adequate defense of U.S. information systems. It is, as we have stressed, extraordinarily difficult to take effective action against an attack once it has taken place. So prevention becomes of paramount importance. This is where we should devote our intellectual energies and our capital. And that is why it is necessary to build a strong defense system, in large part managed and funded by the private sector.

Conclusion.

There are no easy solutions to complex problems, but Kuehl is absolutely correct to stress the seriousness of the threat of information warfare. He is also surely correct in arguing that the DoD has both a role and responsibility in defending the United States from threats, intrusions, and attacks mounted via this environment. To this end, we must avoid the danger of functional paralysis. This comes in a number of flavors. When Spike Bowman from the FBI talks about its role in dealing with transnational threats, he is very FBI-centered. That is the result of his training. When Dan Roper from the DoD makes a presentation on the problem, he offers the DoD as a solution, again an

outgrowth of his training. These are all helpful perspectives, but alone they do not resolve the issue. It is necessary to realize our roles and missions, but it is also important to realize and accept that there is another way of doing business. And that is going to require a tremendous amount of cooperation. That must include not only cooperation among the government branches, which is something that has been much discussed, but it must also include cooperation with the private sector. Together, and surely only together, government and the private sector can find a common solution to a difficult threat.

ENDNOTES - CHAPTER 12

1. The views expressed in this chapter are strictly the author's and do not reflect the official position of NSA. At the same time, my comments and observations have been shaped by my environment, including my current position at NSA. The basic charter of Executive Order 12333 says that NSA provides signals intelligence and communications security for the U.S. Government. There are basically two teams at NSA—the offense and the defense. I work on the defensive side. My views have been enriched by Lieutenant General Kenneth A. Minihan, my former boss as the Director of the National Security Agency, and by a professional colleague, Elizabeth Rindskopf-Parker, based on discussions over the last several years. I also wish to acknowledge a debt of gratitude to Jeffrey Hunker, who is senior director for critical infrastructure for the National Security Council and who worked with me on the President's Commission; to my colleague Phil Williams; and to a an acquaintance made at the conference, Alex Roland.

2. As mentioned earlier, cyber space has a very physical face, and this physical face can be controlled and exploited. Who is in control of the public switch network? Is it the government or is it private entities? Is it the telephone communication companies, AT&T, Ma Bell, Bell Atlantic, etc? Is it the Internet service providers? AOL? Do they have a responsibility for detecting and reporting criminal activity? Do they have a role and responsibility in detecting activity that could be harmful to our national infrastructure?

3. It would be possible in today's environment for an enemy nation-state to jeopardize the U.S. economy by attacking Wall Street.

4. In order to avoid precisely the kind of loss of confidence of which we have been speaking, we will not mention this bank by name.

CHAPTER 13

COMBATING TRANSNATIONAL ORGANIZED CRIME

Phil Williams

Introduction.

U.S. security is currently threatened by a variety of transnational threats. Of these, one of the most menacing is international organized crime and drug trafficking. This chapter will define and evaluate the nature of the threat, identify some important trends in transnational organized crime, and then consider how these threats should be met. Three levels of response will be considered: multilateral responses, the law enforcement response, and the military response. The chapter will conclude with some recommendations.

Assumptions and Concepts.

This chapter rests on several assumptions, which should be clarified from the start. First, not all security threats are military in nature. Second, not all security threats require a military response. And third, threats depend on vulnerabilities.[1] This last is a particularly key point to make in a discussion of this sort. Vulnerabilities to organized crime, as we will see, vary enormously from one state to another. This having been said, let us turn to a discussion of some of the basic concepts which need to be grasped if we are to understand the threat posed by international organized crime.

First of all, what is organized crime? No one definition exists, with academics differing considerably over its meaning. I follow a Clausewitzian paradigm, defining organized crime as a continuation of business by criminal

means. Given the name "organized crime," one might expect a high level of organization to be a defining feature. Though some analysts say that organized crime is really disorganized, I disagree. Organized crime is network-based, and networks may sometimes have a somewhat chaotic appearance but are in fact a very sophisticated organizational form. Setting aside organization per se, however, I would contend that organized crime is marked by three distinctive traits: association for criminal purposes, corruption, and violence.

When we say that organized crime involves association for criminal purposes, we are not implying that the organization must be large. The crime unit can be very small, but the minimum number of persons involved is three or more persons.[2] Organized crime, moreover, makes systematic use of corruption. This is of paramount importance, but has not always been sufficiently emphasized in the literature on the subject. Organized crime also makes occasional use of violence. Russian contract killings, to suggest the scope of the problem, number about 500-600 a year. This figure is high enough to warrant the claim that organized crime challenges the state's claim to a monopoly on the use of organized violence.[3]

The focus of this chapter is not on organized crime in general, but rather on international organized crime. Organized crime has moved a long way from its roots as a local problem threatening domestic law and order. Today it has a "transnational" dimension, involving criminal business enterprises on a global scale. If we compare Al Capone and company with the drug scene in Colombia, the point becomes clear. Whereas Al Capone was a small-time hood with a local fiefdom in Chicago, the drug trafficking organization based in Cali, Colombia, was for a long time the developing world's most successful transnational "corporation."[4] It developed a global marketing strategy and even at one point had application forms.[5] The decapitation, first, of the Medellin organization and then the Cali, forced

the Colombian drug business to adapt itself to changed circumstances.

Now, if anything, it is even more menacing. Colombian-based criminal groups are more numerous (there are about 200 of them) and smaller (but still effective) than before. These groups have shown themselves to be adroit at answering challenges to their business. They have started to grow coca leaves themselves to reduce their dependency on imports from Peru and Boliva. They have diversified their products, now distributing heroin as well as cocaine. They send their products to market using a wide variety of routes and employing a wide variety of ethnic groups. They continue to use Mexicans, although of late they have come to rely more on Caribbeans, especially Dominicans, who demand only 25 to 30 percent of the profit (in contrast to the Mexicans, who want 50 percent). The employment of Sicilians and Russians, in particular, has added to the global dimension.

In what way is organized crime transnational? Or rather, to phrase it differently, who or what crosses borders? First of all, there are those who perpetrate crimes, as for example the hit man who flies from Moscow to New York to do a contract killing and then flies back. Second, there are profits. Today's global financial system is a money launderer's dream. Access to financial systems is easy, the movement of money is instantaneous, trading can be performed anonymously, and, best of all, profits can be placed in safe havens.[6] Many of these are offshore. The offshore financial systems of the Pacific islands offer some interesting insights to what is going on. Their web sites are bilingual—English and Russian. Clearly, they are trying to get a share of dirty money from Russia or capital being processed via the Bank of New York.

Third, people as commodities cross borders. In some instances, they are illegal immigrants, as for example the Chinese who were smuggled into the United States on rusty freighters.[7] A lively traffic also exists in women and children

who are being sold for commercial sex. Products are also moved across borders. Goods range from drugs, arms, and nuclear materials, to stolen arts and antiquities. Most goods flow from south to north, in other words from the developing world to the developed world. The automobile moves from north to south. Arms move in both directions. So, while we worry about drugs coming north to us across the border with Mexico, the Mexicans worry about guns going south towards them from the United States. Finally, one may note the fact that digital signals also cross borders in all directions.

What accounts for this transformation of criminal organizations to international criminal organizations? In part it is a response to the pressures and opportunities of globalization. It is the dark side of the modern trend towards interdependence. All businesses have benefited to a degree by globalization, and criminal businesses have benefited more than most. They have benefited from the internationalization of trade, finance, and communication, and also from the spread and proliferation of ethnic networks. The last is a point of particular importance because organized crime tends, for a variety of reasons, to flourish within the immigrant communities or diaspora.[89] A fascinating example of criminal cosmopolitanism is to be found in a small criminal group once operating out of Rio de Janiero; it was run by a Russian, the gang members themselves were a mix of Nigerians and Ghanians, and the group was trafficking drugs to the United States and western Europe.

Criminal-friendly asymmetries also encourage much of this transnational activity. Criminals cross borders to take advantage of the legal, administrative, or market opportunities afforded by the different countries. Criminals, for example, migrate to countries with criminal justice systems which pose little risk to them. They exploit administrative asymmetries. When taxes are increased on cigarettes in Canada, for example, smuggling across the Canadian border increases. Criminals engaged in financial

fraud seek out the profitable markets. South Africa, for example, has become an important host state for many criminal groups because it is the richest state in the southern part of Africa. The Nigerians now control the drug trade in general as well as the cocaine trade in Johannesburg in particular. Over the last 5 years, the Nigerians truly transformed the South African drug scene. Five years ago, marijuana and mandrax were the drugs of choice. Today it is cocaine and, to some extent, heroin.[10]

Transnational organized crime also flourishes because it brings economic benefits. This is a disturbing notion, but one that must be acknowledged if we are ever to get a handle on the problem. Organized crime is a supplier and multiplier of jobs and other trickle-down benefits. Profits from organized crime are, to some extent, put back into the local economies. It is impossible to understand why so many peasants have become heavily involved in the drug trade in South America if we do not recognize this. Cocaine is a more profitable product than anything else they can grow; if they do not make much from it, they still make more than they would growing the crop substitutes that have been proposed. Moreover, black markets often spring into existence because legal markets do not work effectively.

Finally, it is worth noting that, common opinion to the contrary, organized crime is *not* a direct threat to the global financial system. Though it does do indirect damage by challenging its legitimacy, it is much too dependent on the system to do anything directly to destroy it. The recent scandal involving the Bank of New York elucidates the love-hate relationship that exists between organized crime and the global financial system. The Bank of New York developed relations with a large number of Russian banks. Despite the American CEO's disclaimer, it is clear that the two were engaged in what can figuratively be described as consensual sex in which the Bank of New York was a vigorous partner indeed. The Bank of New York ignored evidence that over 40 percent of Russian banks were

controlled by organized crime.[12] Organized crime and financial institutions, in short, make good bedfellows.

The Nature of the Threat.

International organized crime today poses a mixture of traditional and new threats. Both a Cold War and a post-Cold War paradigm are at work. This increases the complexity of the environment. World politics, as so astutely forecast by James Rosenau, will in the future involve two worlds: the state-centric world, which is the traditional diplomatic world; and the multi-centric world, where there is a multiplicity of non-state actors.[13] The former is a world that we are all used to and within which we have developed some competence. States are very good at dealing with threats from other states. Institutions such as the State Department and the Department of Defense have been created in order to deal with this kind of state threat. The other world is a new phenomenon. It is not clear whether this world presents us with a greater or lesser challenge than the state-centric world.[14] But it is clear that the interplay of the state-centric and multi-centric worlds will shape our ability to respond to threats in both worlds.

Any evaluation of the threat must also take into consideration that threats to us vary, depending upon our vulnerabilities. The threat from transnational organized crime constitutes a direct security threat to vulnerable states, but only an indirect threat to less vulnerable states. Transnational crime does not for the most part *directly* threaten the United States; an exception might be the smuggling of nuclear materials from the former Soviet Union by criminal organizations.

At the same time, it should be recognized that the threat is multi-level. It may be a threat to good governance, to institutions, and to individuals. As such, international organized crime is not just a traditional national security threat. There are three aspects of organized crime that can impinge on the security of states. First, illegal markets,

while impacting largely on individual security, can (as in the trafficking of arms) directly affect national security. Second, the concentration of illegal power can undermine the democratic process and democratic governments. Third, organized crime processes can undermine the rule of law. This is tragically visible in Russia where "cleptocracy" and "mafiocracy" have prevailed, effectively undermining the hoped-for transition to democracy. This important reality explains why corruption must be seen as one of the defining features of international organized crime. Organized crime-related corruption is the HIV of the modern state because it breaks down the defense of the body politic. Corruption is not just a condition, moreover. It is an instrument of transnational organized crime.[15] Organized crime uses corruption for a variety of purposes, and it essentially aims to neutralize and, in some cases, capture the state.

Criminal Organizations and States.

States, as we have already indicated, offer criminal organizations different kinds and degrees of opportunities, depending upon how vulnerable they are. Organized crime thrives best where the state is weak and corrupt. Criminal organizations use such states as home states. States in transition are often especially vulnerable; examples here include Russia, South Africa, and Cambodia. Criminal organizations do their best to perpetuate corruption in such states, because it is this which makes them effective safe havens. Host states, from the perspective of criminal organizations, are states where the good markets are. Willie Sutton, the famous bank robber, was once asked why he robbed banks. He said, "That's where the money is." That is why many organized crime groups use states like the United States or South Africa as host states. These are the states where they can make enormous profits. Transshipment states neighbor home states and are affected by incidental corruption along the way. In Latin America, for example, drug trafficking corruption starts in

home states like Peru, Bolivia, and Colombia, but extends to transshipment states like Venezuela, Argentina, and Brazil. Finally, there are also what might be called service states which serve as financial havens.

