Five Dimensions of Homeland and International Security

Edited by

Esther Brimmer

Brimmer, Esther, ed., *Five Dimensions of Homeland and International Security* (Washington, D.C.: Center for Transatlantic Relations, 2008).

Center for Transatlantic Relations
The Paul H. Nitze School of Advanced International Studies
The Johns Hopkins University
1717 Massachusetts Ave., NW, Suite 525
Washington, D.C. 20036
Tel. (202) 663-5880
Fax (202) 663-5879
Email: transatlantic@jhu.edu
http://transatlantic.sais-jhu.edu

ISBN 10: 0-9801871-0-9
ISBN 13: 978-0-9801871-0-6

This publication is supported in part by the U.S. Department of Homeland Security through a grant (N00014-06-1-0991) awarded to the National Center for Study of Preparedness and Critical Event Response (PACER) at the Johns Hopkins University. Any opinions, finding, conclusions or recommendations expressed in this publication are those of the author(s) and do not represent the policy or position of the U.S. Department of Homeland Security.

Cover Image: In mathematical fractals, images display the same characteristics at different scales. Similarly, there may be connections among security issues although they occur at different levels of "magnification" (local, national, international). Image used with permission of Dave Massey, available at www.free-background-wallpaper.com.

Table of Contents

Acknowledgements

This book results from a project conducted in 2006-2007 by the Center for Transatlantic Relations at the Johns Hopkins University's Paul H. Nitze School of Advanced International Studies (SAIS). The Center for Transatlantic Relations leads the international policy work of the Johns Hopkins-based U.S. National Center of Excellence on Homeland Security, awarded by the U.S. Department of Homeland Security. This National Center for the Study of Preparedness and Catastrophic Event Response (PACER) is one of five merit-awarded U.S. university-based Centers of Excellence in homeland security.

The Center for Transatlantic Relations would like to thank our colleagues Gabor D. Kelen, M.D., of the Johns Hopkins University Department of Emergency Medicine and Lynn R. Goldman, M.D., of the Johns Hopkins University School of Public Health for their leadership of the PACER project. We would also like to thank Guy Barber, MPH, and his colleagues for our good cooperation during the course of the project.

CTR would like to thank the scholars, experts, practitioners and others who attended the February 2007 meeting that shaped our thinking about the project. Many authors in this volume participated in that event.

The editor would like to thank Center for Transatlantic Relations Director Daniel Hamilton, PhD, for his broad yet integrated vision for the project and CTR Program Coordinator Ms. Katrien Maes for her effective organization of the February 2007 project meeting and her help on the PACER project. In particular, the editor would like to thank Ms. Gretchen Losee, CTR Administrative Coordinator, for her careful copy editing and her hard work to facilitate the publication of this volume.

Throughout this project we consulted with a variety of U.S. and other security experts, but the views expressed are those of the authors. Chapter writers do not necessarily agree with each other nor was consensus sought. Rather the project was designed to foster intellectual exploration as a contribution to the policy evaluations made when crafting a comprehensive approach to preparedness.

Esther Brimmer, Ph.D.
Washington, D.C.

Introduction

Five Dimensions of Homeland and International Security

Esther Brimmer and Daniel S. Hamilton

In a globalized world, no nation is home alone; effective homeland security must incorporate international capacities along the continuum of operations, from deterrence/prevention to response/consequence management. This book sets out to understand better the intersections between homeland and international security and the implications of these connections for preparedness.

For decades, strategists endeavored to develop theories that helped policymakers safeguard vital national interests during the Cold War. 9/11 raises the specter of violent non-state actors able to inflict mass casualties even on the most powerful country in the world. Hurricane Katrina reminded us that the violence of nature can also have a devastating impact on the nation. This book considers whether some national security concepts can help orient homeland security thinking to promote preparedness. The objective is to enhance the security of our society by being prepared to address a range of challenges.

The book explores the applicability to homeland security of "5Ds": deterrence, denial, dissuasion, defense and diplomacy. The goal is not slavishly to apply traditional concepts, but to seek nuggets of insight from each to help forge new, effective ways to support preparedness. In the immediate aftermath of 9/11, attention focused on securing the homeland. We suggest that our ability to protect the homeland depends to a significant degree on our ability to forge international networks and arrangements that can strengthen "forward resilience." International security concepts can influence the international environment to make preparedness more effective at home.

This approach provides certain advantages. Not only were national security concepts designed to address vital issues, a feature in common with homeland security, but also national security ideas recognize the integral nature of the international dimension to what might otherwise seem to be a domestic question. National security has long been linked to international security. For example, freedom of the seas, patrolled by the British, and later the American navy, not only facilitated navigation and commerce but allowed the United States to grow and prosper with relatively little interference from other powers. Shaping favorable international security conditions helped safeguard the homeland. In recent decades, American leaders have understood that "forward defense," anchored by alliance structures in Europe, Asia and the Middle East, can also be an important support for security at home. These insights remain valid today. But today the front line may no longer be the Hindu Kush but the Washington D.C. metro or the port of Long Beach. Efforts to ensure "forward defense" must be supplemented with new arrangements for "forward resilience." Our deeply integrated economies and societies mean that the United States cannot secure its own society without the support of other countries. We need international cooperation to secure ports and transportation routes, to contain disease, even to help meet the challenges of devastating natural disasters. Significant international aid flowed to the United States after Hurricane Katrina, yet the U.S. was unprepared to accept or to utilize such assistance effectively.

This book results from a project conducted in 2006-2007 by the Center for Transatlantic Relations at the Johns Hopkins University's Paul H. Nitze School of Advanced International Studies (SAIS). The Center for Transatlantic Relations leads the international policy work of the Johns Hopkins-based U.S. National Center of Excellence on Homeland Security, awarded by the U.S. Department of Homeland Security. This National Center for the Study of Preparedness and Catastrophic Event Response (PACER) is one of five merit-awarded U.S. university-based Centers of Excellence in homeland security. Throughout this project we consulted with a variety of U.S. and other security experts, and commissioned a number of papers addressing ways in which the "5Ds" could be relevant to homeland security, particularly when it comes to efforts to prevent, prepare for and recover from high-consequence events. This volume includes these papers prepared under the auspices of the PACER project.

Our authors focus on two ways the international security dimension contributes to homeland security: first, how national and international security theories can contribute concepts to homeland security planning; and second, how international factors are intertwined with effective homeland security planning and cannot be an afterthought.

One of the most powerful ideas uniting national security and homeland security is the concept of resilience. In his paper, British expert Sir David Omand discusses the approach, which has shaped UK policy and which may also benefit American policymakers. A resilient society is able to absorb and bounce back from both natural "hazards" and intentional "threats" from terrorist or others. Yet as he notes, a nation can only be as resilient as its neighbors. The U.S. is deeply embedded in an integrated, globalized world. Our resilience depends on others. We need to work with other countries and organizations to shape the international context that supports homeland security, both for ourselves and for others. In fact, a key priority should be to focus on ways to "project resilience" with others abroad as we build resilience at home. The 5Ds—deterrence, denial, dissuasion, defense and diplomacy—can contribute to a more resilient society by giving policymakers ways to work with others to influence the international context to support homeland security. Omand argues that this requires a "Nelsonian" rather than "Napoleonic" model of leadership, and a particular challenge to the U.S. to rebuild its "soft power" and "moral leadership," which have suffered considerably in recent years, as well as having the capacity and will to deploy hard power when required. He provides a number of specific suggestions at the strategic, operational and tactical levels.

Amy Sands and Jennifer Machado apply this notion of a systemic framework to the challenge of chemical weapons, arguing for the development of a Chemical Weapons Terrorist Threat Chain including a range of coordinated "cradle to grave" efforts.

Major General Bruce Davis of U.S. Northern Command, a participant in our project, argues in his chapter that an overall approach could best be captured through the creation of a National Homeland Security Plan to complement the National Response Plan. The NRP tends to focus on coordinating agency activities during response, with less application to preventing an attack, leaving a gap in preparedness. He illustrates how the homeland is confronted by threats ranging from national security threats such as ballistic missile attack to law enforcement threats. In the middle is a "seam" of ambiguity where threats are neither clearly military wartime threats nor clearly criminal type threats. He outlines a number of ways a National Homeland Security Plan could bridge the gap in preparedness and cover the "seam of uncertainty."

Building a resilient nation in a globalized world means being capable of receiving assistance, not just providing it. 9/11 and Katrina are two recent catastrophic disasters in the U.S. when foreign help was useful, but for which the U.S. was unprepared. How may U.S. homeland security mechanisms be adapted so the U.S. can vet foreign offers of assistance after a large-scale crisis? What standard operating procedures (STANOPS) may be required within the U.S. government, with U.S. states, with the private sector/NGOs or with foreign authorities?

Deterrence

Deterrence involves threatening to punish someone to persuade them not to take some action. Traditionally, deterrence has been associated with the nuclear stand-off between the Cold War superpowers. Knowledge that each could destroy the other in retaliation for an attack forestalled any action. Many analysts argue that terrorists have no territory, so cannot be deterred in the classic sense. Yet as we argue in this volume, deterrence includes more subtle understandings that are relevant for homeland security. For instance, terrorists may be susceptible to political "influence" if not deterrence in the customary sense.

Thinking of deterrence in new ways can yield a number of useful insights. Jonathan Stevenson outlines a number of suggestions in his chapter. We would add some other thoughts. First, it is important to differentiate between deterring certain actors and deterring certain actions. We may be able to deter actors by finding out what they value, or what their supporters value. This requires a more subtle understanding of the types of potential terrorists. Threats might come from international networks with organized cells, they could come from local affiliate groups, or they could come from self-starters. It may be possible to trace and disrupt international networks. Local affiliates may have limited demands and therefore may be open to deterrence and diplomacy. Even self-starters may be supported by a network; their supporters may be deterrable even if they are not. Suicide bombers may be the hardest case. They no longer value their own lives. In their tragic calculation of weakness, they believe death is their only option. Changing their views may require speaking to them through non-conventional channels, ranging from their mothers to respected religious leaders. If relatives of potential terrorists no longer consider their actions glorious, the calculations of such would-be terrorists might change. Furthermore, the leaders who use or supply suicide bombers do want to live themselves. They are rational and could be deterred by punishment.

In sum, tailored deterrence tactics might usefully focus on the "supply side" of high consequence terrorism: if the prime agents may not immediately be deterrable, go after their accomplices or intermediaries or suppliers.

Deterrence may also be useful by picking apart networks that threaten us. For instance, transnational organized crime is a likely source of weapons of mass destruction (WMD) or WMD materials, and deterrence threats have had some effect when aimed at such groups. As David Auerswald argues, "a wide literature on organized crime groups, and on the deterrence relationship between threatened punishment and criminal behavior, supports the idea that transnational organized crime groups should be susceptible to deterrence threats, given particular, achievable circumstances."[1] Such groups may be willing to develop, transport or steal a WMD device or materials and sell it to rogue states or terrorist groups, but they are less likely than the terrorists themselves to risk detection, injury or death.

M. Elaine Bunn underscores this point: "Focusing on the components and enablers of a terrorist network—operatives, leaders, financiers, state supporters, the general populace—may provide insights about where costs can be imposed, or benefits denied, in order to effect deterrence."[2]

Deterrence and dissuasion of an activity make it harder for antagonists to use certain methods. In the macro sense, we want to deter the use of violence for political ends against civilians. In the immediate term,

[1] Auerswald, David P., "Deterring Nonstate WMD Attacks," *Political Science Quarterly* (December 2006).

[2] See her contribution to this volume. See also: Bunn, M. Elaine, "Can Deterrence Be Tailored?" Strategic Forum No. 225 (Washington, DC: National Defense University, Institute for National Strategic Studies: January 2007).

we want to deter mass casualty attacks on civilians at home, which will also require international action.

There is an important distinction behind deterrence for national security purposes and deterrence for purposes of law enforcement. The message usually conveyed by national security deterrence of high consequence threats is "don't do it at all;" the message often conveyed by law enforcement deterrence of less-than-high consequence threats, on the other hand, is "don't do it *here*." Many nations apply the law enforcement rather than the national security approach to deterrence when they engage in international efforts to combat high consequence threats. Yet the law-enforcement paradigm of deterrence is likely to prove inadequate to the challenges of the post 9/11 world, when non-state groups can easily shift their activities from one location to another and still retain their potency.

Moreover, it is important to recognize that adversaries could also try to deter the U.S. or key allies. Given the potentially catastrophic nature of the challenge, greater attention should be given to the dynamics of an "asymmetrically deterred world," in which the U.S. or key partners may also be deterrable. The United States should consider a variety of steps to take now to counter the threat of blackmail deterrence against it. Lewis Dunn offers a variety of suggestions in *Can al Qaeda Be Deterred from Using Nuclear Weapons?*[3] As a start, he argues, it is none too soon to begin thinking through how a non-state opponent might implement such a strategy operationally. Policymakers should consider issues ranging from how an opponent would prove possession of nuclear weapons to what types of threats might be made and in what manner. Gaming could play a role in this consideration. U.S. officials will need to put in place necessary procedures and capabilities to assess the credibility of any future nuclear threats, including possible assistance to U.S. friends and allies. Officials will also need to identify and assess options for U.S. counter-deterrence strategies in the event of a credible nuclear threat by a non-state actor. Key issues would include what information to make public and when, how to surge detection and defenses, what private posture to adopt, and how to respond in the absence (unlike state deterrence) of a known "return address."

[3] Dunn, Lewis A., *Can al Qaeda Be Deterred from Using Nuclear Weapons?* Center for the Study of Weapons of Mass Destruction Occasional Paper 3 (Washington, DC: National Defense University, July 2005).

What responsibility does the U.S. have to educate state actors who possess WMD about the implications of their WMD possession? In the dawn of the Cold War, it took many years for the U.S. and the Soviet Union to establish communications and control procedures over nuclear weapons. Have all new nuclear powers developed such controls? Is it perhaps in the U.S. self-interest to help such regimes develop such controls, regardless of how distasteful we may find the regime itself?

Jonathan Stevenson makes a complementary point, suggesting that we could engage political Islamism, particularly "partially fulfilled Islamists," who have a stake in gaining a state. We would need to differentiate carefully among such groups. Still, some may be subject to deterrence because they have an interest in gaining territory in the future.

Effective deterrence requires ways to convey deterrent messages to potential adversaries. Currently much of the public message focuses on the disastrous consequences for American society of a high-consequence event. A more effective message should be delivered to would-be opponents of the consequences for their own societies of use of WMD or other high-consequence actions. An attack of contagious disease, for instance, could sicken thousands to millions in the developing world. The U.S. could undertake actions and convey messages to encourage "self-deterrence" among opponents, i.e. reinforce any concerns on the part of would-be attackers that employment of a nuclear weapon or other high-consequence weapon on American society would serve not to rally their own publics but would in fact repulse them.

As Jonathan Stevenson states, "the central question as to deterring Islamic terrorists remains how to jeopardize their popular support"[4]—how to win the battle for hearts and minds. Stevenson points out, however, that this campaign has generally been presented as an alternative to deterrence, rather than as application of it. He argues that it is more useful to think of the latter, and outlines why in his chapter.

Given that terror networks can ally or intersect with criminal organizations and state sponsors, it is important to identify nodes of interaction between criminal and terrorist groupings. It is also important to discover "enabling nodes" of licit and illicit activity that openly or

[4] Stevenson, Jonathan, Chapter 3, page 51.

covertly facilitate high consequence terror activity. Tamara Makarenko argues in her chapter that it is important to dissect the interaction between criminal and terrorist groups. It would be useful to conduct an adversarial network vulnerability analysis of links between international terror networks and four other criminal networks: proliferants of WMD or WMD-related materials; human trafficking; money laundering; and drugs. It would also be important to conduct an analysis of key "enabling nodes" for terrorism—for instance, communication networks; new media and new media technologies; weak regulatory capacities of regional governments; poor tracking of dubious money flows; domestic sourcing of weapons by terrorists by corrupt or complicit governments; facilitated access to WMD-relevant knowledge and materials; or black holes or safe havens. Comparing results from these two exercises could help identify, by function and location, key "vulnerability hubs" of terrorist activity. Makarenko argues that deterrence might usefully be incorporated within international criminal justice strategies that seek to discourage prison radicalization or engaging in document or banking fraud.

Dissuasion

Whereas deterrence focuses on stopping identifiable adversaries from employing real capabilities, dissuasion aims at stopping potential adversaries from ever developing such capabilities. It goes to the heart of new-era vulnerabilities. Once the—initially hazy—concept of deterrence was equipped with a full-fledged strategic theory, it acquired a role of central importance during the Cold War. The same may hold true for the concept of dissuasion today—but only if it too is equipped with the full set of analyses and calculations needed to bring it to life. How can the U.S. dissuade effectively? How might dissuasion theories be adapted and applied to homeland security practice?

The *U.S. National Security Strategy* links the two concepts: "Minimizing the effects of WMD use against our people will help deter those who possess such weapons and dissuade those who seek to acquire them by persuading enemies that they cannot attain their desired ends." (p. 30) *The National Strategy for Combating Weapons of Mass Destruction* identifies dissuasion as the primary method for preventing acquisition of WMD. These documents are very general, however, and do not address the complexities of developing comprehensive dissuasion strategies. They also are currently applied to states—but how could strategies of deterrence and dissuasion apply to terrorists or other non-state actors? Dissuasion is inherently a concept that could potentially link the diverse "homeland security" and "national security" communities. It could become an important new link in national security strategy by covering the grey zone between assuring publics and partners, and deterring adversaries.

In their chapter, Charles D. Lutes and M. Elaine Bunn differentiate between deterrence and dissuasion, noting that deterrence focuses "on convincing an adversary not to undertake acts of aggression," while dissuasion "is aimed at convincing a potential adversary not to compete with the United States or go down an undesirable path." They distinguish between direct and indirect dissuasion, but caution that dissuasion is a long-term approach requiring "patience and time."[5]

These concepts require not only the trust of other partners but also their active cooperation, which means they must be embedded in new diplomatic approaches that accord high priority to U.S. homeland security. The Department of Homeland Security has posted a DHS attaché to the U.S. Mission to the European Union, but how can homeland security concerns figure more prominently in U.S. diplomacy—and how do they relate to evolving U.S. policies of deterrence, dissuasion, denial and defense? For instance, how should arms control treaties geared to states be adapted to non-state actors? The global legal regime focused on the activities of states, not subnational groups or individuals, is weak with regard to monitoring and verification, and fails to deal adequately with different kinds of WMD. On the other hand, recent decades offer clear examples of successful diplomacy regarding nuclear weapons—Belarus, Kazakhstan, Ukraine, Argentina, Brazil and South Africa were all persuaded to abandon their nuclear weapons activities. How can such efforts be adapted to today's more complex challenges?

One option would be to make the transaction costs higher for money laundering, weapons trafficking and other such activities. Analyzing the nexus between crime and terror, Makarenko argues that dissuasion could benefit intelligence-led policing and intelligence-led diplomacy when foreign-based actors are involved, for instance by dissuading

[5] Lutes, Charles D. and M. Elaine Bunn, Chapter 5.

banks from tolerating fraud and encouraging them to disclose all fraud-related losses as a way of providing important intelligence against terrorist networks.

Dissuasion is also a function of preparedness. A culture of preparedness in the U.S. could dissuade adversaries from attacking here. The notion of resilience can contribute to the culture of preparedness. Citizens who appreciate resilience understand that even after an attack, society will continue and they should not panic. A prepared citizenry means that the impact of an attack would not necessarily lead to the political end desired, thereby possibly dissuading such an attack.

Denial

Most analysts associate deterrence with punishment. As David Auerswald defines it, "threatening an adversary with pain if that adversary changes its behavior in ways that you find detrimental to your interests."[6] Yet deterrence can also work by decreasing the benefits an adversary may get from a high-consequence action. This latter element, known as deterrence by denial, may be apt for homeland security strategies. Given the revolutionary pace of bioscientific advancement, for instance, the only serious deterrent against a bioattack may be a robust national and international quick-response capability to produce vaccines. Such capability could deter potential adversaries from ever launching such attacks because they would calculate that it just was not worth the effort.

Deterrence by denial also requires that we identify the opponent's goals with some specificity. This demands excellent intelligence capabilities.

Denial strategies will become important when considering high consequence events—including export controls that inhibit access to the necessary technologies and materials that are essentially dual-use. What opportunities may there be for greater "supply-side security" by working together to deny terrorists the means to carry out catastrophic acts of violence by securing highly enriched uranium and plutonium, or other essential ingredients of mass destruction? Can the Proliferation Security Initiative (PSI) and Cooperative Threat Reduction Programs

[6] Auerswald, David P., "Deterring nonstate WMD attacks," *Political Science Quarterly* (December 2006).

serve as models for other areas of homeland security when it comes to high consequence concerns? The PSI is both defensive and deterrent in nature, for instance.

Robert Quartel underscores the complexity of the situation in his chapter. Maritime security is not just about the seas, he notes. Denial strategies need to include denial via the land-side of ports. He points out that business is developing its own ways to deal with possible disasters.

Defense

We still are suffering from a Cold War hangover, particularly from the perception that civil defense is futile. If the U.S. is truly committed to a "full spectrum" approach to security, active defense must be an essential component. How will U.S. missile defense efforts, passive defenses, or emerging agent-defeat technologies relate to other dimensions of strategy across the spectrum? Broader approaches are required that integrate domestic defensive efforts with those being advanced abroad.

James Lebovic has developed the idea of "defensive denial," a strategy to make the cost of terrorists' failure high (or benefits of success low because we are so well prepared). He argues that potential adversaries may either choose not to attack, attack elsewhere, or delay attack (allowing defense preparations to improve). He describes "limited," "partial" or "flexible" and other forms of "layered defense" including "defensive uncertainty." His latter point conflicts with those of other analysts, who see defensive certainty, not uncertainty, as dissuading potential attackers. Experts in biosecurity, for example, would argue that when facing the challenge of biological threats, defense *is* deterrence.

The networked nature of modern societies should also prompt reconsideration of what, exactly, one needs to defend. Traditional strategies focused on securing territory. Yet al-Qaeda, energy cartels, and cyberterrorists are all networks that could prey on the networks of free societies—the interconnected arteries and nodes of vulnerability that accompany the free flow of people, ideas, goods and services. It is our complete reliance on such networks, together with their potential susceptibility to catastrophic disruption, that make them such tempting targets. In the 21st century, in short, what we are defending is our connectedness. A transformative approach to security would thus supplement the traditional focus on the security of the territory with a clearer focus on the security of critical functions of society.

A security approach focused on defending the connective tissue of modern society would seek to protect critical nodes of activity while attacking the critical nodes of those networks that would do us harm. Given the interdependence of these networks, such an approach would need to merge domestic and international efforts. It would also need to include the private sector, which owns most of such infrastructure yet has its own views of protection that may differ from those of the public sector. In this spirit, Robert Quartel discusses issues involving the transportation sector, while Heiko Borchert and Karina Forster analyze energy security.

Much focus is on defending domestic critical infrastructure, as if it were static. But as David Omand and other participants in our project have argued, much of the nation's critical infrastructure is dynamic, tied to flows of information, power, and substances constantly coursing and shifting. This dynamism creates a new set of vulnerabilities that can be exploited, and could lead to cascading failures through the system. Moreover, U.S. domestic system vulnerabilities could be based abroad. For instance, the entire U.S. smallpox vaccine supply was produced by one private factory outside of Vienna, Austria. This is one example of nodes of U.S. domestic vulnerability that exist outside the United States. Identifying and defending those nodes, as well as seeking to mitigate "connectiveness vulnerabilities," could prove critical to domestic homeland security operations.

Such considerations lead one to consider ways to construct a "homeland security" equivalent to the traditional U.S. military posture labeled "forward defense." Under this rubric, U.S. forces defending the homeland primarily through engagement far forward, in Europe and in Asia. A homeland security version of this doctrine might be considered "forward resilience," i.e. sharing societal defense strategies with allies and enhancing our joint capacity to defend against threats to our interconnected domestic economies and societies. Such an approach would underscore the U.S. interest in helping other nations develop their own resilience to catastrophic threats.

We also must also decide who provides defense for what? As Commander of the U.S. Army's Joint Task Force Civil Support, Major

General Bruce Davis presents the view from the Department of Defense. Lawrence Korb and Sean Duggan explain the challenges faced by the National Guard and argue for a New Guard Operational Model. The National Guard is stretched thin as a strategic reserve for active U.S. forces deployed abroad. Yet its constitutional (as opposed to mere policy) role is to protect the homeland. One option may be to consider bifurcated National Guard activities—one element would focus on protection and response at home; another would be trained and equipped to deploy abroad. Analysts are interested in ways of empowering citizens. One idea would be a DHS Citizens Corp that would empower people rather than frighten them.

Diplomacy

Over the past few years the U.S. and key public and private partners have been forming complex, low-profile and unconventional networks to track terrorist movements, freeze terrorist funds, toughen financial transparency measures, etc. Such networks can build capacities without building bureaucracies. Can such efforts be extended to other fields?