Attitudes of States.

Attitudes of states toward organized crime differ widely. Some do their best to control crime. At the other end of the spectrum, some states are actually controlled by crime. Nigeria, under its military dictatorship, offers us a good example of this kind of state.[16] States do not necessarily remain constant in their attitude towards crime, either. Colombia, for a long time, certainly acquiesced in and perhaps even accepted organized crime, but under U.S. pressure it has adopted a confrontational attitude.

States in transition show a tendency to acquiesce in the activities of criminal organizations. There are several reasons for this. First, if we look at such states as the former Soviet Union, we find that prior to the collapse of central authority and control, organized crime did exist but in circumscribed and controlled form. When the controls were suddenly removed, crime proliferated enormously. Second, states in transition often suffer from massive economic dislocation. This causes people to migrate from the legal economy to the illegal economy. Third, social norms break down in states in transition. This open up the local society to foreign values; in Kurdistan, for example, U.S. 1950s movie-style gangsters live again.

Openness to the world is also a result of what can be called capacity gaps and functional holes. Basically, states in transition—that is, weak states—do not perform all the acts of governance that we associate with states. Organized crime can do two things—it can exploit the hole, or it can fill the hole. For example, in Russia, there has been very little government. Borders are no longer as carefully monitored as they used to be, so that organized crime exploits the hole and crosses them. Because the government

has not done much by way of legal arbitration of business disputes or of debt collection, organized crime fills the hole and takes on those tasks.

Corruption plays a critical role in all of this. Corruption is used to neutralize the state or even capture it. This has happened, at least arguably, in Mexico, Russia, Turkey, and South Africa. In contested states, the results are still being decided. In criminal states, the issue has been decided—on the side of crime.

Trends in Transnational Organized Crime.

Several trends should be noted in transnational organized crime:

• It is becoming more widespread, more prevalent, and more diverse. Fifteen or twenty years ago, organized crime was largely restricted to the Italian community. The Federal Bureau of Investigation (FBI) was able to deal with crime by focusing on this ethnic group. This is no longer true. We are now dealing with what might be called "the new ethnic mobs."

• Organized crime is increasingly gaining control over property and, partly as a result of this, has much greater economic influence than in the past.[17]

• Organized crime is becoming increasingly sophisticated and using increasingly sophisticated weapons. A few years ago, in a classic conflict between criminal organizations, the Hells Angels and Texas Bandidos, in Norway and Denmark, used antitank weapons and grenade launchers against each other.

• Crime groups are trafficking in an increasing variety of goods. The Global Survival Network in Washington, for example, discovered that the same group that was trafficking in Siberian tigers was trafficking in women. Similarly, the groups involved in antiquities trafficking are now involved in the trafficking of nuclear materials.

• Cooperation among criminal organizations is growing, with such growth taking many shapes. While there is no clear connection to terrorists, we are seeing some blurring of boundaries between criminals and terrorists, especially in countries such as Colombia, Kurdistan, Tajikistan. It is often difficult to tell who is who. Sometimes a terrorist who once had a political cause becomes a criminal because that cause has been taken away.

• Criminal organizations are becoming increasingly adroit at the exploitation of information technologies. They use it in much the same way as do other firms, notably to increase their managerial efficiency.

• Criminal organizations have largely abandoned their traditional hierarchical organization and instead are increasingly coming to rely on highly flexible networks and loose coupling. This gives them the advantage of being able to cross boundaries and borders with ease, and cross from the illegal sector to the legal world. It also means that when part of their network is destroyed, criminal organizations will continue to be able to function. The networks make them resilient and the battle space complex.

Responses.

Responses come in various forms: multilateral responses, law enforcement responses, and military responses.

Multilateral Responses. The response to international organized crime comes from many quarters. On the one hand, the international community has taken some actions, though of varying degrees of effectiveness. Conventions are useful inasmuch as they do set norms. The United Nations (U.N.), most notably, held a World Ministerial Conference in 1994, and this year will adopt a convention agreement on transnational organized crime. A financial action task force (FATF) was also established. It is, in essence, a peer review body which checks out its members and encourages others

to join. The objective is to stop such criminal activities as money laundering. For example, the Federal Emergency Management Agency (FEMA) reports transactions over $10,000 and writes reports on suspicious activity. FATF is not very effective, however; participation is time-consuming and requires a lot of work while not accomplishing much. On the other hand, there are some relatively effective regional initiatives. Bilateral-multilateral task forces, such as Europol, have met with some success; the task force approach in general seems to be one that works, at least part of the time.

Multilateral responses, however, have inherent shortcomings. This is especially true when it comes to efforts to regulate international behavior. Some members lack commitment; some even defect. Others simply lack the capacity to implement convention agreements. Moreover, measures tend to become diluted when enacted in a multilateral forum. For example, efforts have been made to create a global money-laundering regime. First there are regulated states. These include the United States and the European countries (which continue, despite regulation, to be the biggest money launderers). Then there are the offshore banks. These are regulated to some degree. And then there is the rest of the world. Here very few regulations apply.

Cooperation between nations is also not very easy to achieve. Some progress has been made on extradition treaties, which make it possible to catch fugitives, and mutual assistance treaties, which make possible the collection of evidence. But problems remain. The fact that different legal traditions prevail in different parts of the world is a perpetual stumbling block. How, for example, does a country know that its partner is reliable? U.S. law enforcement, at the federal level, hesitates to work with Mexicans because they know the information is almost inevitably going to be passed on immediately to criminals. From the Mexican perspective, they have reason to be wary of the United States, which is capable of acting in

heavy-handed fashion. Customs, for example, put together a very good sting operation, called Casablanca. It was, however, a unilateral action, which was sufficiently aggravating to the Mexicans to oblige Secretary of State Albright to offer them an apology.

Law Enforcement Response. Law enforcement agencies across the world have a mixed record. They have engaged in some productive efforts, with the FBI, for example, having met with considerable success, notably in dealing with La Cosa Nostra. The kingpin strategy of the Drug Enforcement Agency (DEA) and the Italian use of Pantiti (defectors who agree to cooperate in return for leniency) have also proved to be effective. But the law enforcement response has some real limitations.

First, it focuses its efforts at a low level. Most of the law enforcement communities fail to target the real source of the problem: profits, organizational integrity, and leadership. Instead they try to seize products, picks up low level personnel, and recover some money. The FBI and the DEA are, perhaps, exceptions to this rule. Second, law enforcement ultimately has no choice but to be preoccupied with cases. This makes it, for the most part, reactive. One consequence of this is that it has failed to develop a comprehensive strategy for combating organized crime. Third, the efforts made by law enforcement are fragmented. There are Federal, regional, state, and local agencies, which do not always cooperate. The problem is compounded by interagency rivalries, which afflict law enforcement much as they afflict the military. Recent efforts to achieve jointness have been only moderately successful. Finally, one of the most serious difficulties comes from the fact that criminals operate in a borderless world. Law enforcement is bordered. Criminals have learned to use borders defensively. This has proven to be a major obstacle to the effective containment of the threat.

Military Response. The military does have a useful role to play in dealing with international organized crime. It has

played a constructive part in the interdiction of drugs and other criminal products. It has made useful contributions in the area of intelligence. It provided a model, which has modified the way law enforcement understands intelligence. Thanks to the military, we now have the National Drug Intelligence Center, focused on strategic intelligence. And even though law enforcement does not always understand how to make use of that intelligence, it is clearly a step in the right direction.[18] The military also provides short-term surge capability in regard to cargo inspections.

The U.S. military has become involved in combating criminal organizations during the course of peacekeeping operations. In places where there are black markets, often the only powers at hand are criminal figures. The situation can be confusing, with no obvious "good guys" and "bad guys." Different factions work together at times and kill one another at times; sometimes they work together in order to get the money to kill one another! The military has had to navigate through these tricky waters, gaining some useful experience dealing with criminal organizations in so doing.

Yet, there are some serious limits to the usefulness of the military in dealing with this particular transnational threat. First of all, when we deal with organized crime, we are dealing with a continuation of business by criminal means. We are, in effect, dealing with business markets. The military provides a very blunt instrument where refined tools are needed. Second, we are dealing with organizations that have safe havens. Where the criminals go, the military cannot always follow.

When considering the appropriate role of the military, we must also remember that the threat differs from country to country. For the United States, the organized crime problem is essentially a law-and-order problem. For states in transition, the problem is much more serious. Should *their* militaries become involved? What of Russia, for example, where you have an iron triangle of politicians,

businessmen, and criminals, and where the military itself has been corroded by the environment?

Again, does the U.S. military have a role to play in assisting these other countries deal with the problem? Only to a limited degree. There are limits to U.S. power and influence. Intervention in weak states does not seem to be a good idea; the lessons of Vietnam should remind us of this. There is a further problem. When the United States intervenes in a weak state, it undermines the authority and legitimacy of that state. And yet it is that very lack of authority and legitimacy that has made the weak state vulnerable to organized crime in the first place. Colombia is a case in point. One thing we can do is to be more careful where we give our aid and encourage the international institutions to be the same. In short, the multilateral response is flawed, the law enforcement response is fragmented, and the military response has limited applicability.

Developing a Comprehensive Strategy.

A comprehensive strategy needs to be developed. The United States is attempting to do this, although more needs to be done. What does this entail? First, we must do what we can to build viable states so that criminals no longer find it so easy to shelter in weak states. This will increase the risks for criminals and distribute the problems more evenly. The United States has taken steps to do this, and, interestingly, its legislation has inspired similar legislation in South Africa.

Second, we must recognize that international organized crime is a national security threat. This will serve several purposes. It will ensure that more resources will be devoted to the task of combating this threat. It will encourage intelligence agencies to become more fully involved. And it will encourage the adoption of military concepts. Military concepts and strategic approaches are often very functional. The military stresses, for one thing, the importance of

defining objectives, which is something that could usefully be emulated by law enforcement. Target hardening is another concept that might usefully be applied to the civilian sector.[19] The military model for jointness could be used to help foster interagency cooperation.

Third, we need to build international law enforcement networks. It takes a network to defeat a network; this is why the Hungary training academy is so important. To defeat international organized crime, it is important, as has been stressed earlier, to attack what really matters to the criminals—their networks, their leaders, and their wealth. This is done, first, by identifying the critical node of a criminal organization, followed by attacking this node and its connections. Then the crossover figures, the legal protectors, must be removed. Criminal markets must be targeted. The risks for criminals must be increased, and their profits reduced. The demand must be decreased, and the supply cut off. Sanctuaries for both criminals and criminal proceeds must be eliminated.[20] Efforts must also be made to undermine the structures which support criminal organizations. These include the criminal nexus with politicians and business. Finally, the environment should be modified. For example, Russia's perverse tax system plays into the hands of members of organized crime. It provides incentives for people to avoid paying taxes, and, since the criminals have access to banking records, they have the means to blackmail a large percentage of the Russian population. This makes it hard for anyone to move against them.

Conclusion.

Organized crime, defined as a continuation of business by criminal means, has recently attained a transnational dimension. This transnational extension is a response to the pressures and opportunities of globalization. It has resulted in a type of criminal organization that is highly adaptable and very slippery to deal with. While clearly harmful in

many ways, organized crime does benefit some, a fact which makes it all the harder to uproot. Responses to the threat have come from many quarters; none has proved to be fully effective. The threat is certainly serious enough to warrant a concerted effort on the part of the United States (and other nations) to develop and implement a comprehensive strategy to counter the threat. This strategy should target the values that truly matter to the criminals. And it should learn from the experience of both the military and the law enforcement communities.