Developing a deterrence strategy for homeland security requires finding ways to communicate the deterrence message. Conference participants discussed unconventional channels including respected religious leaders and the mothers of potential terrorists. Participants suggested efforts to enhance repugnance against use of biological weapons, tagging them as "unmanly." Other ideas included staying in touch with chemists and other experts trained in U.S. or the "West." The notion would be to maintain their sense of obligation to the scientific community, much like the responsibility some nuclear scientists felt to promote constraints in the use of their inventions.

Also, policymakers can use diplomacy to make better use of international tools such as sanctions. Chantal de Jonge Oudraat explains that whereas in the early 1990s, sanctions were geared to "compellence," sanctions are increasingly used for denial of means and for deterrence.

Terrorism tries to simplify complex situations. Audrey Cronin has explained that diplomacy can help maintain clarity and distinctions in international discourse. Diplomacy can delineate roles for compellence, provocation, polarization, and mobilization.[7] As Jonathan Winer has articulated, diplomacy is also important for communicating the messages of name and shame exercises, white lists, and terrorist designation lists.

Written Contributions

After considerable consultation with various experts in the U.S. and abroad, the SAIS Center for Transatlantic Relations invited a number of authors to develop ideas further. The resulting chapters represent a variety of views intended to foster debate and deeper analysis. Authors were asked to tackle different aspects of the 5Ds and international security. The goal was to spark ideas, not to achieve a consensus. Therefore, authors do not necessarily agree with each other. Each author expresses his or her own views, we did not seek to achieve a common viewpoint.

[7] Cronin, Audrey, *How Terrorism Ends: Lessons from the Decline and Demise of Terrorist Campaigns* (Princeton, New Jersey: Princeton University Press, 2008).

Chapter 1

The International Aspects of Societal Resilience: Framing the Issues

Sir David Omand

Resilience is a useful borrowing from the science of materials: the ability, in this case of society, to absorb deforming shocks and to bounce back into shape as quickly as possible. We might also extend our use of the term into the realm of national morale and will as the ability of society to face dangers with fortitude, continuing with normal life and holding fast to cherished constitutional values and the rule of law. Seen in that light, resilience is now a critical component of national security. But resilience must not be seen as just an issue in the domestic political space. 'No man is an island, entire of itself.' Hazards and threats to domestic life respect no international boundaries. Global influences affect the fabric of society. The welfare and security of citizens and commercial interests overseas are directly at risk. More than ever, the nature of the risks we face is dissolving the boundaries between policy making in the domestic and overseas spheres. This paper examines these issues in relation to developed nations.[1]

Horizon Scanning for Risks, Threat and Hazards

I shall use the term 'risk' to mean that combination of the likelihood of an event arising and the scale of its impact (good as well as bad since risk management means exploiting opportunities as well as building defenses against attack). The British government now prioritizes its resilience and civil contingencies planning by a 'risk matrix' classifying risks by the two dimensions of impact and probability. Much planning of resilience can be done by looking at consequences, such as loss of

[1] For wider issues affecting the resilience of developing nations see Conclusions of the International Workshop on Building the Economic Resilience of Small States, Organized by the Commonwealth Secretariat and the University of Malta, at the University Gozo Centre, Island of Gozo, Malta, March 7-9, 2005.

communications or power, regardless of cause. But British experience is that it is also useful to distinguish the management of 'hazards' (impersonal risks, whether from natural causes such as earthquakes and storms or man-made such as accidental environmental pollution) from that of 'threats' (such as terrorism, where there is a malign intelligence behind them that is capable of anticipating our responses and shaping their threats accordingly, for example in cyberspace).

It is now commonplace to see the top teams of public bodies and private sector corporations using risk matrices from the point of view of protecting their enterprises from three types of risk—those whose incidence is outside their control, such as freak weather; the risks inherent in the nature of the business, such as communications failures or industrial accidents; and—especially—the self-imposed risks to business continuity involved in embarking on new ventures such as major technology and information innovation.

Generalizing this observation, we should see a primary duty of government, local as well as central, as being to work with the other sectors of the economy and with allies and partners overseas to secure the safety of the public from all three types of major hazard and threat. Delivering this objective requires (a) taking anticipatory action to influence directly the sources of major risks facing society, and at the same time (b) to take steps to reduce society's vulnerability to the types of disruptive phenomena that we may face. Such anticipatory action will have international consequences that must be managed, and may also crucially require international understandings and arrangement to be in place in advance of a challenge arising, if the response is to be fully effective.

In terms of the first set of responses, the possibilities of acting now to reduce the risks themselves, we can certainly see looking outwards the scope for continuing action in countering jihadist terrorism, and the rise of serious criminal economic attacks against the cyberspace in which we conduct so much of our business and private lives. The spread of destructive CBRN know-how and biotechnology into malevolent hands also remains a real source of uncertain danger and, above all, needs international cooperative action. We can also see trans-national hazards which could significantly disrupt our everyday lives. Current examples include global pandemics such as an H5N1 variant influenza or SARS. If we look further out then we face the prospect of threats driven by hazards[2] as serious, irreversible impacts build up from climate change due to global warming caused by rising levels of greenhouse gases in the atmosphere. Examples given in the Stern Report[3] on the Economics of Climate Change include intra- and inter-state conflicts over access to energy or to fresh water and large-scale migration movements, including those driven by rising sea levels, much of which will be into Europe across the Mediterranean. Southern border control for the United States has of course long been an intractable issue. We can expect severe impacts of climate change in key Muslim countries already facing insurgency or terrorist threats. Will there be increased hostility to the U.S. and Europe, no doubt accused of being responsible for the rise in global warming through disturbance of the natural order of things? And on the other side of the argument, will there be rejection of fundamentalist movements and regimes whose religious ideology would shut out modernity, the application of science and of international support and economic aid in managing the consequences of climate change?

The second response to which I referred relates to reducing the vulnerabilities of an advanced society to disruption.[4] The complexity of modern society makes it more likely that disruptive events will trigger cascading effects, creating more disruption, both physical and psychological. Attention is focusing on the vulnerabilities of the Critical National Infrastructure (CNI),[5] those assets, services and systems that support the economic, political and social life of the nation whose importance is such that any entire or partial loss or compromise could cause large scale loss of life; have a serious impact on the national economy; have other grave social consequences for the community, or any substantial part of the community; or be of immediate concern to the national government.

Here too there are international dimensions, as ownership of CNI goes global, urban mega-cities become ever more diverse and mobile

[2] Human Security and Resilience, ISP/NSC Briefing Paper (London: Chatham House, February 2006).

[3] The Stern Report, 2007.

[4] Castells, M., *The Rise of the Network Society* (Oxford: Blackwell, 1996).

[5] The UK government considers that there are ten sectors of economic, political and social activity in which there are critical elements: Communication, Emergency Services, Energy, Finance, Food, Government and Public Service, Public Safety, Health, Transport and Water.

in their populations and international conventions and regulations govern critical sectors such as sea and air transportation and travel or migration. As we saw in the United Kingdom[6] first in the 2000 fuel dispute, in the floods of 1998 and 2000 and in the 2001 foot and mouth disease outbreak, and over the same period in North America with power outages and severe weather events, modern society is strongly interconnected. We rely increasingly on complex computer and telecommunications systems in power, telecommunications, transport, food and water distribution, and finance to keep normal life going. Strongly coupled markets operating globally can transfer financial shocks quickly around the world. 24/7 communications can quickly lead to rumor and panic buying. Protecting and strengthening critical infrastructure both physically and psychologically is therefore going to be an increasingly important component of national security and well-being, a challenge when 80 percent of the CNI is owned by the private sector, which in turn operates increasingly on a global or trans-national basis. To which, as I have mentioned, we can add the psychological dimension driven by the ease and speed of communication, rumor and propaganda which in an internet age is as likely to start offshore in cyberspace. We need to be very aware of the effect on societal cohesion of serious events overseas affecting minority populations at home.

It is in the judicious combination of these two responses, reducing the risks and reducing societal vulnerability to the risks, that we will find future 'national security.' The expression 'creating the protective state' is one that I have coined for this task.[7] The international dimensions arise naturally from this way of framing the issue since the potential global hazards and threats that really should command our attention are not going to be susceptible to simple solutions, least of all purely domestic remedies. Tackling most of these risks involves international cooperation and action, as does reducing some of the key vulnerabilities in society (for example, in relation to cyberspace). In this short paper I therefore suggest a framework for considering the international dimensions of resilience at the strategic, operational and tactical levels at each of which different issues arise.

[6] Mottram, Sir Richard, "Protecting the Citizen in the 21st Century", in *The Protective State* (Continuum Books: London, 2007).

[7] Omand, Sir David, "Using Secret Intelligence for Public Security," in *The Protective Stat*e, op. cit.

Framing the Issues: at the Strategic, Operational and Tactical Levels

Modern government is so complex that we cannot hope centrally to plan and coordinate all the contributory activities to building resilience. Even at the domestic level, a coherent approach to resilience is going to involve government working through many independent organizations in the private sector, at local level and even at voluntary community level. Many of these contributing organizations are not, and short of wartime conditions cannot be, 'under command.' Instead, the approach must be to establish consensus over the threats and hazards to be faced and the strategic objectives to be secured, to build strategic partnerships to work together, but all the time recognizing that what is being sought is the freely given alignment of independent actors working to a shared purpose and inspired by the same goals. Internationally, it is even more essential to apply the same approach, given cultural differences and national sensibilities.

Along with the analysis of risks and vulnerabilities arising overseas goes the parallel consequence that solutions too require international action. The activities to that end can only be mutually reinforcing if their various decisions are guided by understanding of and general sympathy for the 'Grand Strategy' being followed. This has significant implications for national leadership, for the framing of strategy and for the international presentation of the shared values that underlies it. The strategic paradigm must be the 'Nelsonian' rather than the 'Napoleonic' model of leadership. For the United States in particular, this represents a challenge to rebuild 'soft power' and moral leadership,[8] as well as having the capacity and will to deploy hard power when national interests demand it.

At the Strategic Level

Good strategic process with partners overseas can therefore help give a sense of direction and of shared priorities. The process must involve the key players being brought together in an orderly program of:

[8] For example, as advocated by Professor Joe Nye: Nye, Joseph, "Soft Power: Propaganda Isn't the Way," *International Herald Tribune* (January 10, 2003).

- Discovery and sharing of understanding of the nature of the threats and hazards, leading to identification of where shared strategic aims can be created;
- Recognition of and reconciliation of different interests (what diplomacy is about);
- Recognition of interdependence; international as well as domestic;
- Emergence of strategic concepts, shared initiatives and campaigns between the nations most concerned;
- Agreement on the developments of international institutions to carry forward this work, UN agencies, G8, NATO, EU, regional fora etc recognizing that for the most part such institutions were designed to deal with the containment of State power not to act to restrain non-State actors;
- Underlying such strategic discussion should be wherever possible, reduction of complexity to a simple conceptual framework that can be understood widely internationally, thus enabling independently captained ships to sail in convoy towards common destinations, dealing in common ways with the dangers and enemies found en route.

A sound strategic principle in relation to national resilience is to take an anticipatory view of national security. ‘Clear and present dangers’ do of course arise unexpectedly. Such dangers have to be faced nationally with whatever weapons, defenses and allies are at hand at the time. That will always be the case, but it is more important now than for some time past that we look ahead and recognize what may lie ahead; preferably, when the prospect of danger is sufficiently clear to justify attention but before the danger becomes present; ideally, acting in advance so as to avert the problem altogether but if not then reducing its likely impact on our lives; and certainly, preventing the needs of the moment crowding out the necessary preparations to face the future with confidence. And a similar statement can and should be made in respect to spotting opportunities when they are real enough prospects, and early enough to allow the necessary investment to capitalize on them. Risk management is about seizing opportunities as well as avoiding loss. To take an obvious example, should we be encouraging parts of the developing world to join global action to divert resources now into tackling CO_2 emissions before the problem becomes significantly worse, or allow a decade or more of further growth to create societies that can then better afford the costs of action, with the better technology that will then be available but at the expense of all of us having to devote a much greater share of national wealth to tackle what by then will be a significantly more dangerous problem?

It is not hard to list the subject areas on which we should be seeking to arrive at a strategic consensus with allies and partners. They include:

- Increased influence of non-state groups such as international terrorist and criminal activities, noting that the 2005 UN World Summit did not accept the Secretary General's draft Counter-Terrorism Strategy and that international corruption remains a major problem despite the work of OECD and the Financial Action Task Force (FATF);
- Climate change, and associated tensions including population migrations, noting the difficulties with following up the Kyoto Protocol process;
- Growing pressure on natural resources, noting the difficulties of delivering international support for such agreements as the 1992 Convention on Biodiversity and the Convention to Combat Desertification, and the need for internations agreements on water as well as increasing energy security issues;
- Cultural and religious divisions, including those that inspire jihadist terrorism, noting that the UN has consistently failed to agree on a definition of terrorism;
- Adjusting to the likely return to multipolarity in world affairs as the relative dominance of U.S. economic and military power declines;
- Disease, poverty and environmental degradation, with growing inequalities of poverty and deprivation, and despite the medical cooperation through the WHO and FAO, the need for practical arrangements to deliver support to poorer countries when outbreaks occur;

- Proliferation of WMD and related knowledge, noting that the main NPT, Chemical and Biological and Toxin Weapons Conventions need to be kept effective, and the current difficulties with Iran;
- The impact of scientific and technological advances that may require future international safety regulation, noting that there is no current multilateral regime addressing biosecurity.

Nor is it hard to spot some of the significant changes in the international environment in which these policies will have to be pursued:

- The changing nature of the risks, demanding both soft and hard power;
- The dissolving boundaries between domestic and overseas affairs;
- The impact on domestic social cohesion of instant access to world events and opinions available through the internet and personal video;
- With internationalization and interconnections, globalization and the rise of China and India;
- Domestically, the rising public expectations of security;
- The changes wrought by global 24/7 media.

At the Operational Level

Many of the broad classes of risk referred to earlier are of uncertain nature and require early-targeted responses when they start to emerge. The first requirement at the operational level is therefore specific risk identification at expert level through horizon-scanning and where appropriate intelligence analysis, leading to methodical risk assessments. Arrangements are then needed to share the resulting risk assessments, internationally as well as domestically, developing the networks of experts and policy makers subject by subject. As an example, in the important area of counter-terrorism, more and more nations are creating special coordinating centers. In the United Kingdom, the Joint Terrorism Analysis Centre, in the U.S., the Terrorist Threat Integration Center later replaced by the National Counterterrorism

Center (NCTC), in Australia, the National Threat Assessment Centre, in Canada, the Integrated Threat Assessment Centre, in New Zealand, the Combined Threat Assessment Group (CTAG), in Spain, Centro Nacional de Coordinacion Antiterrorista, in France, L'unité de coordination de la lutte antiterroriste.

Not only can relevant terrorist threat assessment be passed quickly between such centers, the developing bilateral relationships between them improve the mutual understanding of the underlying thinking behind national approaches to counter-terrorism and thus support strategic alignment as well as providing greater confidence for tactical engagement. Shared assessments can in particular lead to the development of common or aligned planning assumptions on which specific measures to build resilience can be based. In many areas of risk, individual nations can be only as resilient as their neighbors are. The development of the EU Situation Centre under the European Council to share national assessments is a notable recent development to that end.

A similar approach can be found in the international network of public health authorities under the WHO, with the operational arrangements made for sharing research findings on communicable disease, including animal diseases where there is a risk of the species barrier being jumped, and for harmonization of the relevant regulations for notification, quarantine and case management. International arrangements for ensuring the integrity of air safety and security, for sea container transport, for regional power grid management and oil and gas pipelines, and the management of nuclear facilities are other examples that relate directly to the confidence individual nations can have in the resilience of their own critical national infrastructure in the face of international inter-dependence and influence. With the growth of advanced control and logistics systems using modern data management and internet communications technology the need for international cooperation in cyber-defense will in particular inexorably grow.

Each subject area has over the years developed its own networks and preferred approach. At the operational level, what is needed now is a systematic mapping of critical infrastructure identifying its international dimensions (in terms both of the import and the export of causative events), and the systematic development of the cross-border, regional and global understandings and where appropriate regulation to provide greater assurance and predictability to national resilience assessment.

Finally, we might note that future national security, as at key moments in the past, is going to have to draw on the national talent for innovation in applying science and technology to resilience. And that has organizational consequences for international cooperation in this area, a good example of which is the U.S./UK bilateral Homeland Security Contact Group,[9] which provides an umbrella for the sharing of experience and technology between those two nations.

At the Tactical Level

At the tactical level, the issue for government is the ability on the day to use the strategic understandings and various collective operational policy arrangements described above to manage holistically a disruptive challenge so as to reduce its impact in terms of severity and duration. The elements of an effective response are well understood nationally, but the international dimensions may be less so.

A series of initial questions suggest themselves:

1. Is there a clear and promulgated 'operational doctrine' (to use a military term) that sets out in advance the mandates and levels of authority of decision-makers at the national, regional/state/*länder*, and local levels? Are the international dimensions identified and responsibility for managing them allocated?

2. Are the likely international neighbors and partners aware of how the national system will operate in a crisis, and thus know when, how and where to plug in and connect their own emergency management arrangements?

3. Is it clear what issues would benefit from prior international decision/consultation and which issues are already the subject of international notification or control agreements?

4. For multi-point and multi-dimensional challenges, is it clear to all when higher level (up to Head of Government) control will be exercised? And when conventional diplomatic channels

[9] See the Ministerial statements available at: http://www.iwar.org.uk/news-archive/2003/04-01-2.htm.

for international communication will have to be replaced by direct communication between national command centers—and do secure and reliable communications channels exist for that purpose?

5. Are there practiced public information arrangements for mutual sharing of statements and clearing of lines to take on events with cross-border and international implications?

6. Are there specific international arrangements for mutual aid in a crisis, and are the mechanisms understood? At the EU level for example who will be in charge, and operating from which command center? What are the arrangements for EU/NATO coordination?

7. Are there well-rehearsed casualty notification and handling schemes for foreign nationals caught up in domestic incidents,[10] and for own nationals affected by events overseas, in each case respecting the different religious and cultural issues that may arise?

Institutional Implications

Clearly, there are many other questions that could be added to such a list in terms of tactical preparations. The key to effective tactical working once crisis looms is careful anticipation of the types of issues that may arise, and testing of arrangements through exercises (ranging from table-tops to full blown playing out of scenarios on the ground with real responders). The international dimensions need to be rehearsed as part of those preparations, building on the patient strategic and operational campaigns that will have hopefully prepared the way. A model is the way that the UK and Canada have worked with the United States Homeland Security Department and have actively participated in TOPOFF exercises[11] to test cross-border and trans-Atlantic dimensions of events such as pandemics and terrorist attacks.

Let me turn very briefly to some implications for key components of national government.

[10] The plans for London are described at: http://www.londonprepared.gov.uk/londonsplans/emergencyplans/massfatality.jsp.

[11] http://www.dhs.gov/xnews/releases/press_release_0641.shtm.

First, the centers of national government must have the capacity to provide strategic direction, mobilize resources across the whole of government, and manage the international implications of a major disruptive challenge. In turn, such national centers need to be able to work confidently and securely with opposite numbers in other capitals affected by the crisis. All that needs to be thought through in advance, in relation to the full range of possible hazards and threats, and not just the traditional national defense threats.

For defense establishments, the direction of travel is already clear, for example in the provision of specialist support for homeland security, for example in explosive ordnance disposal, and chemical, radiological and biological defense, under the doctrine of aid to the civil power and with the ability to deploy such support overseas. But in the UK, at least defense thinking needs to be taken further. In such areas as the security of borders, sea and air space, the capacity to provide response to severe dislocation, for example in providing emergency communications connecting seamlessly with neighboring nations that may be affected, and in proving the framework of permanent joint command in the home theater of operations.

Likewise for foreign offices and international development departments, there is increased need to work at multilateral and bilateral strategic and operational levels as well as the basic day-to-day diplomacy and consular support. I would add too that given the nature of the international risks ahead international development agencies and financial institutions must participate in the formulation and execution of modern national security strategy.

For the homeland security and interior ministry functions, we have new organizational drivers: key aspects of national security are once again major preoccupations that should not just be seen as a subset of what in the past would have come under police and criminal justice arrangements. Add the immigration, intelligence, law enforcement and security communities and you now have significant parts of government with major overseas liaison roles working for the most part out of embassies but with their own direct links back to their parent agencies or departments. Overlapping global networks are thus being developed that demand new levels of coordination within the operational level campaigns suggested above.

Conclusion

Change on an international scale takes a long time, particularly if a new international consensus has to be built, so a greater emphasis on the international dimensions of resilience is needed now. The words of that old Victorian, the Duke of Cambridge, whose statue stands outside the Old War Office in London, hover in the air: "There is a time for everything, and the time for change is when you can no longer help it." But in building national resilience against the range of threats and impersonal hazards we may face we do not have the time to wait for such realization of inevitability of global interdependences to dawn unaided, nor should we wait for fresh disaster to strike before acting. So to accelerate the process we need to work with allies and partners overseas at the strategic level to show that the necessary changes fit a narrative that explains convincingly where and how hazards and threats are to be expected. Operational arrangements are needed to realize the contribution that international institutions and relationships can make, how they are evolving and why the time has come to accelerate the pace of change towards common goals. This brief paper is offered in that spirit.

Chapter 2

Chemical Weapons Terrorism: Need for More Than the 5Ds

Amy Sands and Jennifer Machado

Introduction

Even before the events of September 2001, the threat of terrorism involving chemical or biological materials gripped leaders of the United States. President Clinton indicated in January 1999 that he was "kept awake at night" because he believed that within a few years there would be an attack on a civilian target using chemical or biological materials. Since 9/11, the concern over the possibility of a chem-bio terrorist attack has increased, and many experts continue to believe that it is not a question of whether, but when such an attack might occur.

As the United States has tried to develop a response to these concerns, some experts have argued that it is time to expand the concept of national security beyond traditional, national security paradigms focused on the 5Ds: diplomacy, deterrence, dissuasion, denial and defense. While these concepts worked well when dealing with states, relying on them to frame a counterterrorism program may be a misplaced effort. Failed states, fundamentalist religious beliefs, and decades of alienation and anger may not be affected by diplomatic initiatives, denial of access to sites, resources, or capabilities, or threats of retaliation. As efforts are moving forward in the Department of Homeland Security (DHS) and elsewhere to develop meaningful counterterrorism strategies, it makes sense to ask whether we have the appropriate conceptual framework and tools to be able to understand and thus address effectively these emerging security challenges. A starting point for this exploration involves examining whether the traditional tools of national security, the 5Ds, help address the challenges presented by terrorism in general, and more specifically against chemical weapons terrorism.

This paper will attempt to examine the question of what a strong counterterrorism program should use as its organizing concepts. The first section will help define the chemical weapon (CW) threat, with the next section reviewing the history of CW terrorism. The final part of the paper will assess the value of the 5Ds framework in addressing the CW terrorist threat and make suggestions for how DHS might use these thoughts in its own activities.

The Chemical Weapons Terrorism Threat

The threat from chemical weapons emerges from three sources of chemical materials that can be intentionally developed and misused to cause great harm. The first two categories include not only traditional sources such as blister, nerve and choking agents, but also more commonly found toxic materials. Agents used to make traditional CW such as sarin or VX are strictly prohibited and regulated by international treaties and domestic legislation. However, *toxic* materials, such as chlorine, organophosphate pesticides, and incendiary gases and liquids, are readily accessible and in most cases available legally.[1] A third category often overlooked when reviewing CW is a conventional attack on a chemical plant or industrial complex with the express purpose of releasing toxic materials in order to harm or further terrorize the population. The defining factor in the latter two categories is linked to intent. A conventional bomb exploding near a gas station that subsequently ignites the petroleum causing harmful smoke to be released into the air should not be considered a chemical weapon. However, a strategically planned attack on a chemical facility designed to release toxic smoke in order to poison the nearby population would be included. Similarly, conventional weapons that utilize chemicals such as cyanide in hopes that it will vaporize into a toxic cloud would also be considered chemical weapons.

Regardless of the type of CW, it is important to remember that, like other weapons of mass destruction (WMD), if a CW attack should occur it will likely have an effect that goes well beyond the casualties at the site. The very nature of chemical weapons—often invisible and perhaps odorless—is designed to cause fear and panic in addition to

[1] Karasik, Theodore, *Toxic Warfare* (Santa Monica, CA: RAND, 2002) p. ix.

the physical damage caused by the actual attack. Additional impacts on the broad community may include:

1. putting an overwhelming strain on a health care system having to deal with the seriously injured as well as the "worried well";[2]
2. exposing first responders and others trying to address the crisis to toxic materials impairing their abilities to be responsive; and,
3. creating a societal psychological trauma that could have economic, political, and social implications.

Unlike bullets or bombs that are limited in range, a toxic cloud from a chemical weapon could travel for miles, indiscriminately affecting everything in its path; also, unlike conventional weapons that tend to have an immediate and finite effect, chemical weapons can linger and effect people differently as time passes.