ENDNOTES - CHAPTER 13

1. Lawrence Friedman made this point about strategic nuclear power.

2. Two's company; three's an organized crime syndicate.

3. The Ridgway Center at the University of Pittsburgh has a database on Russian contract killings, which number about 500-600 a year. It is an interesting list because it enables one see what sector Russian organized crime is influencing. For example, in 1993-94, there were numerous contract killings in the banking sector. It was clear that Russian organized crime was becoming entrenched in the Russian banking system. In 1995-96, there were numerous killings in the aluminum industry surrounding Lev Churney and the Churney brothers, who were linked to some important people in Moscow. It has been suggested that Churney was involved in laundering money through the Bank of New York, along with a long line of other people. He was involved in various forms of corruption and also resorted to violence occasionally. In a 6-month period, close to ten people associated in some fashion with the aluminum industry were killed. It was not clear why. In some cases, the killings appear to have been linked to a desire to cover tracks.

4. Though often referred to as a cartel, it never really was one.

5. One interesting dimension of these application forms was that the applicant was asked to include next-of-kin so that there was someone to exact retribution against in the event that he stepped out of line.

6. For example, there are walk-in accounts where you can put money in one jurisdiction and then move it on immediately to another. These have bank secrecy restrictions such that if the FBI or some other law

enforcement agency asks for and receives information, the bank employee who supplies the information is in some cases then subject to criminal prosecution in that jurisdiction.

7. In fact, about 90 percent of the illegal Chinese immigrants come in by air and only about ten percent by sea.

8. Nicholas Passus, at Temple University, developed this theory. Transnational organized crime is deeply imbedded in ethnic networks. This is not to say that all immigrants are criminals. More often than not, they are the victims rather than perpetrators of crime.

9. As additional examples, the turn to the growing of coca some 15 or 20 years ago, and the turn to opium in Southeast Asia, were both market-driven.

10. It seems to this author that the Bank of New York did have actionable intelligence. Even if it did not know specifically which banks were controlled by the mobs, it certainly could have shown at least as much diligence as it showed in checking up on its partners, which it did not.

11. He wrote a book in 1989 called *Turbulence in World Politics*. This was written before the collapse of the Soviet Union and the end of the Cold War. It was one of the few academic studies that predicted the end of the Cold War and had a clear sense of the way in which world politics would change.

12. The problem is that many states defect. Defection is one of the decisive factors shaping international relations, and, increasingly in the future, bilateral relations. We do not have to expect the clash of civilizations so much as a clash between those states that are essentially law-abiding and those states that represent criminal interests.

13. Headly Bull once raised the questions in relation to nuclear deterrence, "Who is trying to deter whom, from what actions, by what means?" An analogous question can be asked regarding corruption: "Who is trying to corrupt whom, for what purposes, using what means?"

14. David Kaplan published a wonderful story in *U.S. News and World Report*, calling North Korea a wise-guy state representing not a case of organized crime taking over the state, but of the state taking over organized crime.

15. David Kaplan did another wonderful piece, again in *U.S. News and World Report*, on the Yakuza's role in the financial crisis in Japan.

16. The center has several problems, one of which is its eccentric location in Johnstown, Pennsylvania, dictated by pork barrel politics.

17. For example, major oil companies have coordination units that work with law enforcement to try to keep mischievous intruders out of their industry. Some of their employees have been sent as students to the Ridgway Center.

18. At the moment, the off-shore world is a major sanctuary which we are currently attempting to eliminate.

CHAPTER 14

PHIL WILLIAMS' VIEW OF CRIMINAL ORGANIZATIONS AND DRUG TRAFFICKING: ANOTHER PERSPECTIVE

Thomas V. Fuentes

Dr. Phil Williams' chapter provides a comprehensive and valuable assessment of the threat posed by international organized crime and drug trafficking and an interesting discussion of the measures taken to deal with it. The purpose of this brief chapter is to respond to Williams' views from the perspective of the Federal Bureau of Investigation (FBI). I am writing from my experience running the FBI office concerned with organized crime. This office deals with all international organized crime cases except those concerned with specific Mexican/South American drug cartels.[1] Besides monitoring crime developments around the world, this office also runs investigations worldwide.[2] For the most part, my disagreement with Williams is minor, centering upon his contention that the FBI is not doing all that it can do to combat organized crime.

Points of Agreement.

Williams' analysis of how criminal organizations operate is, in general, borne out by this author's own experience. Several points deserve to be emphasized. It is indeed true that organized crime can bring "benefits." An interesting example of this can be found in the United States, where we may point to the marriage of organized crime and the federal government during World War II. The American La Cosa Nostra and Lucky Luciano struck a bargain with the U.S. Navy, agreeing to use their

organizations to protect the docks, particularly on the eastern seaboard, from Nazi sabotage.

Also key is Williams' observation that organized crime is not a threat to the United States in the same way that, say, terrorists are. Criminals are not, in fact, interested in attacking us or defeating us for political purposes or through some kind of ideological imperative. They do not want to take us over. As a matter of fact, it is in their best interest not to do us too much damage. If you imagine the United States as a blood donor, and organized crime as a leech, you will understand the point. It is not in the best interest of the leech to kill the donor. International criminals want to bring their money to the United States. They want to bring their operations here or at least take advantage of our protective measures. They want to operate within our structures and within our economy.

The famous movie, *The Godfather*, is revealing in this regard. It portrays how criminal groups started in the Italian community and then expanded. They gradually took over key labor organizations and the related industries—from trucking to longshoremen and hotel workers. The actual La Cosa Nostra operated, in fact, very much in this way, particularly in New York and some of our major northeastern cities. This is the sort of agenda on the minds of criminal organizations. We should not minimize the problems created for us by organized crime, but we should also keep the threat in perspective. In the final analysis, these groups are anxious to continuing feeding at the golden trough, and this offers us some safeguards.

Williams is also right to stress that organized criminal groups are becoming globalized. The traditional American crime organizations are, to be sure, a bit of an exception in this regard. They are well entrenched, satisfied with their situation, and reluctant to change. The Italian mobs are structured on the model of the Roman army and not, as yet, much interested in networking. They have become involved

in technology and off-shore organizations only to a limited extent.

Nonetheless, globalization is indeed a trend to be noted. It is certainly very true of Eurasian-Russian organizations. These do indeed rely on networking and have become very international. They now operate on every inhabited continent, even on the South Sea Islands! Russian crime groups have infiltrated the countries of Eastern Europe, turning Budapest, Hungary, for example, into a kind of a Moscow south. Also bothersome, given the volatile nature of the Middle East, is that 18 percent of emigrés to Israel come from the former Soviet Union. Probably seven of the top nine crime bosses in Russia have dual citizenship in Israel. "Specter," that sinister group of global criminals of James Bond fame does have some real world equivalents. They are becoming dominant on a number of continents and are taking advantage of what Dr. Williams called the "vulnerable" states.

Transnational organized crime groups, notably those from the former Soviet Union, are also invading our turf. They are interested in exploiting our bank and investment system in order to more freely access the global financial network—something they find difficult to do from Moscow. Williams quite correctly highlighted that the criminal organizations to emerge in Russia today are groups that had already learned to operate successfully under the communist regime. They are used to operating a surrogate economy, regardless of official boundaries. Though there are no indications that they want to take over either the United States or any other Western country, there is also no question that under certain circumstances they do pose a serious threat to national security. It is, for example, a matter of considerable concern that organized crime groups are able to compromise a country like Russia, which has, among other dangerous assets, a nuclear capability.

Points of Disagreement.

In most regards, I find myself in cordial agreement with Williams. There are, however, a couple of exceptions. One of these concerns the Bank of New York (BONY) scandal.[3] The Bank of New York has been sharply criticized for developing banking relations with a large number of Russian banks in spite of the fact that over 40 percent of the Russian banking system was known to be controlled by organized crime.

It is not clear to me, however, that what happened was quite as nefarious or damaging as has been suggested. In the first place, we are not necessarily looking at an effort on the part of the Russians to use BONY for money laundering purposes. For this to be true, it has to be shown that the money sent to New York was gained illegally in Russia. This has not been proven.[4] Second, Russia was not self-evidently a loser from these transactions. The problem is that the Russians do not have a functional consumer banking system. In order to expand the economy, all the foreign aid, including loans from the IMF, had to be put in foreign banks. It was logical enough to rely on American banks, given the stability of the dollar.[5] A lot of the money that was sent to the United States was returned to Russia. What took place, in other words, was not so much the one-way looting of the vast resources of the Russian economy as it was an exercise in fund management.

Are we perhaps exaggerating the significance of this episode? If we look at the sorts of things that might have happened over the last 10 years and have not, we might gain a clearer perspective. After all, we have not had to resort to military action since the Berlin Wall came down. Nor have we faced a military coup or a communist takeover in the former Soviet Union. For that matter, we have now witnessed approximately 10 years without a revolutionary change in regime. For all the entrenched presence of organized crime, disaster has not struck. We need to take a closer and less emotional look at the role played by the criminal element in Russia.

The second point of contention that I have with Williams concerns the role of the FBI. Williams' view is that the FBI tends to be reactive and has not as yet developed a comprehensive strategy. It thus fails, in his view, to tackle some of the more important problems. The FBI also, he charges, fails to cooperate with other branches of government to the extent it might.

Whether the FBI has what can be called a comprehensive strategy may perhaps be questioned, although it certainly does have a strategy, here outlined in brief:

• Identify the organized crime groups posing the greatest threat to the United States or our significant partners throughout the world;

• Determine the structure of the group and the scope of its criminal activities;

• Develop prosecutable cases against priority groups using the criminal and civil provisions of the RICO statute in order to disrupt and dismantle criminal enterprise; and,

• Establish working relationships with domestic and foreign law enforcement and intelligence community agencies to accomplish this mission.

The other charge—regarding failure to cooperate—calls for a more detailed rebuttal. Many critics claim that intelligence and law enforcement agencies do not share information because they do not like each other, do not want to work together, and are protecting their turf. They also argue that it is the culture of law enforcement and the culture of the intelligence community that create tension. This is to trivialize what is going on. These organizations do recognize the advantages to be gained by cooperation and do, in fact, work together with other agencies. The FBI section that I run, for example, is in touch with both the Central Intelligence Agency (CIA) and the National Security Agency (NSA).[6] If these organizations are reluctant to share information, it is for quite legitimate

reasons: the sharing of information carries with it some serious hazards. Moreover, not just cultural, but also legal barriers exist between the intelligence and law enforcement communities.

To understand the reluctance to share information, it is important to appreciate one of the fundamental realities about the prosecution of cases by the FBI. This organization must litigate its cases in the public sector. As is well known, in U.S. criminal prosecutions, the defendant has a right to face his accusers in court and challenge the manner in which evidence was obtained by the prosecution. A series of pre-trial hearings is held to determine what items of evidence are admissible. The main focus of every trial is proving facts to a jury in order for that jury to conclude beyond reasonable doubt that the defendant is guilty of the offenses charged.[7] In prosecution cases based upon FBI investigations, it is imperative that the FBI employ constitutionally permissible means to obtain the evidence used, both to build its case and to present it in court. The government must explain how the evidence was obtained and who provided the information used to further the case.

The discovery process, as this is called, creates a serious dilemma for both law enforcement and intelligence. An intelligence agency that provides law enforcement with key information must disclose the sources and the methods it used to obtain that information. Clearly this poses problems. If the intelligence community has a highly-placed source reporting on sensitive espionage matters, it naturally does not want to risk having that penetration or capability exposed in a U.S. courtroom. It also needs to protect the sources and methods of its overseas partners. At the same time, the law enforcement agency runs the risk of being ordered by the judge to either identify the source or drop the entire prosecution. To be put into this quandary after spending 3-4 years, not to speak of thousands of work hours and other resources, on a case is no small risk.

The lack of smooth communication between law enforcement and intelligence, moreover, is due to certain legal barriers. These, it should be stressed, did not happen accidentally, but deliberately. The National Security Act of 1947, which created the intelligence community as we know it, put up walls between the different agencies. The fear was that if intelligence and law enforcement were to merge completely, an Orwellian type of government would result, and "Big Brother" would watch the American people too closely.

The concern for the preservation of the liberties and the privacy of the public is not unique to our country. My FBI office is currently directly and indirectly involved with the working groups of some 30 countries. They are acutely sensitive to this issue, particularly those who come from countries like Germany and Italy, which suffered under the fascist yoke during World War II. They have been given extremely limited police powers. It took about 10 years (1984-1994) for the FBI, for example, to persuade the Italians to allow the use of a "Pantiti"— a confidential informant or a cooperative witness.[8] The Italian police were not allowed to collect intelligence and conduct operations, even in their capacity as members of a law enforcement agency. They were certainly not allowed to cooperate with the intelligence community and take advantage of its assets, sources, and methods. The foreign partners of the United States, in short, share our concern for the preservation of liberties.