The availability of CW depends on the type of the weapon. Traditional weapons including nerve agents, blister agents, blood agents, choking gases, incapacitants, riot-control agents, and vomiting agents are for the most part prohibited by the Chemical Weapons Convention (CWC) and are monitored by the Organization for the Prohibition of Chemical Weapons (OPCW). The CWC mandates that all chemical weapon stockpiles be destroyed. As of April 30, 2007, 100 percent of the declared CW production facilities have been either destroyed or converted for peaceful purposes and each facility is subject to a strict verification regime. However, only 30 percent of the 8.6 million chemical munitions and containers have been destroyed and only one-fourth of the world's declared stockpile of chemical agent have been destroyed.[3] Not one of the declared CW states will meet the original deadline set by the CWC and all have received extensions.[4] Russia is

[2] After the Aum Shinrikyo attack with Sarin poison in 1993, there were 3,227 victims defined as "worried well" who self-reported to hospitals, had not been exposed to any Sarin poisoning, but were suffering from several anxiety and psychosomatic symptoms. See Tucker, Jonathan B., *War of Nerves: Chemical Warfare from WWI to Al-Qaeda* (New York: Pantheon Books, 2006), p. 347.

[3] "Chemical Weapons Destruction Underway," OPCW website: http://www.opcw.org/factsandfigures/index.html#CWDestructionUnderWay.

[4] Interview with Jean du Preez, Director, International Organizations and Nonproliferation Program of the Center for Nonproliferation Studies, Monterey Institute of International Studies, May 29, 2007.

far behind in its destruction process creating great concerns about the safety and security of its remaining CW munitions given the size of its remaining stockpile and its poor security.

These existing stockpiles destined to be destroyed as well as those of the non-CWC member states are of great concern because of the potential for their theft and misuse. Additionally, non-member states who are not subject to verification by the OPCW and could pose a serious risk to CW security and management. Egypt, Iraq, North Korea, Israel[5] and Syria still remain outside the oversight of the OPCW. Iraq has already been accused of allowing chemical weapons to fall into the hands of extremist groups affiliated with al-Qaeda.[6] Although the United States and other states have supported better security and accountability for these materials via various international, regional, and bi-national programs, it is still recognized that much greater attention needs to be given to the protection, accountability, and control of chemicals that are CW precursors, critical ingredients, or potential targets.

In all of the cases mentioned above, chemical weapons are available in their most dangerous form. While some are stored in bulk containers, many of the agents are already loaded in munitions. Even so, smuggling a large warhead filled with a chemical agent across international borders would not be an easy task. And while it is possible to manufacture some of these agents in a small laboratory, it could be a daunting and dangerous task. A much simpler way of obtaining the chemicals needed is to buy them. Many of the materials needed to make a toxic weapon are readily available and legal to purchase on the open market. Toxic substances are common at chemical facilities, industrial complexes, pharmaceutical companies, oil and gas installations and fertilizer plants. Although in recent years, DHS has tried to partner with commercial private organizations to improve self-policing of private industry, much remains to be done especially outside of the United States.[7]

[5] While Israel signed the CWC in 1993, it has yet to ratify the treaty.

[6] Gellman, Barton, "US Suspects Al Qaeda Got Nerve Agent From Iraqis," *Washington Post* (December 12, 2002).

[7] *Toxic Warfare*, p. 41; *Report on Building International Coalitions to Combat Weapons of Mass Destruction Terrorism*, International Security Advisory Board, U.S. Department of State, February 2007.

The third option for creating a chemical weapon is to target a chemical facility with conventional weapons. Many of the private chemical industry plants, such as electronic manufacturers, pesticide plants, or chemical manufacturing plants are not well protected, while other community facilities could serve as potential targets, such as airports, harbors, or even universities, may not have made the security of chemical materials a high enough priority. Attacking a chemical facility would add exponentially to the damage caused by the bomb alone as even the perceived release of toxic gases may incite panic and cause chaos in the nearby population. Several examples from the "worst-case scenarios" that companies are required by law to provide the Environmental Protection Agency (EPA) demonstrate the hazards and challenges of securing facilities in an open, mobile society. According to its EPA report, Dow Chemical has one facility that if attacked might release 800,000 pounds of hydrogen chloride, which would in turn endanger approximately 370,000 people.[8] The 2005 train wreck in Graniteville, South Carolina that released chlorine gas and forced extensive evacuations, dislocations, and economic disruptions in the region demonstrated the potential for an intentional train wreck or port collision becoming an "impromptu WMD" incident.[9]

A final component to consider when reviewing the CW threat is the technology and expertise needed to make the weapon. In the case of traditional chemical weapons that use sophisticated compounds and chemicals, scientific expertise would be needed. However, in the case of the simpler toxic weapon, the Internet provides unlimited communication regarding every subject including how-to guides and manuals for all kinds of weapons and warfare. Unfortunately, it now appears that someone with basic laboratory skills and access to the materials could probably put together a dangerous toxic weapon. For example, according to the Iraqi Survey Group (ISG) Report, the efforts by the Iraqi insurgent group known as "Al-Abud network" to produce CW agents were impressive although not successful. The ISG Report noted: "The most alarming aspect of the Al-Abud network is how quickly and effectively the group was able to mobilize key resources and tap relevant experts to develop a program for weaponizing CW agents."[10]

[8] Karasik, p. 42.

[9] Schneidmiller, Chris, *Critical Infrastructure Protection: Safeguarding the Components of Everyday Life*, WIIS Policy Brief, 2006.

[10] Tucker, p. 378.

Terrorist Use of Chemical Weapons

While the threshold for CW terrorism has been crossed, it has not yet become common to use CW in terrorist attacks. Perhaps it is because of the indiscriminate nature of chemical weapons or perhaps the technological expertise to produce a highly effective weapon on the black market still remains to be harnessed. However, there are numerous examples of attempts and successful uses of all three of the above mentioned types of chemical weapons.

In 1986, a Christian Identity group known as The Covenant, the Sword, and the Arm of the Lord obtained potassium cyanide with the intention of poisoning the water supply.[11] The 1995 sarin attack in the Tokyo subway by Aum Shinrikyo killed eleven and injured more than a thousand.[12] The Liberation Tigers of Tamil Eelam (LTTE) used potassium cyanide in tea in order to cripple the Sri Lankan tea industry.[13] LTTE has utilized other forms of chemical warfare including a gas attack on Sri Lankan troops in 1995 and the firing of chlorine gas cylinders into a military camp in 1990.[14] There are also examples of attacks on industrial facilities with the intent of releasing toxic gases into the air, "…Serbian forces in Croatia used rockets, bombs, artillery, machine gun tracers and mortars on six occasions between 1993 and 1995 to attack the Petrochemia plant, which produced fertilizer, carbon black and light-fraction petroleum products."[15]

In addition to these specific incidents, there are claims that CW have been used in current military engagements. In Chechnya, both the Russians and the Chechens report that the other side has attacked with ammonia and chlorine.[16] In Iraq, Iraqi insurgents have used chlorine gas and nitric acid against American troops.[17] Also, there are reports

[11] Stern, Jessica Eve in Tucker, Jonathan, ed., *Toxic Terror* (Cambridge, MA: MIT Press, 2000), pp. 153-154.

[12] David Kaplan in Tucker, Jonathan, ed., *Toxic Terror* (Cambridge, MA: MIT Press, 2000), p. 218.

[13] Soafer, Abraham D., George D. Wilson and Sidney D. Dell, *The New Terror: Facing the Threat of Biological and Chemical Weapons* (Stanford, CA: Hoover Institution, 1999), p. 82.

[14] Karasik, pp. 22-23.

[15] Karasik, p. 21.

[16] Karasik, p. 23.

[17] Press Advisory, "Issue Briefing: Chemical Weapons, Terrorism and Nonproliferation," National Press Club, March 30, 2007.

that al-Qaeda members established a weapons lab in Kirma, Iraq with the intent of producing ricin and cyanide.[18] While specific use from al-Qaeda has yet to be sufficiently documented, there are examples of Osama bin Ladin expressing an interest and attempting to procure CW. In 2002, the Cable News Network (CNN) aired a video revealing al-Qaeda to have some form of toxic gas as viewers watched dogs die from an unseen poison.[19] While this revealed al-Qaeda's interest in utilizing CW, it also demonstrated its rudimentary capability.

This diverse list of examples of previous CW use illustrates that the threat from chemical weapons against U.S. interests or on U.S. soil cannot be limited to either the international arena or the domestic one. International terrorist groups such as al-Qaeda should be considered capable and willing to use CW. But domestic organizations such as right-wing extremists, para-military or apocalyptic groups should not be forgotten.

Security Policy Implications

Given the diverse nature of the terrorist threat, unlike the simpler Cold War threat framework, there is not a one-size-fits-all approach that can be taken. Challenges to using the concepts of the Cold War emerge immediately. The first challenge is that today the distinction between an "international" and "domestic" terrorist is not always clear. In the current world of fluid borders and cyberspace, nothing is entirely domestic or international, it is a blend. Analysis of potential al-Qaeda attacks on U.S. soil must include capability and precedent set outside the United States. Meanwhile, traditional domestic groups (e.g. Neo-Nazis) have sympathetic organizations internationally. Organizations or groups living overseas could:

1. influence activities by taking action in their own country;
2. provide materials and other technical support and/or;

[18] Center for Nonproliferation, *Chart: Al-Qa'ida's WMD Activities*, WMDTRP, May 13, 2005. Available at: http://cns.miis.edu/pubs/other/sjm_cht.htm.

[19] Robertson, Nic, "Disturbing Scenes of Death Show Capability with Chemical Gas," *CNN.com*, August 19, 2002. Available at: http://www.cnn.com/2002/US/08/19/terror.tape.chemical/index.html.

3. respond within their own country to an action in the United States, turning a primarily domestic incident into a global one.

In reality, today's terrorism should be looked at as having potential global linkages and effects, but needs to be managed at the local level where the critical support for action is available and where the damage may be done.

Another stumbling block revolves around the fact that the intelligence requirements are very different, with critical collection efforts occurring within and outside of the United States. This necessitates the collaboration of all members of the Intelligence Community and greater international coordination. The jurisdictional lines of responsibility also may become quite blurred as the targets of observation move across borders and travel frequently between and within countries. While there have been improvements in information sharing between agencies such as the FBI and the CIA, much work remains to be done. A good example of the new commitment to collaboration is the National CounterTerrorism Center (NCTC), which was established in 2004 to ensure all appropriate agencies would have access to and receive all-source intelligence to execute any counterterrorism plan and perform its tasking. The NCTC is collocated with CIA and FBI agents and works with eleven other counterterrorism operation centers daily. It has created the NCTC Online (NOL) which serves as the counterterrorism community's library with 6,000 users, 6,000,000 documents, and 60 agencies contributing materials.[20]

A third area of divergence from past national security strategies is that countering terrorism rests on excellent intelligence about individuals and small groups and not about large troop movements or clandestine missile tests. The critical piece of data that can be used to prevent a terrorist attack may reside in understanding the local social network and dynamic. Gathering and analyzing this information may require monitoring an American citizen both inside and outside of the United States in ways that may infringe on the individual's civil rights and liberties. The concern over the degree to which the Patriot Act may have infringed on these rights as the government seeks access to enough information to prevent an act of terrorism reflects a tension that was not

[20] *National CounterTerrorism Center and Information Sharing: 5 Years Since 9/11—A Progress Report*, September 2006. Available at: http://www.nctc.gov/docs/report_card_final.pdf.

for the most part an issue for the last 40 years. Unlike spying during the Cold War, monitoring U.S. citizens who may be helping a terrorist group or are even part of one challenges the delicate balance between security and individual liberties that a democratic nation must be careful not to upset.

While other areas of divergence between today's threat of transnational terrorism and the Cold War's superpower struggle could be identified, the point is that it is not possible to take the policy strategies designed for nation states and apply them universally to terrorists. The five dimensions of policy exist as a sort of continuum with none standing completely alone or being sufficient. If first attempts at *dissuasion* do not work then *deterrence* and *denial* must be added to the equation. Finally, if none of the above prevent an attack then *defense* must have been prepared for and utilized when appropriate. Throughout each and every aspect *diplomacy* plays a critical role. Diplomacy is necessary in order to: keep citizens and other nations aware of possible consequences (dissuasion); negotiate in order to prevent use (deterrence); undercut training, technology, materials and funding (denial); and reassure the public in a time of crisis (defense). But, applying these traditional national security concepts to the terrorist challenge limits the set of activities undertaken and may lead to serious policy errors and a flawed counterterrorist strategy.

By definition, terrorists are challenging the status quo, and thus may not adhere to accepted social norms and mores. Terrorists are focused on a campaign to win the "hearts and souls" of key constituents, whether through fear or faith—their war revolves around a communications strategy that can succeed even when a specific incident might appear to fail. As a result, today's terrorist threat cannot be dealt with using just the traditional tools of national security. For example, there are few standard denial practices that can be implemented when confronting terrorist organizations, i.e. embargos cannot be placed, nor can trade be restricted. In addition, some of today's terrorists do not appear deterrable or open to diplomatic overtures. They could, however, be denied safe-havens or assistance if their state sponsors and enablers were persuaded to discontinue their support. Here is an excellent example of how traditional approaches of state-to-state relations should be integrated in any counterterrorism strategy.

While the 5Ds cannot be applied to terrorists "as is," they do have value as part of a larger conceptual framework that recognizes the breadth and scope of effort needed to truly take on the terrorist threat. A much more systematic and sustained effort must be used that confronts the appeal of the terrorists while also limiting its ability to act successfully and effectively.

Chemical Weapon Counterterrorism Policy

As with other forms of WMD, the counterterrorism strategy for chemical weapons should focus on the continuum of activities that span prevention to consequence management. Prevention would encompass those elements associated with dissuasion, deterrence and denial while consequence management would deal with defense, remembering that diplomacy is active throughout the process. Such a counterterrorism strategy would also have to be holistic, providing a systems framework that recognizes social networks and linkages, multiplicity of levels of effort, complexity of any terrorist event and response, and the dynamic and evolving nature of terrorist strategy, organization, and practices. Applying this concept to the CW terrorist threat requires a CW Terrorist Threat Chain, which has yet to be fully identified and then integrated. Specifically, it should include: a "cradle to grave" control and security system for dangerous chemicals; the deconstructing of a possible terrorist attack on a chemical facility starting with the initial impetus and ending with the mitigation of effects; and, a much better sense of the root cause of terrorism in general, and specifically of CW terrorism, starting with understanding in a given context the driving forces behind the terrorism, the means of recruiting, and the catalyst for individuals and groups to use violence to address their grievances, alienation, and anger. Basically, it would require an enormous effort linking experts from multiple and diverse disciplines, such as terrorism, critical infrastructure, chemical industry, chemical weapons, chemistry, military operations, and explosives.

Numerous policy recommendations have been developed and made since the inception of the CWC, the attacks of September 11th, and the initiation of the "global war on terrorism," and many have been instituted.[21] None has tried to create a comprehensive framework that recognizes the full-scope of the terrorist challenge. It is not just for the State Department, Defense Department, and DHS—its underlying causes must be acknowledged and dealt with in meaningful ways, whether it involves making progress on Israeli-Palestinian peace or providing better lives for second generation Muslims living in Europe. These causes are ones where the U.S. government may be able to only impact marginally since they often have to do with the inner workings of communities and reflect a lack of equity, opportunity, and purpose. Moreover, these problems are not ones that any of the 5Ds can provide a conceptual framework for as they don't address the social and psychological dimensions of security. The result is that the 5Ds do not fit the new broader concept of security relevant to understanding and responding effectively to today's terrorist threat.

Prevention—Specific Suggestions in the Area of Prevention Include:

- Improve interagency coordination in regards to CW counterterrorism policy;
- Ensure that intelligence collection remains on unconventional terrorist threats;
- Continue encouragement and incentives for private industry to self-police;
- Strengthen anti-terrorism training programs for local law enforcement, especially in the chemical weapons arena;
- Analyze the underlying concerns of extremist and terrorist groups and make recommendations to the State Department;
- Promote increased cooperation with allied states and encourage other CWC member states to adopt domestic legislation outlawing CW;

[21] Jonathan Tucker outlined several policy suggestions in his chapter in *Terrorism with Chemical and Biological Weapons*, Roberts, Brad, ed. (Washington, DC: Chemical and Biological Arms Control Institute, 1997). While the book is now 10 years old and many of the recommendations have been implemented, it is important to consistently review and upgrade them as the terrorist threat changes. Many of the approaches listed here originated in Tucker's chapter, pp. 95-111.

- Bolster programs that work to separate terrorist organizations from mainstream religious and national groups;
- Increase preparedness so that a chemical attack would be less effective or even futile;
- Strengthen the health care system including first responders, treatment facilities and follow-up care;
- Create standards for dissemination of sensitive scientific information.

Consequence Management—Items That Should Already Be In Place:

- Improved coordination of federal emergency response plans with state and local authorities;
- Established emergency medical response teams, especially in urban areas;
- Determined retaliation plans;
- Stockpiles of chemical defensive materials in large urban areas;
- Developed public service announcements for emergency broadcast, informing the public of safety precautions as well as how and where medical treatment is available;
- Upgraded CW detection and identification devices;
- Enhanced antidotes and therapeutic drugs.

Conclusion: Role of the Department of Homeland Security Must Mature

DHS must continue to mold itself into one organization, stripping away any residual institutional and cultural barriers to full integration. It should, as part of this process, continue to build on its funding for the training, equipment, and exercises that are critical to limiting the impact of any CW terrorist attack as well as perhaps to helping to deter such an attack. DHS must also facilitate communication and information sharing between organizations that already work on these issues, taking the lead at filling in the gaps in security policy, especially in the areas where "international" and "domestic" touch. While it has begun to establish a network between the appropriate local, state, federal, and international agencies and individuals—much more needs to be done.

The DHS already has in place several mechanisms that can aid in the implementation of the policy directives mentioned above. In addition to the federal office of DHS, there are the individual state offices (Office of Homeland Security [OHS]). The Department of Homeland Security looks to these offices for implementing training and programs at the state and local level. In addition, DHS can call upon the multi-faceted expertise set forth in its various National Centers of Excellence. These centers include some of the most prominent figures in the field with regard to chemical weapons, terrorist motivations, and consequence management. Finally, the various state fusion centers that state OHS offices play a part in, such as the California State Threat Assessment Center, serve as an ideal way to facilitate communication between the federal, state, and local levels. The threads tying these groups together need to be strengthened and ensured of ongoing, sustained support if there is to be consistency in threat assessments, coherence in information provided the public during times of peace and crisis, consistency of standards and procedures, and robust communication capabilities.

Specific activities that DHS could undertake include the creation of agreements that allow for international intelligence to be shared. While this project will certainly involve numerous federal organizations, DHS could lead the diplomatic effort to get things started. Additionally, there is an abundant need for diplomacy on a national level between federal and state/local responders. Jurisdictional battles should be fought well before any crisis reveals weaknesses or gaps in coverage. Because toxic materials are so easily available, there is a need for an extensive risk assessment to determine the areas of greatest concern. DHS could also be instrumental in authoring a national initiative to protect chemical facilities. Much more attention needs to be paid to this threat as the potential targets remain too vulnerable, especially given the ease of acquiring explosives that could be used to release toxic materials. Whether it is additional legislation, better law enforcement, or industry-wide regulations and codes of practice, DHS should take a lead in identifying and then advocating for steps that will better deter, dissuade, and deny terrorists opportunities for CW terrorism.

The Department of Homeland Security, however, should go beyond the 5Ds—it should be the catalyst to establishing the holistic system for countering the terrorist threat in general, and specifically as it relates to CW terrorism. It should lead the way to casting off the 5Ds for a more appropriate and useful comprehensive paradigm that stretches from motives to materials to mitigation.

Chapter 3
Reviving Deterrence

Jonathan Stevenson

Compellence vs. Deterrence

In the 1960s, Thomas C. Schelling—who won the 2005 Nobel Prize in economics in part for his application of "the dismal science" to strategic problems—articulated the distinction between deterrence and what he called compellence. Deterrence fundamentally entails a state's threatening to harm an adversary in order to persuade the adversary to forego some action inimical to the state's interests. Compellence involves a state's threatening to harm or actually harming an adversary in order to induce it to affirmatively take some action favorable to the state, even though it may disfavor the adversary. As Christopher Layne has recently pointed out, while the United States has been quite effective in deterring states from directly harming American interests and assets, it has had significantly less success in compelling adversaries—state and non-state—to act decisively against their perceived interests, whether through direct military threats or coercive diplomacy. Yet since 9/11, the United States' approach to counter-terrorism has been predominantly compellent. That is, it has substantially involved direct action by U.S. military assets to kill or capture terrorists so as to compel their leadership to stand down.

The array of tasks for special-operations forces (SOF) contemplated by the Pentagon's 2006 Quadrennial Defense Review—direct action, foreign internal defense, persistent surveillance, information operations, counter-proliferation—conjures visions of SOF darting willy-nilly across the globe, from one hotspot to another, smashing terrorist cells wherever they arise. These missions would be feasible, from both an operational and a political point of view, if most al-Qaeda affiliates were territorially-based groups like the Moro Islamic Liberation Front (MILF), in the southern Philippines, which present readily identifiable legitimate military targets and have limited objectives that do not have a substantial strategic impact on American interests and are therefore susceptible to accommodation. Increasingly, however, al-Qaeda affiliates are more invisible, having infiltrated urban milieus. Leaving a dearth of effective targets, and given the inextricably piecemeal nature of law enforcement and the impossibility of airtight homeland security and passive defenses, this reality calls for an approach that leverages preventive or pre-emptive action that has a deterrent effect more than more ambitious measures aimed to modify behavior wholesale—that is, deterrence more than compellence.

A Death Exaggerated

Deterrence, in its most basic form, embodies the power to keep an adversary from acting in a hostile way by threatening what that adversary values. A state values its population, its military-industrial base, its territory, and regime security. During the Cold War, these were easy to imperil with nuclear weapons and massive conventional militaries. An individual, however, has less to worry about—especially if he considers himself divinely guided and assured of a privileged afterlife—and is a much more difficult target for a conventional military to detect and threaten on an ongoing basis. Thus, in the immediate aftermath of the September 11 attacks, the new conventional wisdom was that deterrence was dead, or at least moribund. Terrorists who were willing to take their own lives and had religiously-driven apocalyptic designs, no state or infrastructure to protect, and no feasibly negotiable political agenda could not be expected to show restraint even when confronted by a credible threat of retaliatory punishment. Furthermore, rogue states like North Korea and Iran whose leaders had obscure and seemingly irrational mindsets could not be trusted to avoid suicidal behavior in the face of American nuclear superiority. The non-state threat produced an invigorated pre-emption doctrine, enunciated in the National Security Strategy released by the White House in September 2002. The rogue state threat galvanized the United States national and theater ballistic missile defense programs.

Gradually, however, analysts and officials have retrieved some faith in deterrence *vis-à-vis* states and, to a lesser degree, non-state actors. Time and again, Pyongyang has pushed the five powers engaged in curbing its nuclear ambitions near their diplomatic limits, then relented. Iran, unlike North Korea, does not yet have a nuclear weapon and Tehran's behavior is consequently more complicated. But its tactics—teasing engagement, diplomatic withdrawal, enrichment activities, missile tests, qualified hints of compromise—follow the same basic pattern as Pyongyang's, the most salient feature of which is preserving the possibility of a negotiated political settlement, a "grand bargain" that guarantees the existing regime. Overall, then, the recent conduct of these two troublesome states suggests that while they doggedly seek the political muscle that nuclear capability affords and are willing to endure political ostracism and visit serial crises of the rest of the world to get it, they are in fact deterrable under the traditional criteria.

Soon after 9/11, analysts at the RAND Corporation, where nuclear deterrence was nurtured and refined, began talking about the susceptibility of at least some of the new terrorists to political "influence" if not deterrence in the customary sense. Their basic idea, developed in a 2002 monograph by Paul K. Davis and Brian Michael Jenkins,[1] was that since a diffuse movement like the transnational jihadist one enlists followers of myriad degrees of belief and commitment, many members will be amenable to co-optation or accommodation even if the core leadership remains maximalist and intractable. Leading academics like Mia Bloom, Farhad Khosrokhavar, and Robert Pape have also demonstrated that suicide attacks, though ostensibly senseless and desperate, are regarded by their perpetrators as the most efficacious option for the vastly weaker of two adversaries and have in fact proven to be strategically effective—particularly in the Palestinian territories and Sri Lanka. Furthermore, even those groups employing suicide attackers are subject to deterrence by punishment. Over the course of the second intifada that began in late 2000, Israel's "targeted killings" of top- and mid-level operators in Hamas and other Palestinian militant groups may correlate positively with a lower level of terrorist violence. While the suicide bombers themselves—the foot-soldiers of such groups—may be unconcerned about their physical well-being, their planners and supervisors apparently have less existential abandon and in any event remain operationally necessary for the groups to remain viable.