Does this mean that cooperation between the various agencies is an impossible task? Clearly not. Indeed, here in the United States some changes have been made over the last couple of years. The National Security Act was amended and several useful presidential directives (for example, PD-42) were issued. These directives stated that the FBI did have the right to use information collected by the intelligence community for intelligence purposes, if that information could be of benefit for law enforcement purposes. These measures have not brought an end to all

the difficulties, however. The FBI has had to set up a protocol establishing how intelligence information gets into its hands from the intelligence community and then gets disseminated to its agents in the field. This is an arduous task. It is also a challenging one, since the intelligence community is still not exempt from the discovery process.

One final point should be made. The insistence on the need to subject criminal investigations to careful public scrutiny and to maintain the barriers between law enforcement and intelligence should not be seen in an entirely negative light. The FBI enjoys an exceptional reputation with its overseas counterparts. Its operations during criminal prosecutions are held up as role models. Thanks to this reputation, the FBI can play a role in extending the rule of law overseas. Through its working groups, joint investigations, training programs, and other efforts, the FBI promotes support for tough, but fair, laws and constitutional safeguards to ensure the proper balance between protection of the people and individual liberties. These are concepts that are regrettably absent in many parts of the world. In the long run, promotion of these values will do as much as anything to reduce international crime. Thus, while it is true that investigations and prosecutions are to a degree handicapped by legal requirements, these safeguards are the very things that give the United States credibility. They should not lightly be cast aside.

In short, the FBI recognizes the need to obtain information to prosecute its cases. And it is certainly taking steps to improve communication with other intelligence agencies. Yet, whether it is tactical intelligence, as the FBI calls it, or actionable intelligence, as the intelligence community calls it, the bottom line is that information must be obtained in a usable fashion, and has to stand up to public scrutiny and the jurisprudential process.

Conclusion.

In conclusion, Williams offers a valuable assessment of the threats posed by transnational organized crime and indeed makes many valuable suggestions as to how those threats should be addressed. In weighing his discussion of the role of law enforcement, however, all readers need to be fully cognizant of the realities that govern the operation of the FBI.

ENDNOTES - CHAPTER 14

1. When Russian and Italian organized crime are involved with South American drug-trafficking organizations, Mr. Fuentes' section is involved. His section at FBI headquarters covers organized crime of Asia, Eurasia, Russia, Eastern Europe, Africa, and South Africa.

2. The FBI has close to 1,000 investigations in process overseas, in virtually every country with the possible exception of North Korea and a couple of Middle Eastern countries, where the United States is still not very popular.

3. An article in the *New York Times*, August 18, 1999, claimed that billions of dollars of IMF loans were stolen or diverted by Russian organized crime, and that much of this was transferred to the Bank of New York. Similar media accusations followed.

4. If the money concerned had originated as direct U.S. aid and had been stolen before it arrived in Russia's Central Bank, the FBI would have been given jurisdiction in the case. However, the funds concerned were IMF loans and did reach Moscow. Hence the responsibility for the billions of dollars transferred out of Moscow is Russian. For these transactions to be defined as "money laundering," they must involve money that was obtained illegally. Since the FBI has no jurisdiction in Russia, only the Russian authorities can obtain and turn over the evidence concerning how the money transfers were initiated, and who is responsible. In the BONY case, we have identified 165,000 individual transactions totaling $7 billion. The transfers occurred over the course of an 18-month period. The funds moved from Moscow through 100 banks in over 50 countries to accounts at BONY. Russian authorities, including the MVD, FSB, Tax Police, and officials of the Central Bank, are still investigating the matter.

5. This was especially true up to 1988 when the ruble was devalued.

6. The author has a group in his section working full time on this matter. An operations officer has been assigned to him from the CIA, and he maintains dual contacts with the NSA.

7. The O. J. Simpson trial, for example, clearly centered on how the investigators secured the evidence. Who got the DNA? Should they have gotten it? How was the evidence processed? Where did the investigators go?

8. A “Pantiti” is someone who is caught up in an investigation and agrees to cooperate instead of going to jail.

CHAPTER 15

PHIL WILLIAMS' VIEWS ON COMBATING INTERNATIONAL ORGANIZED CRIME: ANOTHER PERSPECTIVE

James R. McDonough

My chapter derives from my experiences as Director of the Florida Office of Drug Control Policy, and prior to that as Director of Strategy for the Office of National Drug Control. These jobs have put me in a position to appreciate the complexity of the drug control problem. I have been involved in developing national and state strategies to deal with transnational threats as they pertain to the illegal drug threat. At the same time, I have experienced first-hand the difficulties that follow in trying to implement those strategies at a local level. Incidentally, one thing I learned very early in the game is that there is a danger in classifying drug trafficking in the same way as other types of international organized crime. Drug trafficking may constitute a unique category, and for this reason it may not be possible to apply the same sorts of solutions as to other types of organized crime.

Let me begin by endorsing the effort being made to understand transnational threats and to find ways to deal with them. As one who participated in writing the 1998 National Defense Panel report calling for homeland defense, I am very sympathetic to the goals of Triangle Institute for Security Studies (TISS) and the Army War College (AWC). Nonetheless, I urge caution in applying general solutions to what constitute complex, multi-dimensional problems.

To put this chapter in context, two points must be made. First, I cannot agree with Dr. Williams' contention, if that is what he meant to imply, that there might be some benefit in

some criminal organizations. While the theoretical foundation of this view can be appreciated, in practice this position is quite untenable. There are about 1.2 million drug users in the state of Florida. About 700,000 of these are addicted or on their way to addiction. Last year, the death rate from drug overdoses in Florida surpassed our murder rate. Our heroin overdose rate is now growing at something like 50 percent a year. About 250,000 of the addicts the Florida Office of Drug Control seeks to assist are children. Of these, many are children of the middle class. No one is immune from the threat of illegal drugs, regardless of geographic location, economic status, educational background, or ethnicity. Drugs underlie a great proportion of the crime, ill health, social malaise, child abuse, economic waste, and family disintegration in America today. We have a massive problem on our hands, and it does not seem to me that we can claim that much good comes out of drug trafficking.

Second, we have a drug problem in the United States because we have a high demand for drugs. We ask for the drugs and pay top dollar for them. A strategic approach to the business of drug trafficking must logically, therefore, start with a reduction in demand. The Florida Drug Control Office, and the Office of National Drug Control Policy as well, puts most of its effort not in the reduction of the supply and not towards undermining the organizations that supply the drugs. It focuses most of all on a reduction in demand. It does so by discouraging the onset of drug abuse by those who have not yet begun to use them, and by treating those who are addicted to drugs so that they can once again become productive citizens. And this is as it should be. If somehow we could reduce demand for drugs to zero, our supply problems would go away.

Observations.

I offer a number of observations and suggestions as they relate to the problem of drug trafficking.

• We should not underrate our ability to deal with the threat. To be sure, at times it looks as if we have made no progress. But we also have not made the kind of concerted effort of which we as a nation are capable. While it is true that the organizations that traffic in drugs are rich and powerful, hiring good communicators, bankers, and lawyers, we are the United States of America. We have taken on capable foes before and vanquished them. We can defeat this threat if we make the effort, and it is of critical importance that we do.

• Law enforcement and intelligence must improve their ability to cooperate with one another. While both have real successes to their credit, they have not combined efforts and shared their capabilities in an intelligent fashion. On February 2, 1997, in the White House, I was called upon to brief the Mexican government's drug czar. He had just been checked out by the Drug Enforcement Administration (DEA), the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and others. Less than a week later, he was found hanging by his ankles in a Mexican prison in the northern part of the country, corrupt up to his eyeballs. This was news to me. The Customs operation Casablanca, mentioned by Williams in Chapter 13, was beautifully conceived and, in many ways, well executed. It did not help, however, that my boss Barry McCaffrey, who is in charge of the Office of National Drug Control in the White House, first found out about the operation when he read it in the newspaper! Nor did it help that the Attorney General was kept in the dark. Joint operations hold great promise for countering such unilateralism. Not only do they tend to keep all the critical players informed, they promise to produce a whole greater than the sum of their parts.

• By and large, the military should be kept out of the fight against drugs. There are only limited things the military can do to combat international organized crime, and many of the things it can do, it should not. The Army War College solicited some advice from us: my advice was to stay away from a direct operational role. That is not to say

that the military has no role at all to play. Williams did a very good job outlining the ways in which the armed forces can make a useful contribution. They do an excellent job training people; they can (and do) train other agencies, including law enforcement personnel; they can train other nations in a variety of ways, including the use of technology. They are good at handling equipment. They are good at communication, and no better group of translators is to be found anywhere.

They also can do some things that they would be better off not doing. They can, for instance, work the ports. A glimpse of the soldiers put to work manning the docks in Florida will shed light on my argument. Soldiers stand by a large sea-land container, unload boxes, put them through an X-ray machine, and then stick them back in the container. That is what they do all day, 7 days a week, indefinitely. While their performance of duty is admirable and the work crucial, this is probably not the best use of precious military manpower.

Soldiers also are entrusted with reconnaissance duties along the borders. Here the problem is a little different. There is a real danger that they will react unwisely and precipitate a crisis. Imagine to yourself a group of pretty tough guys, rather gung-ho, who have been told to keep alert for crossers. They see somebody moving and assume he is trying to flank them. They get nervous and fire. And they shoot a boy dead. In this instance, the problem is not that they cannot (legally) do the job, but that they may not be the personnel who have the training and disposition to handle the threat in the optimum way.

Williams also rightly stressed that the military has learned a lot about organization and working jointly with others. Lending that expertise to other organizations would probably be very helpful. Barry McCaffrey has, in fact, taken note of this. He has gathered a bank of military or former military people around him to help organize and coordinate the national counterdrug efforts of the myriad

federal, state, and local agencies that contribute to the endeavor. I have taken a page out of his book, trying to apply the lessons of organizing to solve complex problems that I learned during a long career in the military.

• We would do better to approach the drug-trafficking problem from an operational level as well as the oft-discussed strategic level. We should move, in other words, from preoccupation with solutions at the strategic level to what could be applied at the operational level. The chapters in this book are largely devoted to a consideration of transnational threats as seen from a national perspective. They have discussed what can be done by such national agencies as the FBI, CIA, NSA, U.S. Customs, and others. That is all well and good, and must be done if we are to develop a comprehensive strategy. But America is a big country, and drug trafficking is a major issue. Focusing on an operational approach that would integrate regional and local efforts into the larger strategic effort promises to improve the return on our investments.

This calls for some explanation. Let us consider what happens in a real war. First of all, a strategic plan that commits resources is developed at the national level. Theaters of war are identified. In World War II, Europe, the Central Pacific, and China-Burma-India were instances of theaters of war. But in each of these theaters, separate geographical and functional campaigns were developed. Consider an intelligence campaign. First of all, strategic intelligence is obtained (e.g., satellite pictures) from national sources. Then strategic communications intelligence is added to flesh out the strategic picture. But at the same time reconnaissance patrols are sent out on the ground so as to obtain a clear picture at the tactical level of what is going on. The strategic view and the tactical view are then merged at the operational level. Geographically, different lines of operation are developed. They are constructed to support major objectives in the theater of war. They define theaters of operation. It is the fusion of

such efforts at the operational level that allows the translation of tactical events into strategic outcomes.

In countering the drug threat, we should remember the criticality of an operational approach. That means we must be prepared to focus, perhaps functionally, perhaps regionally. We must mount a strategic effort and mount a local effort, and then fuse the two. We are trying to do that right now in Florida. For example, we invite colleagues in the DEA, the Counter Narcotics Center of the CIA, the FBI, and the National Drug Intelligence Center to come to Florida and provide us with critical analyses on what we are doing. We add to that input the information received from the El Paso Intelligence Center. At the same time, we try to involve Florida's sheriffs and policemen. We encourage them to meet one another and work together. In this way we will be able to develop an improved operational intelligence picture that fuses perspectives from both the strategic and local levels.