More broadly, in a penetrating 2005 book entitled *Deterrence*, Lawrence Freedman noted that "deterrence is ubiquitous"—neither

[1] Jenkins, Brian Michael and Paul K. Davis, *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda*, (RAND Corporation, 2002).

terrorists nor rogue states attack all the time—so there should still be a way to harness and stabilize deterrence with respect to non-state actors.[2] He and others, while admonishing that there is no magic bullet, have suggested that deterrence by denial may be the most promising approach to the new terrorism. Subtler than deterrence by punishment, the denial version—which Glenn Snyder originally distinguished in 1959—involves frustrating or obviating an adversary's political objectives such that hostile action in their pursuit will appear futile or unnecessary and be dismissed. To work against a networked and increasingly pervasive threat like that of transnational Islamist terrorism, establishing deterrence by denial is admittedly a stiff challenge: it requires the consolidation of a kind of new world order that generally does not tolerate terrorism and in which central terrorist grievances have been largely resolved. Deterrence by denial can also be achieved by frustrating terrorists' operational objectives, which calls for robust passive defenses, including border and port security, infrastructure protection, prophylaxis through vaccination and early detection, and first response.

The possibility has also been raised that even al-Qaeda's ostensibly intractable core leadership may be deterrable. Al-Qaeda's inner council, or *shura*, was divided as to whether the U.S. takedown of its Afghanistan base that would likely follow the 9/11 attacks was worth the prize. Indeed, the United States' failure to effectively retaliate for the October 2000 bombing of the USS Cole—that is, to attempt to deter by punishment—seems to have been a key factor in bin Laden's decision to go forward with the attacks. Whether recent trends reinforce or dilute the validity of that decision is unclear. On one hand, the post-Afghanistan dispersal and atomization of the global Islamist terrorist network has arguably given jihadists even less to treasure and consequently rendered them less deterrable. The spread of jihadist propaganda and urban warfare techniques via the internet has proven an effective, though perhaps not a perfect, substitute for radical madrassas and terrorist training camps.

On the other hand, operational authority and initiative have shifted to local or regional "start-up" groups like the Madrid and London culprits, and away from the core al-Qaeda leadership now besieged in the tribal areas around the Afghan-Pakistani border. As suggested by the RAND

[2] Freedman, Lawrence, *Deterrence* (Cambridge, UK: Polity Press, 2004).

analysts, some local and regional groups have more parochial and geographically circumscribed basic grievances than does Osama bin Laden himself, however much they may sympathize with his grand vision. Thus, in *International Security*, Robert F. Trager and Dessislava P. Zagorcheva recently made a solid case that some combination of deterrence by punishment and qualified local political accommodation can translate into effective global deterrence with respect to some al-Qaeda affiliates—citing, in particular, the co-optation of the MILF in the Philippines.[3] There is logic in this finding: while the frustration of political objectives at the regional and national level led bin Laden and second-in-command Ayman al-Zawahiri to globalize their fight, the partial fulfillment of comparable objectives may preclude their transnationalization.

There is, however, a rising recognition among radical Muslims of a pervasive if notional Islamic world community—the *umma*. In that light, the possibility remains that despite the flattening of the terrorist network, a sufficient number of operators of a maximalist bent—eschewing local agendas in favor of a global one—will arise to maintain the strategic threat to the United States and the West that 9/11 appeared to affirm. The received view remains that such highly-motivated terrorists cannot be permanently deterred because they value non-negotiable objectives more than their lives or other assets, but may be amenable to temporary deterrence for tactical reasons and to indirect influence. Several Western intelligence agencies do anticipate that transnational terrorists will seek a new territorial base—a chaotic Iraq would be a candidate, and Somalia remains a possible destination—and once again become susceptible to deterrence or, in any event, direct military strikes. But that vulnerability would presumably be transitory: any new sanctuary would, like the Taliban-run Afghanistan, provide the United States and its partners a casus belli, and once they destroyed it the terrorists would presumably regard dispersal and virtuality as all the more advantageous. Finding a solid basis for deterring a global network would again become a difficult challenge. Better to face that challenge now.

[3] Trager, Robert F., and Dessislava P. Zagorcheva, "Deterring Terrorism: It Can Be Done," *International Security*, 30:3 (Winter 2005/06), pp. 87-123.

What Islamist Terrorists Value

If terrorists have a stake in a relatively non-violent status quo, deterring them is feasible. The stakes on which deterrence of a state would be based include the state's territorial and political integrity, the survival of a constituent population, regime security, and a supporting industrial and military infrastructure. Terrorists, though perhaps not as obviously, value analogous aspects of a world short of outright chaos. Whether deterrence can take hold depends on whether terrorists' adversaries—in particular, the United States and its allies and partners—can credibly imperil those things so as to ensure the terrorists' substantial forbearance.

Those who count themselves terrorists or terrorist supporters increasingly regard themselves as members of the *umma*, which has no corresponding politically integrated state and hence no matching territory. Superficially, this characteristic contra-indicates the effectiveness of deterrence: with no state to defend, transnational terrorists seem to present nothing for their adversaries to hold hostage through the threat of punishment. But in a deeper sense, somewhat as the Provisional Irish Republican Army considered the entire island of Eire their state-in-waiting, jihadists regard the entire Muslim world as their caliphate in the wings. Whether jihadist leaders actually consider their stated aim of a global caliphate that reprises Islam's eleventh-century hegemony—that is, an Islamic super-republic covering much of the world—a plausible objective is open to doubt. What matters more is that they do care about other Muslims—even those who do not directly support them.

Still, turning jihadists' prudential solicitude for the welfare of their fellow Muslims into a credible tool of deterrence is problematic. Although rank-and-file Muslims do not take kindly to Muslims' killing Muslims, they are even less tolerant of Westerners' killing Muslims, so Western threats to target Muslims in general have an antagonistic rather than a deterrent effect. Iraq is a case in point. Although such threats would also be unacceptable under the laws of war—which bar the intentional military targeting of civilian non-combatants—this problem can be finessed if it is assumed, as it was during the Cold War nuclear standoff, that the deterring party does not intend to carry out the threat unless its enemy strikes (proportionately) first. But the difficulty remains that even making the threat offends Muslims and perforce risks the consequence of swelling the ranks of the jihadists. For substantially this reason, even terrorism employing weapons of mass destruction (WMD) is considered difficult to deter: the only identifiable population for the would-be deterrer to threaten would be general, and therefore would not pass the proportionality test.

In any case, fellow Muslims are not all that Islamist terrorists hold dear. As Robert Pape has shown in his book *Dying to Win*, many of them graft nationalist sentiments onto religious ones and vicariously value ostensibly Muslim territory—in particular, Saudi Arabia, Egypt, Palestine and Iraq, but also Jordan and the small Gulf Cooperation Council states—that they consider to be occupied or otherwise compromised by Western powers.[4] Pape's argument is that substantial Western disengagement from such places, under a strategy of offshore balancing, would quell the jihad. This position critically downplays the purely religious and transnational dimensions of jihadism and the universalizing effect they have had on Muslims worldwide. Yet it's hard to deny that reducing U.S. primacy in the Persian Gulf would take steam out of the jihadist narrative. To most American officials and analysts, offshore balancing is a drastic and high-risk grand strategy. But primacy is also proving to pose prohibitive risks. A strategy of moderate accommodation—such as selective engagement—could have more efficacious deterrent-by-denial impacts.

Beyond Arab lands, other geographical areas appear to be of tactical interest to the al-Qaeda leadership. In April 2004, shortly after the Madrid bombing committed by a jihadist "self-starter" cell, bin Laden released an audiotaped message implicitly claiming complicity in the attack and offering to spare European states from terrorist attacks provided they withheld operational and political support for the United States' strategic agenda. Certainly bin Laden did not seriously expect anyone overtly to accept this "offer," and it was disdainfully rejected by European capitals. Nevertheless, it made sense as part of a psychological operation designed to make them think twice about adopting a robust counter-terrorism enforcement strategy towards jihadists. Indeed, France had used a sanctuary approach against North African terrorists operating on French soil in the 1980s until its

[4] Pape, Robert A., *Dying to Win: the Strategic Logic of Suicide Terrorism*, (New York: Random House, 2005).

apparent ineffectiveness in discouraging terrorist operations caused them to reverse course.

Were al-Qaeda's gambit to work, Europe, or at least parts of it, could become an operational sanctuary for European jihadists—and, once again, a platform for launching attacks on the United States. Of course, this would not be a desirable result. But the larger point is that Islamist terrorists do have rational reasons to exempt certain areas from attack. Foreign policies well short of providing sanctuary that give the appearance of greater neutrality could deter attacks on national territories without compromising hard counter-terrorism capabilities. For example, U.S. partners might wish to publicly de-emphasize their strategic alignment with the U.S. while maintaining robust operational counter-terrorism links. In fact, that course of action describes the one France has actually taken. Unlike the UK and Spain, which have been more unabashed U.S. allies, France has not suffered a major terrorist attack since 9/11.

Jihadists are also keen to protect the integrity of their message, and to preserve the broader expectations of their supporters as well as their adversaries. Because the jihad is essentially a populist movement, the relevant audience in terms of losing or saving face consists not of states but rather of other Muslims—that is, the *umma.* Thus, in an intercepted July 2005 letter (generally considered genuine) Zawahiri, speaking for bin Laden as well as himself, importuned al-Qaeda in Mesopotamia leader Abu Musab al-Zarqawi (who died in a U.S. air strike in June 2006) to stop killing Muslims—even Shi'ite Muslims—in Iraq and publicizing the mutilation of hostages. Zawahiri's fear was that Zarqawi would alienate Muslim "common folk." He decried Zarqawi's practices not because they were morally objectionable, but because most Muslims failed to fully comprehend the bankruptcy that the leadership elite saw in Shi'ism and were repulsed by beheadings. The upshot is that al-Qaeda's leaders do rate popular acceptance on a par with religious objectives as a perpetuating element of the jihad. This reality cuts against the notion that even unwavering Islamist terrorists are fanatically implacable religious zealots.

Deterrence and Equilibrium

The central question as to deterring Islamist terrorists remains how to jeopardize their popular support. It is true that terrorists aim to revolt the general public enroute to instilling fear, so that up to a point public opprobrium only furthers their agenda. But when such condemnation is shared by the terrorists' notional constituency, they are vulnerable to deterrence. To deter them, their adversaries must win over their constituents in the *umma*. This conclusion, of course, is analytically just another way of saying that the United States and the West must win the battle for hearts and minds. But that campaign has generally been presented as an alternative to deterrence rather than an application of it. It is more useful to think of it as the latter.

Israeli military historian Martin Van Creveld has famously noted that when strong states confront terrorists with brute force, they are bound to lose in the long run. "He who fights against the weak—and the rag-tag Iraqi militias are very weak indeed—and loses, loses. He who fights against the weak and wins also loses. To kill an opponent who is much weaker than yourself is unnecessary and therefore cruel; to let that opponent kill you is unnecessary and therefore foolish."[5] This formulation confirms that deterrence by threat of punishment *vis-à-vis* terrorists will be unavailing—not because of their recalcitrance, but because of political advantage that accrues to their weakness. For the same reason, it also indicates that military pre-emption may ultimately be futile. Deterrence by denial, very broadly construed, emerges as the best option.

Following Van Creveld, its essential component would be the willingness of al-Qaeda's adversaries to accept a substantially greater number of casualties than it visited on al-Qaeda and its affiliates. Arguably, this worked for the British against the IRA. Enduring multiples more in casualties—military and civilian—than did the IRA and its putative constituency, the United Kingdom was eventually able to reach a modus vivendi with the IRA with its honor and status as a great power more or less intact. It accomplished this by approaching counter-terrorism as a function mainly of law enforcement and political engagement rather than military coercion. Although the UK deployed

[5] Van Creveld, Martin, "Why Iraq Will End as Vietnam Did," November 18, 2004. Available at: http://www.lewrockwell.com/orig5/crevald1.html.

up to 30,000 soldiers in Northern Ireland, their function was primarily to deter civil war rather than terrorism per se. About five years into the 25-year conflict, in 1976, the Northern Irish police were given primary counter-terrorism authority, and terrorist offenses were statutorily accorded criminal as opposed to political status and terrorist prisoners officially treated as ordinary inmates.