Then we try to move from intelligence to operations. That is the purpose of developing an intelligence picture—to act on it. There are, it must be conceded, some difficulties involved. Intelligence is defined in at least two distinct ways in the drug control business. First, there is evidentiary intelligence wherein the purpose is to gather information for the prosecution of cases. In this sort of intelligence, interest focuses on finding out what happened, and whether the evidence collected is sound and untainted. Second, there is predictive intelligence. This is the type of intelligence with which we are largely concerned. Its purpose is to develop the kind of information that will permit us to anticipate and react to threats. The process starts at the national level. For example, to find out who is trafficking internationally, Florida must turn to its friends at the federal level. The process continues with a progressive effort to focus ever more narrowly on the problems nearer home. What have the drug traffickers targeted, and when are they coming? What ports will they use? What avenues?

As these questions are answered, they must guide operations. That means that law enforcement must be capable of receiving and acting on fused intelligence analysis on short notice. That means organizations must be in a position to receive information, plan, and react. Seldom should these steps be unilateral, that is, by a single agency. Better to have in place standard operating procedures for joint efforts across agencies and across jurisdictional boundaries that maximize the unique skills and advantages of all involved.

My remarks have focused on only one part of transnational organized crime, i.e., the organizations that traffic in illegal drugs. I have tried to bring to the discussion both strategic insights (that derive from my having been the national counterdrug strategist) and operational considerations (that ensue from my responsibilities in connection with Florida's drug problem, fusing these two perspectives in a pragmatic way.

We have a vast amount of resources committed to address illegal drug trafficking. And while I grant that the criminal organizations we oppose are wealthy, ruthless, and determined, I believe that if we organize appropriately, if we make better use of available intelligence, and if we better integrate strategic, operational, and tactical efforts, we have the advantage.

CHAPTER 16

PREPARING FOR WAR IN THE FOURTH DIMENSION: A REALITY CHECK

David M. Crane

You can never plan the future by the past.[1]

Introduction.

The revolution in military affairs (RMA) has not yet been fully accomplished. There is still room for an honest assessment of how Department of Defense (DoD) will decide to fight the wars of the 21st century. A reality check is needed. As a global power, the United States is not in an enviable position. The United States will have to be prepared to engage in armed conflict in all environments and dimensions.[2] Until the recent Balkan crisis, conflict occurred in only three dimensions—air/space, land, and sea.

To these must now be added a fourth, that of cyberspace. Future conflict will range from tribal scuffles to computer network attacks.[3] Planners will have to field a trained and ready force that can deal with a warlord, an industrial-age tyrant, and a cyber terrorist or cyboteur.[4] Force planners will have to conceptualize, train, and equip this force. The hard part in all of this will be to strike a balance that allows the United States to fight and win in all four dimensions. We may not be ready to do this, yet.

The information age has arrived and has almost left the military establishment behind.[5] Five years ago information warfare was a concept new to the Pentagon, a fascinating idea tossed about in seminars and conferences alike.[6] It was little more than this, however. The concern at that time was fighting and winning a two-theater war consisting of industrial-age struggles fought in the traditional three-dimensional manner. This is still a valid strategic

issue. But now, as the fourth dimension reveals itself and information warfare becomes a reality, the defense problem becomes more complicated. We must now find a way to balance our needs. How do we fight the cyber war of the future while facing the traditional military threats of the industrial age? Throw in the asymmetric challenges of terrorism, international criminal cartels, and weapons of mass destruction (WMD), and the balancing act becomes even more delicate.[7] But to defend the national security of the United States and its interests around the world, our armed forces must update its thinking and capabilities, and soon. In a practical sense, how can this be done?

There are two general (but certainly not all-inclusive) needs that should be considered. First, thought should be given to reform of the Planning, Programing, and Budgeting System (PPBS) within DoD. Second, we need to consider bolstering our intelligence community's ability to provide timely, all-source intelligence to face any threat, anytime, anywhere. Let us consider these two needs in greater detail.

Reform PPBS.

The current 5-year budget cycle, created in the 1960s, has served the needs of a three-dimensional industrial-age armed force.[8] With the advent of the information age and the fast pace of technological development, as well as changing missions and threats, this time-tested but cumbersome process is not moving fast enough to allow the armed forces to meet these new challenges.[9]

Weapon systems and programs coming online were and are developed and fielded using technologies that may already be dated or outmoded.[10] Costly modifications and changes become necessary during the development of the system and afterwards during the fielding of that system. The relevant technology is simply changing too fast for DoD to handle.[11] Reform may be needed.

Congress and DoD have undertaken several initiatives to streamline this process through the Quadrennial Defense Review, the Joint Requirements Oversight Committee, the Unified Command Plan, acquisition reform, better business practices, and increased use of off-the-shelf technology.[12] There appears to be an understanding, however, that the process could and should be more efficient. Yet the entire department is so linked to the current three-dimensional process that wholesale functional and organizational changes may be needed in order to rectify the problems. Unfortunately, this may be just too hard to do.

Preparing the Defense Intelligence Community for Four-dimensional Warfare.

The defense intelligence community faces two challenges to its ability to provide timely all-source intelligence to the combatant commands in all four dimensions of warfare.[13] These challenges relate to the way the community is organized and to its ability to manage and disseminate the information it obtains from numerous collection sources and methods.

The intelligence community of the United States, largely nonexistent until World War II, was organized to fight the Cold War.[14] It owes its birth mainly to President Harry Truman, who realized early in his presidency that he needed information on the many world events happening around him, particularly as they related to the aggressive policies of the Soviet Union.[15] In signing the National Security Act of 1947, Truman created the national security structure that still exists today.[16] The concept of centralized intelligence was no longer a theory but reality. Over the years the intelligence community has served this nation well, in the shadows and out of the public eye, facing new and unheard-of challenges. There were many successes and some failures.[17]

As technology evolved, the collection capabilities of the intelligence community increased manyfold, providing key

information to policymakers and warfighters alike.[18] Technology elevated the intelligence community's role in our nation's defense against the Soviet threat. Before the advent of the information age, which has given relatively easy access to information to everyone, research and development in imagery and cryptology moved the United States into the forefront of information systems technology.[19] New agencies evolved to handle these new collection methods.[20] All of these agencies became a part of the vast defense intelligence community. Designed to fight the evil empire through functional organization, this community is now facing serious organizational and philosophical challenges as it tries to meet the asymmetric threats and cyber wars of the future. It is a daunting challenge.

Roughly centered on the Director of Central Intelligence (DCI) and the intelligence community management staff, each of the intelligence agencies operates separately, answering to either the DCI, the Secretary of Defense, or both.[21] Though the DCI heads the intelligence community, the reality of it all is that the Secretary of Defense manages and controls most of the intelligence assets.[22] The organizational shortcomings of the intelligence community posed substantial problems even when we faced the single Soviet threat; it is still more of a problem today. Essentially, the intelligence community is too large, too compartmentalized, and unable to share the vast amount of data it collects on a daily basis in a collaborative manner.

The DCI, moreover, continues to be head of the community in name only. This hampers the ability of the community to develop the kind of strong central focus it needs as it faces the transnational, multi-dimensional, and asymmetric threats of tomorrow. Driven by this historical and still very real dichotomy, the community is approaching these various asymmetric challenges in a fragmented and patchwork manner, causing duplication of effort and expense. Congress, through the Intelligence Committees, is all too aware of this predicment and is becoming

increasingly frustrated. Is it time for a wholesale reorganization of the intelligence community? This course has been studied, yet there have been no executive or legislative remedies forthcoming.[23] Reorganizing the intelligence community, it has been said, is like turning around an aircraft carrier. It cannot be done quickly or with a great deal of precision without assistance. It may be that what is called for is something on the scale of the Goldwater-Nichols Act (DoD Reorganization Act of 1986) to move the intelligence community into the 21st century.[24]

Another challenge is the intelligence community's inability to manage and disseminate the vast amount of information funneling into its receiving systems. To date, the effort has been piecemeal. Attempts have been made to secure collaboration in the development of various collection and analytical tools, but they have not been consistently managed or monitored.[25]

Technology is starting to become a threat as well as a benefit.[26] On the one hand, increasing technological sophistication means that our ability to access and gather information is increasingly being matched by our ability to manage and disseminate it. This development will, over time, reduce the problem alluded to in the preceding paragraph.[27] On the other hand, the increasing openness and availability of information made possible by the Internet have created new threats by reducing the relative advantage once held by the U.S. intelligence community. The information systems are also increasingly vulnerable to penetration by state or non-state actors. Computer network defense is becoming a key operational concern that all policymakers and commanders must consider in their planning.[28]

Conclusion.

There is no reason to regard these challenges as insurmountable. Historically the nation's armed forces have succeeded in overcoming an endless succession of

problems. New political, social, cultural, doctrinal, and technical challenges have confronted our armed forces from Valley Forge to Kosovo. What is needed now are new ideas and initiatives enabling our nation to better deal with the transnational threats and asymmetric challenges that will assuredly face us in the years to come. It is to be hoped that this chapter will generate creative thought and further dialogue to assist DoD in its efforts to achieve such goals.

ENDNOTES - CHAPTER 16

1. Edmund Burke, Letter to a member of the National Assembly, 1791. Burke goes on to state,

> To complain of the age we live in, to murmur at the present possessors of power, to lament the past, to conceive extravagant hopes of the future, are the common dispositions of the greatest part of mankind.

Quoted in Robin B. Wright and Doyle McManus, *Flashpoints*, New York: Alfred A. Knopf, 1991, p. 15.

2. John Shalikashvili, *Joint Vision 2010*, Washington, DC: Joint Chiefs of Staff, July 1996 (hereinafter *JV 2010*). See also, U.S. Joint Warfighting Center, *Concept for Future Joint Operations*, Fort Monroe, VA: Joint Warfighting Center, May 1997, p. i.

3. James Adams, *The Next World War*, New York: Simon & Schuster, 1998, p. 4. See, generally, Heidi and Alvin Toffler, *War and Anti-War*, New York: Warner, 1993; Robert W. Chandler, *The New Face of War*, McLean, VA: Amcoda Press, 1998; and Wright and McManus.

4. See Daniel Verton, *Federal Computer Week*, April 23, 1999, excerpted in the J*oint Staff Information Assurance Digest*, ed. 89, May 15, 1999, p. 5. The author surveys a recent study by the RAND Corporation titled "The New Terrorism," highlighting the use of technology and the Internet by terrorists in a form of conflict called "netwar." Verton discusses the report, declaring: "Netwar relies less on hierarchical command and control organizations and more on dispersed Information Age network designs." The report predicts that cyber terrorists will put more effort into building "arrays of transnationally internetted groups" than into developing stand-alone organizations.

5. Heidi and Alvin Toffler as early as 1993, in their ground-breaking and thought-provoking book, *War and Anti-war*, discuss this subject at length. See particularly p. 29. See also their book titled *Powershift*, 1990.

6. Five years ago the author designed and taught the first-ever course on the legal aspects of future war, using as course text David M. Crane, ed., *Legal Aspects of Future War*, The Judge Advocate General's School, U.S. Army, 1996. In Chapter 5, "The Impact of New Technologies on Armed Conflict," Lieutenant Colonel Alan Barna discusses the concept of information operations, highlighting the early efforts of DoD in coming to grips with this new concept.

7. See, generally, *The Report from the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction*, 1999; The United States Commission on National Security/21st Century, "New World Coming: American Security in the 21st Century," The *Phase I Report on the Emerging Global Security Environment for the First Quarter of the 21st Century*, September 15, 1999 (hereinafter, *The Phase I Report*).

8. See, generally, Department of Defense Regulation 7000.14-R, *Financial Management*, Vol. 2A, "Budget Formulation."

9. See *The Phase I Report*, p. 4. See also Peter F. Drucker, "The Age of Social Transformation," *Atlantic Monthly*, November 1994, p. 53.

10. Tofflers, p. 79.

11. Peter Drucker discusses this concept of information and technology outstripping organizations' ability to reconfigure fast enough in *Post-Capitalist Society*, New York: HarperBusiness, 1993, pp. 19-97. Also, see his article, "The Age of Social Transformation."

12. See *Concept for Future Joint Operations,* Chap. 8.

13. See comment in *The Phase I Report, supra*, p. 6: "U.S. Intelligence will face more challenging adversaries, and even excellent intelligence will not prevent all surprises."

14. Christopher M. Andrew, *For the President's Eyes Only*, New York: HarperCollins, 1995 p. 149. See also G. J. A. O'Toole, *Honorable Treachery*, New York: Atlantic Monthly, 1991; John P. Finnegan, *The Military Intelligence Story*, 2d. ed., Fort Belvoir, VA: History Office, Office of the Chief of Staff of the Army, Intelligence and Security Command [1997?]; David M. Crane, "The History of the Role of Intelligence in the United States," *Cases and Materials on Intelligence*

Law, Charlottesville, VA: Judge Advocate Generals School, 1996, Chap. 1.

15. Andrew, p. 163.

16. 50 USC 401, and following. The National Security Act of 1947 created the Central Intelligence Agency, DoD, the United States Air Force, and the National Security Council, among others.

17. For an excellent general discussion of the history of intelligence in the United States, see Andrew.

18. Finnegan, p. 54.

19. *Ibid*., p. 114.

20. Director of Central Intelligence, *A Consumer's Guide to Intelligence*, Washington, DC: Central Intelligence Agency, 1999, p. 7.

21. *Ibid*., pp. 28-29. The intelligence community of the United States consists generally of the Central Intelligence Agency; Bureau of Intelligence and Research, Department of State; Department of the Treasury, Department of Energy; and the various inteligence agencies and offices associated with DoD (see note 22).

22. See Executive Order 12333, United States Intelligence Activities, 46 F.R. 59941, December 4, 1981. See also 50 USC 401 and following. The defense intelligence community consists of the Defense Intelligence Agency, National Imagery and Mapping Agency, National Reconnaissance Office, and National Security Agency, along with the service intelligence components and the unified commands, among other organizations.

23. *Report of the Commission on the Roles and Capabilities of the U.S. Intelligence Community, Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, 1996 (also known as the Aspin/Brown Commission). In the 1995 time frame, the House Permanent Select Committee on Intelligence considered a restructuring of the U.S. intelligence community called IC 21.

24. 10 USC 161 and following.

25. See, generally, Robert K. Ackerman, "Intelligence Architecture Augments Area Expertise with Data Access," *SIGNAL Magazine 2000*, January 2000, extracted from the *Joint Staff Information Digest*, Ed. 97, January 15, 2000, p. 37.

26. See *The Phase I Report*, p. 6. The report states:

> Micro-sensors and electronic communications will continue to expand intelligence collection capabilities around the world. As a result of the proliferation of other technologies, however, many countries and disaffected groups will develop techniques of denial and deception in an attempt to thwart U.S. intelligence efforts—despite U.S. technological superiority.

27. The Tofflers declare in *War and Anti-War,* p. 160:

> . . . the Third Wave explosion of information and communication means that more and more of what decision makers need to know can be found in open sources.

28. See Joint Publication 3-13, *Joint Doctrine for Information Operations*, October 9, 1998, Chapter III. See also *Concept for Future Joint Operations,* p. 41; and excerpt from Joint Chiefs of Staff Brochure, *Information Operations: A Strategy for Peace and the Decisive Edge in War*, March 1999, p. 14:

> Computer Network Defense (CND) is emerging as a unique [information assurance] discipline. It consists of all measures to defend computers and other components that are interconnected in electronic telecommunications networks against [computer network attack] by an adversary. Such measures include access controls, detection of malicious computer code and programs, and tools to detect intrusions.

In the forward to this brochure, p. 1, Chairman of the Joint Chiefs of Staff General Henry H. Shelton declares:

> Our reliance on technology makes protecting critical US infrastructure against hostile IO [information operations] a paramount mission.

CHAPTER 17

TERRORISM AND NATIONAL DEFENSE: THE CONGRESSIONAL PERSPECTIVE

William Natter

I have spent a number of years working for Representative Ike Skelton, Ranking Minority Member on the House Armed Services Committee, during the course of which I have had the chance to observe firsthand the workings of Congress and think seriously about the issues that concern us in the present book.[1] I do not consider myself an expert in the field of national security. However, I do have a working knowledge of the matters at hand. I am on even firmer ground when I speak about my place of employment—Congress—and its inner workings. And it is to this dimension of the problem that I will reserve my comments.

I would like to present a perspective which both comes from Congress and sheds light on it. To grapple with the more important issues raised in this book, we should understand the role and viewpoint of Congress. Such understanding brings to light the pressures and motivations that result in congressional action which, in turn, affects national security, for better or for worse. Above all other relevant observations, it is important to remember that Congress is accountable—accountable for events, accountable for explanations, accountable for the very actions and decisions pursued by the various agencies of the federal government. If any readers are skeptical on this point, I would encourage you to join your congressman at a town meeting so you can hear for yourself the variety of questions, comments, and criticisms he or she is required to address in 30-second responses. In terms of accountability, this means that every 2 years elected representatives must stand before their electorates and renegotiate their

contract. For senators, it is, of course, every 6 years. And each must stand in the shoes of his or her constituency, represent their respective values, and judge the worthiness of particular ideas or proposals—both proposals of response and proposals of prevention.

For our present purposes, it is most important to remember that congressional accountability includes what I refer to as "accountability to the unreasonable." Much of the American public is extremely passionate about protecting the homeland from terrorist attack or protecting their sons and daughters from random acts of violence abroad—and they demand answers. They demand action and demand results. Members know this and respond accordingly. American citizens often ask, what is being done? What assurances do we have? How much money has been spent? And, perhaps the most significant question, have we as a nation done everything possible? To a member of Congress, they ask, "Have you done everything conceivably possible?" This last question leaves representatives and senators vulnerable if, heaven forbid, something catastrophic occurs. Consider for yourself the difficulty of responding to such a question.

All of these questions require members of Congress to seek results. Understanding these pressures goes a long way towards understanding particular spending priorities and congressional directives. Why are new initiatives undertaken? Because they provide "answers." Additional money is given for research in chemical and biological defense programs because it is an answer. The Marine Corps' Chemical/Biological Incident Response Force (CBIRF) is created because it, too, is an answer. The creation of the National Guard Rapid Assessment and Initial Detection (RAID) team concept is an answer, as is a proposal for additional spending for the Health and Human Services' Medical Strike Teams. All of these initiatives are answers, as is the existence of more than 43 departments and agencies claiming an interest in responding to a potential terrorist threat or incident. All are responses of a

sort. And, although I must admit that they may not necessarily represent appropriate or effective responses, they are *something.*

So what does this mean for actions that Congress might take? In short, Congress needs a plan, and the more comprehensive, the better. It needs to be a plan preferably provided by a non-congressional source, such as from members of the various federal departments or agencies, or from business, academia, or the executive branch as part of the President's annual budget submission to Congress. The more comprehensive the plan submitted, the more favorably it will be received. If such a plan is not submitted, mark my words, Congress will enact a version of its own. It has been known to do this from time to time. Yet, if the historical experience is any indication, I suspect a congressionally-initiated response to terrorism would likely prove to be a hodgepodge, inefficient, driven by parochialism and partisanship at the expense of the national interest, and thus ineffective. This would be unfortunate.

Although I do not want to get in the position of prescribing the response, let me mention a few points that should be considered as part of any policy that is proposed. First, there should be a greater awareness of the problem at hand, and this awareness should be institutionalized. For instance, Chairman of the Joint Chiefs of Staff General Henry Shelton, with his anti-terrorism initiative, is a case in point. Known as J-34, the Joint Staff's Deputy Director for Combating Terrorism oversees the preparation of worldwide vulnerability assessments for U.S. forces and installations. This office is responsible for performing more than 90 assessments a year, in addition to those performed by the individual services. I would argue that this initiative has already improved DoD's force protection measures and command awareness. It should continue, and General Shelton should receive additional support from the highest levels of the administration.

Interagency training exercises represent another method for improving our state of awareness. Such field exercises should continue, and be repeated over and over again. The participants in these exercises should invite congressional representatives and staff in order to improve executive-legislative branch relations. I had the benefit of serving as an observer at such an exercise more than a year ago in Norfolk, Virginia, one that proved to be a most rewarding experience. However, readers may be surprised to learn (at least I was) of the initial resistance I received from officials of the Federal Bureau of Investigation (FBI). The top participating FBI official said he did not want a congressional staff member to be present. He particularly did not want congressional staff at the standard closing critique where discussion would invariably include a discussion of "lessons learned." Fortunately, the Special Operations community recognized the potential value of my participation and urged my involvement. The experience has served me well in my official duties. If we believe the service axiom, "We must train the way we fight," then in order to facilitate the availability of necessary resources, the legislative branch must fully understand the inseparable concerns of resource needs and resource employment requirements.

Second, the president needs to take a greater interest in this subject, and not just for speaking engagements. I am talking about day-to-day operations. The national coordinator for transnational threats, Mr. Dick CLarke, sits on the National Security Council (NSC) staff in accordance with Presidential Decision Directives (PDD) 62 and 63. Clarke and his assistant, Ms. Lisa Gordon-Hagerty, should be commended for their good work.

However, the NSC staff is advisory in nature. True influence, true power—at least in the budgeting process—and therefore true results must derive directly from the president and not from an advisor. Future presidents must be cognizant of this point. They should make a habit of asking all cabinet secretaries for regular

progress reports on the effort to address transnational threats.

Third, we need to rethink legislative and regulatory oversight, modifying and updating the existing statutes, if necessary. Again, I do not pretend to be an expert in this area, but would implore such individuals as Elizabeth Rindskopf-Parker, Richard Marshall, Spike Bowman, and those with comparable experience to assist with the exploration of needed and feasible improvements. It is easy to sit in one's office and make a policy determination based on the facts at hand. It is a little more difficult, however, to anticipate the subsequent interpretation and implementation of statutory fixes. On such a complicated issue involving the convergence of national security, law enforcement, and intelligence involvement, it is important for us to examine legal issues with great care. If the information age has brought with it a need for updated laws, then let us examine the proposals. But, again, Congress will need to receive convincing testimony from noncongressional sources prior to approval of any far-reaching statutory revision.

My fourth and final point concerns the pursuit of structural reforms. Structural reforms are needed, perhaps on the scale of the DoD reforms of 1986. That is, perhaps we need a "Goldwater-Nichols Reform Act" equivalent for the defense, intelligence, and law enforcement communities. As we have heard, there is a need for a "cross-pollination" of expertise. Perhaps we should establish programs whereby mid-level professionals, from intelligence, DoD, FBI, the Federal Emergency Management Agency (FEMA), the State Department, etc., are required to spend 2- to 3-year stints in positions outside their agency of origin, further mandating that such a joint criterion be a prerequisite for promotion. Such a requirement would certainly get the attention of the national security and law enforcement communities and, moreover, elevate the issue of transnational threats within their respective departments or agencies.

Perhaps we could open further the DoD senior service schools to these same individuals, and establish exchange programs for mid-level U.S. Government professionals and members of the business world as well. It may well be that at this juncture such ideas are a bit premature and that more time is needed for the prerequisite bureaucratic and cultural "percolation." But the idea of cross-pollination certainly has gained a greater audience since I first discussed it with National Defense University professor Bard O'Neill a few years ago. I suspect the idea will continue to gain support. Perhaps it and the other proposals will soon receive the necessary consideration. In any event, I would not delay for a universal consensus to coalesce in the executive branch, thus causing Congress itself to take the lead.

In conclusion, I will echo earlier sentiments: "So many questions, so few answers." Still, the four points for consideration mentioned above must be addressed before we embrace any proposed solution.

ENDNOTE - CHAPTER 17

1. The opinions expressed in this chapter are those of this author and do not necessarily reflect the views of the House Armed Services Committe or any other individual.

CHAPTER 18

NEW INSTITUTIONS AND NEW WAYS OF OPERATING

Jeffrey A. Hunker

Introduction.

The U.S. economy is now an information economy. The Commerce Department reports that during the mid-1990s over one-third of U.S. economic growth originated in information technology fields; no doubt that percentage is already much higher. Along with the benefits of this development come some costs in the form of increased dependency on secure and reliable cyber systems. Business and government, including the military, have come increasingly to depend on these networked systems. Unfortunately, these systems are subject to deliberate disruptions, theft, and outright attack. The perpetrators can be pranksters, but they can also be terrorists, organized criminal cartels, and hostile nation-states. Most break-ins have been mere inconveniences, albeit costly; but the potential for truly serious disruption is growing exponentially.

President William J. Clinton has acted to protect our cyber networks. In 1998 he called for a national cyber defense strategy. Then in January 2000, he released version 1.0 of the National Plan for Information Systems Protection (the *National Plan*).[1] A month later he met with leaders of the Internet industry to plan additional actions for cyber security. In March 2000, he ordered federal departments to take extraordinary steps to provide protection against distributed denial of service attacks.[2] Two fundamental factors shape this program. First, cyber security is one component of an overall redefinition of national security. Second, cyber security poses an agenda that can be

managed, but never solved. The program underway is only a partial solution to the challenges, and much remains to be done. These two factors shape not only those efforts that are currently underway, but also the next generations of initiatives for information systems protection.

Fundamental Rethinking of National Security.

Our agenda for cyber security represents a fundamental rethinking of what we mean by national security, and how we act to protect it. This rethinking is the consequence of a complex shift of our enemies, our priorities, and our vulnerabilities. In the past, national security has been strictly a government responsibility. Military, diplomatic, and intelligence assets protected the United States against overseas threats. Law enforcement—carefully excluded from playing any role in *national* defense—was employed to defend the United States against domestic threats. The threats were usually well defined—they emanated from country X or group Y. U.S. business had almost no direct role.

The emerging threat of cyber attack turns this paradigm upside down. The private sector—U.S. corporations—has to solve this problem in partnership with the federal government. Like the Internet itself, no single organization is responsible for the security of our cyber systems. However, since most of the critical information systems are owned and operated by the private sector, they must share in the responsibility for defending them. This responsibility cannot be regulated. The fast pace of Internet developments precludes such a traditional approach. Furthermore, the anonymity afforded by networks, and their international reach, complicates the task of making a clear, a priori identification of emerging threats. As in the recent distributed denial of service attacks, it may be some time before we know the source or intent of the disruptions—foreign or domestic.

One thing stands clear—the nature of threats to our nation, in the domestic sphere in particular, has changed. This is forcing the United States to reexamine its traditional views of national security and the way it is organized to face threats. As the chief law enforcement organization, the Justice Department will play a leading role in facing the security challenges of critical infrastructure protection, terrorism, and the threat from weapons of mass destruction (WMD). The private sector has a major role to play in working with the Department on these issues. With its special role as the voice of business, the Commerce Department serves as a central point of contact and coordination with the private sector. It is supported by other departments and agencies which enjoy special relationships with individual sectors, as for example the Department of Energy does with the energy sectors of the nation.

The Emerging Agenda.

The *National Plan* lays out ten programmatic initiatives.[3] New institutions, and new ways of operating, are being developed by both the federal government and leading industries to address the new responsibilities and challenges. The ten initiatives can be condensed into the following five broad areas: building an effective public-private partnership; government as a model of information security; education and training; research and development; effective law enforcement and national security capabilities. Let's look at each.

Building an Effective Public-Private Partnership. Three characteristics of the Internet dictate that a federally-centered national program will fail: (1) most of the Internet and networked information systems are in private sector hands;[4] (2) only the loosest structures oversee Internet activity; and (3) the pace of Internet investment far outstrips the established Federal regulatory pace. These factors dictate a shared approach—a voluntary partnership

between the federal government (in particular, the federal national security community) and the private sector. What drives the success of this partnership will be self-interest: the recognition that the Internet needs to be secure and reliable if it is to succeed as an e-commerce medium.

Core to this emerging partnership is the newly formed Partnership for Critical Information Security, which brings together over 130 Fortune 500 companies for joint action on cyber security. Sectoral dialogue and cooperation are fostered by a system of Federal "sector liaisons" in appropriate departments (e.g., the Treasury Department working with the banking and finance industries). New ways in which trusted partners in business and government can share threat and vulnerability information are being developed—e.g., the Financial Services Information Sharing and Analysis Center (FS/ISAC), which provides a mechanism by which participating companies may anonymously share incident and vulnerability data.

Government as a Model of Information Security. While the private sector must take responsibility, the federal government can provide models and leadership. The federal government can exemplify cutting-edge best practices and drive the deployment of new technologies. This agenda includes the following topics:

• Building a Trained Organization reflects the desperate shortage of trained Federal cyber security experts.

• Developing a Framework of Best Practices that federal agencies and departments (and those outside the federal government) can apply. Unfortunately, there is no commonly accepted framework now.

• Vigilance against Vulnerabilities is a dominant goal as large and complex organizations proceed to identify and prioritize their information security needs. For the first time, Federal civilian agencies are being directed, with generally inadequate resources, to improve cyber security.

Again, there exists no accepted and fully adequate methodology for accomplishing this.

• Sharing Information across federal agencies, with non-Federal security organizations (e.g., the Carnegie-Mellon CERT), and with the private sector.

• Warning, Response, and Recovery. The Government Civilian Agency Computer Emergency Response Center depends heavily on the capabilities of Carnegie-Mellon, and is still developing an effective protocol for alerting and sharing information among Federal agencies.

• Resources and Accountability remain major challenges, which may require fundamental reforms to address. Federal budgeting, on both the executive and congressional sides, does a poor job of addressing cross-cutting needs that are not directly linked to organizational mission. To address Y2K reprogramming requirements, for example, both Congress and the executive branch created new exclusively dedicated mechanisms.[5]

Education and Training. The United States faces a desperate nationwide shortage of workers skilled in both information technology in general and cyber security in particular. The *National Plan* seeks to address this problem by creating a series of educational and training initiatives. These aim to bring into the federal government a cadre of highly skilled information technology (IT) security professionals and to upgrade the existing skills of IT professionals within the federal government. However, these Federal initiatives will not in themselves address the nationwide shortages, and should be viewed only as pilot programs for a much more extensive national commitment involving substantial business participation.

Central to the educational iniatives of the *National Plan* is the Federal Cyber Service "scholarship for service" program. The concept is based closely on the 1958 National Defense Education Act. In both NDEA and the current

proposal, the government pays for the education and living expenses of persons earning a bachelor's or master's degree from an accredited university in the requisite fields, in exchange for a commitment to serve with the federal government for a stipulated period of time. Preliminary discussions with a number of universities are underway.

Research and Development. To preserve U.S. cyber security, it is vital that we retain our technological edge, hence the need to foster Research and Development (R&D). Two major R&D actions are underway or proposed. First, Federal R&D spending for cyber security is being increased 35 percent in the 2001 FY Federal budget—to $606 million. Most of this will be directed to Defense Advanced Research Projects Agency (DARPA)[6] and the National Security Agency. Proposals have also been made to increase support for certain civilian R&D programs, such as the National Institute of Standards and Technology at the Commerce Department. The increases proposed are substantial, although they would be added to a very small base.

Second, industry and government are working together to design a new Institute for Information Infrastructure Protection (IIIP). The IIIP is necessary because existing federal and private R&D programs still leave gaps in the national cyber security research portfolio. The Y2K episode amply illustrates this problem. A concern arising from the widespread remediation of computer systems was that a malicious code might also be inserted into the systems. It would have been very useful had some automated process for detecting such a malicious code been available. However, neither government agencies nor private sector sources engaged in R&D were developing such tools. Researchers in the private sector had neglected this area of investigation because there was no market demand for such a product. The public agencies had neglected it because they could not see how such a product would help them fulfil their missions. Yet everyone agreed that such a product would have been extremely useful. Clearly there is need to develop a new kind of R&D institution that focuses on issues

neglected by existing federal programs and market-driven R&D.

IIIP would concentrate primarily upon funding, coordinating, and integrating research on advanced science and technology areas that are not being addressed through existing industry or government programs. It would not compete with industry. It would fund top-quality basic research. It would also fund and/or conduct more applied activities such as modeling and identifying vulnerabilities in U.S. information infrastructure systems and providing testbeds for information assurance technologies. To meet these needs, the Institute would:

• Have only a small expert staff. The Institute would carry out its missions by funding and tasking existing organizations or groups, operating in a manner similar to DARPA.

• Supplement, not absorb, existing research. It would coordinate its information infrastructure protection activities closely with ongoing efforts in the U.S. Government, the private sector, and academia. The Institute would also provide demonstration and development support for key foundations of cyber assurance such as benchmarks and standards, provision of testbeds, and curriculum development.

• Have close working ties to both industry and concerned Federal agencies. To ensure coordination and relevance to Federal priorities, the Institute would report to a federal Coordinating Council consisting of principal science and technology leaders. The Institute would also seek industry guidance from the National Infrastructure Advisory Council (NIAC) and Sector Coordinators. Private corporations and Federal agencies would be encouraged to fund and support projects or to lend in-kind support.

Effective Law Enforcement and National Security Capabilities. Unlike earlier national security issues,

domestic law enforcement and overseas defense responsibilities may be difficult to disentangle. This requires coordination and information-sharing between previously separate organizations. It also requires new structures and capabilities. These include:

• The National Infrastructure Protection Center. This is designed to fuse defense, intelligence, and law enforcement capabilities for threat analysis and warning, and incident response and investigation. Though part of the FBI organization, the NIPC has substantial staff from the defense, intelligence, and other law enforcement agencies. The eventual goal also includes a close operating relationship with local and international resources, and with the private sector.

• Intrusion detection monitoring systems. These are intended to provide additional warning and notice of illicit system activity. The Department of Defense (DoD) has already invested significant effort in creating a series of systems, integrated through the Joint Task Force-Computer Network Defense (JTF-CND). Federal civilian agencies would be protected under a proposed parallel system, the Federal Intrusion Detection Network (FIDNET). However, the technological currency and functionality of these systems need to be improved. The *National Plan* proposes to undertake new research to improve on the existing DoD technology. The ultimate goal is for a proven intrusion detection system to migrate to the private sector where it can protect key corporations.

• Information Sharing and Analysis Centers (ISACs) or Computer Security Centers. In networked environments, it is critical that information about vulnerabilities and threats be shared among key network players. Historically, both legal and administrative concerns have largely prevented such interchange. ISACs are mechanisms to facilitate such information exchange, whether among corporate members only, or between the private sector and the federal government. The Financial

Services Information Sharing and Analysis Center (FS/ISAC) mentioned earlier is one model—providing anonymous information exchange among participating banks and financial institutions. Computer security centers for telecommunications, the Internet community, electric power, and oil and gas companies are also either in early stage launch, or under development.

Challenges of the Future.

Ongoing initiatives in the five areas described above—public-private partnership, government as a model, research and development, education and training, and enhanced law enforcement and intelligence capabilities—capture most of the activity now underway as part of the *National Plan*. This work, however, is only the beginning. Major challenges remain in our efforts to deal with transnational threats. Among the principal outstanding unresolved issues are the following:

An Agenda for the Federal Government. Government organization is in need of fundamental restructuring in several areas.

• Government Decisionmaking that Matches Internet Speed. Budget cycles and technological cycles do not coincide. Internet "years" run from 2 to 3 calendar months. Sometimes, the actual level of funding remains uncertain until well into the current fiscal year—when a final budget deal between Congress and the president is at last agreed to. Moreover, there is no assurance that funding from fiscal year to fiscal year will be sufficiently predictable to support consistent program planning and implementation.

• Reorganizing and Clarifying Responsibilities. Interagency cooperation and coordination remain inconsistent at best. National defense, intelligence, and law enforcement must find common ground. The founding by President Clinton of the National Infrastructure Protection

Center was an important step on the way to providing operational coordination. Unfortunately, it has not yet generated the intended result. In the area of policy coordination, there still is no single official accountable for cyber security within the federal government, or even within the civilian Federal agencies. A vigorous discussion of this deficiency is underway within Congress and the executive branch. To date, however, no solution is in place.

• Increasing Effective Effort. The president has requested over two billion dollars in support of the *National Plan* for fiscal year 2001, which would double the amount spent 3 years earlier. In addition to increased resources, spending is proportionately shifting towards civilian agencies. In FY 2000, 90 percent of the cyber security budget was in national security accounts; for FY 2001 the corresponding proportion is 75 percent. These proportions are moving in the right direction. However, many Federal agencies still do not receive adequate funding. Nor is there a system in place to make sure that funds will be allocated for the best uses.

• Articulating Clear Goals to Shape Technology and Commercial Market Development. The federal government has not yet presented to industry a unified vision of our national security needs. The potential for government leadership through procurement and the bully pulpit is large but untapped. While the government constitutes only a small part of the overall market, it is also the largest single customer. In a network environment, particularly in defense procurement, the federal government has an extraordinary ability to shape the eventual development of standards or interoperability protocols[7] that will eventually be adopted by the rest of the economy and, arguably, by the rest of the world. For example, government research and procurement play key roles in shaping the ongoing evolution of intrusion protection systems and public key infrastructure (PKI) systems. An interoperability standard for different vendor offerings is needed in both these technologies. Were the

federal government better organized, it might be able to assert a leadership role.

• Intelligence Collection and Analysis for Ambiguous and Asymmetric Threats. National security threats to the United States will change. They will increasingly come to share several common characteristics. First, the means used by those threatening the United States will not be conventional nation-state force projection (missiles, bombers), but forms that are both cheaper to develop and whose sources are harder to identify (cyber, chemical, biological). Second, the targets will likely be homeland assets, in particular commercial and economic infrastructures. Third, the threats will come from a far more diverse group of enemies, be they terrorists, organized criminals, or isolated individuals of whatever mental or political persuasion.

The expanding range of these ambiguous and asymmetric national security threats challenges the Cold War intelligence system—which was adept at counting missiles and tanks, but was not designed for these amorphous, low-profile, and shifting threats. There is a fundamental need for a thorough review of our intelligence and law enforcement information-gathering, analysis assessment, and distribution systems.

An Agenda for Industry. We must adapt risk-management techniques to cyber security. Insurance and audit tools are well-established mechanisms by which companies and organizations assess and manage their exposure to various risks—financial, legal, natural, and commercial. Legal and management practices dictate that these concerns rise to the Board of Directors and senior management. To date, only very limited progress has been made in extending these techniques to the management of cyber security threats. A number of factors slow the use of risk-management techniques—the absence of a widely accepted benchmark of cyber security practices defining "due diligence," the need for management education, and

the absence of a compelling legal or liability regime addressing cyber security risks.

Arguably, however, the widespread extension of insurance, audit, and other commercial risk-management techniques to cyber security is the single most powerful force for improving network security. The National Security Council and others in the federal government are aggressively working with these risk-management communities to help extend the use of these techniques. Difficult issues emerge in regard to cyber security insurance. For example, most insurance is void under acts of war.[8] Yet what *is* war in an information systems environment? Such issues, spanning legal, policy, and economic concerns, may have significant ramifications for the eventual form of the market for cyber security insurance.

Joint Federal-Private Sector Concerns. Several relevant concerns are unique neither to the federal nor to the private sector, but rather are shared between the two.

• A System for Cyber Reconstitution. Work addressing Y2K concerns helped to illustrate that widespread or system-wide computer failures would have devastating effects on the nation. Such work also concluded that effective computer system reconstitution and rebuilding will require coordinated responses across both Federal and private sector communities, with the private sector having to contribute much of the expertise and resources. Unfortunately, the nationwide system required for such a coordinated response does not exist. While the Federal Emergency Management Agency (FEMA) has the authority and capability to coordinate non-cyber disaster relief, there is no agreement or system in place for a corresponding cyber incident. Nor are the legal underpinnings for coordinated national cyber reconstitution in place. Federal decisionmakers are not, at the moment, clear as to how key statutory measures, especially the Defense Production Act and the Stafford Act,

should be applied to address the consequences of a cyber attack.

• Expanding the Educational Agenda. Cyber security needs to become a factor in corporate, legal, and government decisionmaking—reflecting the reality that secure and reliable information systems have now become a fundamental necessity of U.S. commerce and governance. Law and business schools should include courses on transnational threats in their curriculums. America's future decisionmakers must be educated on such issues, irrespective of whether their careers are in the public or private sector. Transnational threats are not a matter of concern for the government alone, nor are they merely a technical concern.

• Creating a Legal Framework for Cyber security. How we deal with information that resides on these networked systems and prepare for and react to system failures raises complex legal and policy issues. One critical and contentious area is how both public and private sector activities affect privacy interests. Other issues include: How will courts determine and apply standards for liability? What levels of due diligence exist for information security challenges? How should lawmakers generate new policy options in this highly technical environment? The Electronic Communications Privacy Act and other key statutes need to be carefully reexamined in light of the rise of more sophisticated cyber threats and the development of new technology. There are even more basic and unanswered legal issues affecting privacy, security, and liability in an environment of growing cyber security threats.

• Who is "us"? The cyber security agenda is manifestly international in scope. Yet, while government and industry must work together to deal with cyber security threats, it is not clear which corporate citizens should be considered as part of the U.S. security establishment. To enhance security, information of a sensitive nature (classified or unclassified) may have to be passed on. But to whom?

Should we base our decision on whether or not potential recipient companies are U.S.-chartered? What if they are multinational in nature? This issue is of long standing, and no good framework for addressing it appears to exist.

Conclusion.

The agenda for cyber security is still under construction. New organizational structures must be developed, the legal framework for further public-private partnership must be built, challenging international issues must be addressed. The *National Plan* is subtitled "An Invitation to a Dialogue" for the very good reason that significant work remains to be done in building the framework for a new national security partnership.

ENDNOTES - CHAPTER 18

1. *The National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue*, Washington, DC: The White House, January 2000. Available at *www.ciao.gov*.

2. A "denial-of-service" attack is an attempt by attackers to prevent legitimate users of a service from using that service. See *http://www.cert.org/tech_tips/denial_of_service.html#1*

3. These are (1) identify critical infrastructure assets and shared interdependencies, and address vulnerabilities; (2) detect attacks and unauthorized intrusions; (3) develop robust intelligence and law enforcement capabilities to protect critical information systems, consistent with law; (4) share attack warnings and information in a timely manner; (5) create capabilities for response, reconstitution, and recovery; (6) enhance research and development in support of programs 1-5; (7) train and employ adequate numbers of information security specialists; (8) conduct outreach to make Americans aware of the need for improved cyber security; (9) adopt legislation and appropriations in support of programs 1-8; and (10) ensure the full protection of American citizens' civil liberties, their rights to privacy, and their rights to the protection of proprietary data.

4. A frequently cited statistic is that 90 percent of networked information systems are non-federal; the factual basis for this statement is unclear, but it is probably not a bad guess.

5. These included the Special Assistant to the President for Y2K (John Koskinan), with responsibilities for coordinating Federal and national Y2K preparedness, and the special Senate Y2K appropriations subcommittee chaired by Senator Bennett. Both institutions cut across the preexisting divisions of responsibility.

6. The Defense Advanced Research Projects Agency (DARPA) is the central research and development organization for DoD. It manages and directs selected basic and applied research and development projects, and pursues research and technology where risk and payoff are both very high and where success may provide dramatic advances for traditional military roles and missions and dual-use applications.

7. Common protocols are currently being developed in order to promote the evolution of the Web and ensure its interoperability. The challenge is to make the Web accessible to all by promoting technologies that take into account the vast differences in culture, education, ability, material resources, and physical limitations of users on all continents.

8. This is a requirement of many reinsurers.

ABOUT THE AUTHORS

JEFFREY F. ADDICOTT is currently a Visiting Professor of Law at St. Mary's University School of Law, San Antonio, Texas. In 2000, he retired from the U.S. Army Judge Advocate General's Corps after 20 years of service, specializing in international law. Dr. Addicott holds a Doctor of Juridical Science degree (1994) and a Master of Laws degree (1992) from the University of Virginia School of Law. He received his Juris Doctor degree from the University of Alabama School of Law in 1979.

SPIKE BOWMAN is Associate General Counsel, Federal Bureau of Investigation. He holds a Juris Doctor degree from the University of Idaho and a Master of Laws degree from George Washington University.

DAVID M. CRANE is Director, Office of Intelligence Review, Office of the Inspector General, Department of Defense. Prior to appointment to his current position, he was the Assistant General Counsel, Defense Intelligence Agency. Mr. Crane holds a Juris Doctor degree from Syracuse University and is currently completing his Doctor of Juridical Science degree at the University of Virginia School of Law.

THOMAS V. FUENTES is Chief of the Organized Crime Section, Criminal Investigative Division, Federal Bureau of Investigation.

BRUCE HOFFMAN is presently Director of the RAND Corporation office in Washington, DC, and heads RAND's terrorism research. He is the author of *Inside Terrorism* (Columbia University Press, 1998).

JEFFREY A. HUNKER is Senior Director for Critical Infrastructure on the staff of the National Security Council. In this role, he is responsible for bringing together an integrated national plan for protecting U.S. computer and information systems from organized threats. He has an A.B. in Engineering and Applied Physics from Harvard College

and a D.B.A. from Harvard Business School. He has written several articles and one book on topics of public policy and corporate strategy.

DANIEL T. KUEHL is Director, Information Strategies Concentration Program, Information Resources Management College, National Defense University, Fort McNair, Washington DC. He holds a Ph.D. from Duke University and is writing a book on the early history of electronic warfare. His most recent publication is "Information IN War or Information Warfare—Is the Distinction Meaningful?" published in *The Canadian*, Fall 1998.

PHILLIP E. LACOMBE is the Senior Vice President for Policy and Communications of the Veridian Corporation, a leading provider of information and network protection, information operations capabilities, information and technology-based solutions, and test and evaluation capabilities. In 1996 he was Staff Director for the President's Commission on Critical Infrastructure Protection. Prior to assuming his current position, he was Executive Director for the Critical Infrastructure Transition Office.

RICHARD MARSHALL is Associate General Counsel of Information Systems and Security at the National Security Agency.

JAMES R. MCDONOUGH, a retired U.S. Army colonel, is the Director of the Florida Office of Drug Control. He is responsible for the coordination of all state efforts to decrease drug abuse and its consequences in Florida. From 1996 to 1999, he was Director of Strategy for the Office of National Drug Control Policy. He served a full career as a U.S. Army officer, holding a number of key assignments, to include command at every level through brigade, directing the Army's School of Advanced Military Studies, and producing the 1993 edition of the Army's Field Manual 100-5, *Operations Doctrine*.

KENNETH A. MINIHAN, a retired lieutenant general in the U.S. Air Force, served as Director of the National Security Agency/Central Security Service from 1996 to 1999. Prior to this, Lieutenant General Minihan was Director of the Defense Intelligence Agency, Washington, DC (1994-96). He holds an M.A. in National Security Affairs from the Naval Postgraduate School.

WILLIAM NATTER has spent a number of years working for Representative Ike Skelton, Ranking Minority Member on the House Armed Services Committee.

WILLIAM J. OLSON is the Staff Director for the U.S. Senate Caucus on International Narcotics Control. He holds a doctorate from the University of Texas at Austin. Dr. Olson is the coauthor of the study series *International Organized Crime* and is the cocreator and coeditor of *Trends in Organized Crime*, an international journal that focuses on ways to disrupt criminal organizations.

CAROLYN W. PUMPHREY is the Program Coordinator for the Triangle Institute for Security Studies (TISS) and the Duke University Program in Asian Security Studies and a Visiting Assistant Professor of History at North Carolina State University. She holds a B.A. in Literature and History from the University of York, England, and a Ph.D. in History from Duke University, North Carolina (1985). She has taught a wide variety of courses at a college level, including "War and Society in Ancient and Medieval Times" and the "History of Restraints on War." She served as the Triangle Institute for Security Studies Post-Doctoral Fellow between 1997 and 2000 and is currently co-editing the conference proceedings from the TISS Study of War Summary Conference and a book on "Conflict in Africa."

ELIZABETH RINDSKOPF-PARKER is General Counsel to the University of Washington system. She holds a Juris Doctor degree from the University of Michigan School of Law. Ms. Rindskopf-Parker was formerly General Counsel for the Central Intelligence Agency and the senior legal adviser to the U.S. Intelligence Community.

DANIEL S. ROPER, a lieutenant colonel in the U.S. Army, is Politico-Military Planner, Global Division, Joint-Staff, Strategic Plans and Policy Directorate (J5). Commissioned in the field artillery from the U.S. Military Academy in 1982, he holds an M.S. in Nuclear Physics from the Naval Postgraduate School, and a Master of Military Art and Science degree from the U.S. Army Command and General Staff College.

VICTOR UTGOFF is Deputy Director of the Strategy, Forces, and Resources Division at the Institute for Defense Analyses. He holds an M.S./Ph.D in Electrical Engineering from Purdue University, and is the author of numerous papers, reports, and books, including *The Challenge of Chemical Weapons: An American Perspective* (Macmillan, 1990). His latest book is an edition titled *The Coming Crisis: Nuclear Proliferation, U.S. Interests and World Order.*

PHIL WILLIAMS is Director of the University of Pittsburgh's Ridgway Center for International Security Studies, and is also a professor in the Graduate School of Public and International Affairs at the University. He holds a Ph.D. in Political Science from the University of Southampton, England. He is currently completing two books, one on transnational organized crime and international security, the other on human commodity trafficking.