It is true that the IRA resisted criminalization, and won a degree of credibility by way of the prison blanket protest and the 1981 hunger strikes, which also increased popular backing for Sinn Fein, the IRA's legal political wing. Nevertheless, in the long term the British approach effectively denied the IRA the ability to indoctrinate a sufficient number of its supporters, both within and outside of Northern Ireland, to prevail in its "armed struggle." Throughout "the troubles," the Social Democratic and Labour Party—"constitutional" nationalists who believed that Ireland should be united only through non-violent political means—enjoyed more than double Sinn Fein's popular support in Northern Ireland. Only after the IRA declared a cease-fire in 1994 and chose a largely non-violent political path was Sinn Fein able to build the electoral base to become the strongest Irish nationalist party and draw determinative political support from major outside players such as the United States.

For the current global campaign against Islamist terrorism, the lesson is that military action designed to defeat al-Qaeda and its followers, even if tactically successful, is likely to be strategically disappointing. No matter how many jihadists are killed on the battlefield, at least as many will be sufficiently inspired by the aggression of the infidel (or its apostate Muslim proxy) to take up the struggle. Just such a vicious cycle appears to have been triggered by U.S. intervention in Iraq, and might be replicated in miniature by Ethiopia's American-backed intervention against Islamists in Somalia. The antidote, to be sure, is not for the United States and its partners to be passive in war and take casualties profligately—that too would fuel recruitment—but rather to avoid war against Islamists when possible.

As to how to deter terrorists, then, the central analytic quandary becomes whether what they value can be politically threatened more by physically endangering it less. The fact that they feed on the perceived oppression of strong states suggests that the answer is yes: if, conversely, they are denied that oppression, they may become politically starved.

Like bin Laden before him, Zarqawi became the jihad's most charismatic player by surviving the American military onslaught in Iraq and adding to that insult by killing Americans. He personified the manner in which the United States perversely handed al-Qaeda a new and potent grievance and made it less rather than more deterrable. As Charles D. Ferguson and William C. Potter suggest in *The Four Faces of Nuclear Terrorism*, the Madrid bombers might not be as willing as core al-Qaeda leaders to kill 200,000 rather than 200, and "old" style ethno-nationalist terrorists or single-issue groups certainly would not be given their desire, respectively, to preserve political options or focus public attention on a finite set of perceived culprits.[6] Both political liabilities and anticipated retaliation appeared to play a part in the Chechen rebels' decision not to detonate a dirty bomb in 1995. More generally, extreme operational objectives—insofar as they would inspire extreme response—may discourage recruitment.

As the global jihad disperses, it logically has to rely more on numbers and pervasiveness and less on command and control. While Ferguson and Potter make the point that nuclear capability would bring a terrorist organization closer to statehood, the post-Afghanistan trend appears to be for jihadist organizations to regard territorial cohesion as a defensive liability. This disposition, however, could change not only if jihadists come to possess WMD but also, more benignly, if they encounter greater political success within Islam. Greater political legitimacy would render the physical reconstitution of radical Islamism more justifiable, and any coercive attempt to dislodge it proportionately less justifiable. This incentive would probably, on balance, make Islamist leaders favor the establishment of some form of state. By the same token, to retain a sufficient degree of legitimacy to protect that state from attack by a threatened government, any Islamist leadership would have to exercise considerable military restraint. Operations like 9/11 obviously would still constitute grounds for war, and demonstrable operational (as opposed, say, to merely financial) sponsorship of insurgencies or start-up terrorist groups would at least provide adversaries with a prima facie case for the responsive use of force.

[6] Ferguson, Charles D. and William C. Potter, Amy Sands, Leonard S. Spector, Fred L. Wehling, *The Four Faces of Nuclear Terrorism* (Monterey, CA: Center for Nonproliferation Studies, 2004).

Having both experienced the United States' willingness to destroy the Taliban regime in Afghanistan and registered the political cost of the United States' excess in Iraq, the Islamist leadership might be deterred from launching mass-casualty attacks against Western targets and inclined to relinquish the initiative to use large-scale force to its putative adversaries. The result would be, in brief, a new equilibrium in which each side sought to sustain its political legitimacy by advancing its ideology with a minimum of force. In this new cold war, radical Islamists would behave more like the African-American civil rights leaders of the 1960s than the al-Qaeda of the past decade. Though doubtless a few analogs to the Black Panthers would emerge, concern for legitimacy would make the new incarnation of Islamism disinclined to put its reputation for action in defense of interests and constituents at undue risk. That would mean avoiding over-commitment—that is, resisting anything resembling a public vow that it is not likely to be capable of fulfilling. Whereas a big part of the old al-Qaeda's political arsenal was lurid and sensationalistic rhetoric—for example, spokesman Suleiman Abu Ghaith's oft-quoted proclamation that four million Americans would have to die before the United States were ripe for mass conversion to Islam—the fanciful grandiosity of such statements would disfavor them in the new situation. Their suppression, in turn, would tend to diminish recruitment and stabilize the confrontation between Islamism and secularism.

Appreciating Hezbollah

Under this scenario, deterrence would obtain not in any pure univalent form, but as an indeterminate and shifting combination of deterrence by punishment, deterrence by denial, and self-deterrence—as it did during the first cold war. The implicit strategy of encouraging the political legitimacy of Islamism and its constitution in state-like forms seems, at first blush, counter-intuitive to say the least. Why would we want to promote a religious ideology that has heretofore counseled the destruction of our own state structures, political systems, and cultures? The answer is to furnish its leaders with something tangible to value—and, therefore, to threaten. Paradoxical as this formulation may sound, it is no more so than deterrence itself, which aims to maintain peace by promising destruction.

The slow—and as yet incomplete—evolution of the militant Shi'ite group Hezbollah from an unregenerate anti-Israeli terrorist group into a powerful and substantially legitimate political player in Lebanon is a case in point. Having enjoyed electoral success for several years, Hezbollah in 2006 entered into a political alliance with more mainstream Druze and Christian parties because, with Syria ousted from Lebanon, Hezbollah needed new political cover for its stance of resistance to Israel. Although Hezbollah still sporadically harasses Israel with small-scale attacks, a kind of equilibrium has been reached. Absent provocation—which of course Israel did provide in the summer of 2006—Hezbollah's wholesale return to violence would give rise to substantial opposition among its coalition partners, such that its political viability in the new Lebanon would be in jeopardy. Hezbollah admittedly does not have strong incentives for disarming, and may be content with accepting the patronage of its partners in exchange for their endorsement of its armed status. At the same time, its freedom to return to large-scale violence is limited because doing so would mean forsaking a large measure of its hard-won political clout.

The general formula for establishing similar foundations for deterrence elsewhere is the United States' exercise of political tolerance on a global scale to an extent that has been unthinkable since 9/11. Granted, the programmatic solution to the problem of extirpating terrorism's root causes has been to institutionalize tolerance writ large by establishing or enhancing democracy and individual liberties in the Greater Middle East. But the accompanying factual assumption has been that liberal democracies discourage radicalism and political violence, and that their creation would simply diminish the threat of terrorism rather than make it more deterrable. This view almost certainly would not be borne out in a number of key countries. The belated recognition of this reality—spurred by frustrated efforts of the United States to build a liberal pluralistic state in Iraq—has prompted the U.S. government to acknowledge that the exportation of democracy under the Bush doctrine must proceed more slowly, gently and selectively than originally hoped in 2003. But illiberal regimes, the thinking runs, must remain secure in places like Egypt lest Islamists gain decisive political power and reject U.S. and broader Western influence.

Proactively organizing the dismantling of such governments would indeed be imprudent, in that it could undermine crucial bilateral American relationships or produce traumatic shocks that might touch off wider violence and instability. Passively allowing Islamists to non-violently gain political legitimacy at the national level, however, might yield them a concrete position in an existing polity that they would be loath to jeopardize through transnational jihadist violence. The political success of Hezbollah within Lebanon has quite clearly dimmed any out-of-area ambitions it may have had and tamped down extra-territorial terrorist operations, and Hamas's victory in the Palestinian Authority elections has rendered it less rather than more likely to make tactical alliances with al-Qaeda or its affiliates. Partially fulfilled Islamists like Hezbollah and Hamas would be easier to manage—and perhaps eventually to influence and co-opt. More immediately, they would be deterred from transnationalizing political violence and striking American territory.

Chapter 4

Criminal and Terrorist Networks: Gauging Interaction and the Resultant Impact on Counter-Terrorism

Tamara Makarenko

The connection between crime and terrorism is identified and measured along two lines of interaction: the first is focused on *crime* and *terrorism* as concepts defined within specific definitional parameters; whereas the second concentrates on crime and terrorism as distinctly identifiable non-state actors which challenge security on all levels of analysis through their actions. Although these two lines of interaction can be separated to ease enquiry and provide explanatory clarity, the relationship between crime and terrorism exists along a dynamic continuum which plots the organizational and operational interaction between both phenomena. Thus crime and terrorism as concept and entities cross-over on several analytical planes: first, through the creation of alliances between distinct entities; second, through the operational use of terror tactics by a criminal group or criminal tactics by a terrorist group; and third, through the convergence of criminal and terrorist tactics within a single group, thus creating a hybrid entity. The notion that crime and terrorism exist along a continuum is used to illustrate the fact that, in addition to situations of cooperation between a criminal and terrorist group, a single group can slide across a definitional scale between what is traditionally referred to as *organized crime* and *terrorism* depending on the environment in which it operates.[1]

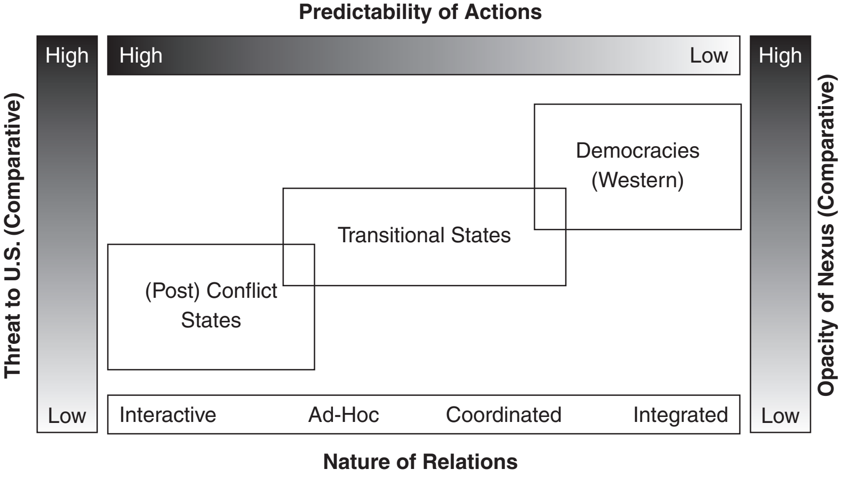
[1] The notion of a convergence between organized crime and terrorism was first published by Tamara Makarenko, see: "Crime and Terrorism in Central Asia," *Jane's Intelligence Review*, 12:7 (July 2000). The crime-terror continuum as an aid to understanding the interaction between organized crime and terrorism was subsequently developed in greater detail in the following: "Transnational Crime and its Evolving Links to Terrorism and Instability," *Jane's Intelligence Review*, 13:11 (November 2001); "A Model of Terrorist-Criminal Relationships," *Jane's Intelligence Review*, 15:8 (August 2003); "Transnational Crime and Terrorism: the Emerging Nexus," in Smith, Paul, ed., *Transnational Violence and Seams of Lawlessness in the Asia-Pacific*, (Armonk, NY: M.E. Sharpe, 2004); and, "Terrorism and Organized Crime," in Galeotti, Mark, ed., *Global Crime: the Changing Face of the Modern Underworld*, (London: Frank Cass Publishers, 2004).

Although understanding the dynamic nature between *crime* and *terrorism* within the context of the crime-terror continuum provides insight into the overlap of these two concepts, it is the actual interaction between *crime* and *terrorism* as distinct entities which will frame the discussion of this paper. Since 9/11 it has become widely accepted that terrorist groups engage in criminal activities as an operational tactic used to both secure financing and to manipulate established criminal processes to access materials and know-how. As such, arguing that terrorists engage in criminal activity is a pedantic exercise. The notion, however, that criminal and terrorist groups collaborate is an observation that requires greater attention; especially given common reticence within the academic community to consider arguments which go contrary to the widely accepted view that criminal and terrorist groups have no interest in cooperating because any interaction is faced with inherent risks associated with trust, loyalty, divergent views on the necessity of the state, and transaction costs which naturally increases vulnerability of both sides to the authorities. It can thus be argued that dissecting the interaction between criminal and terrorist groups carries the potential of providing further insight into the actual crime-terror continuum, while also highlighting deficiencies in the current strategic focus of counter-terrorism.

Identifying Points of Interaction

The nature of a relationship between a criminal and terrorist group varies in terms of longevity and depth. They range between the ad hoc (i.e. one point in time) to longer-term strategic alliances; and, are formed for a variety of reasons such as seeking expert knowledge (i.e. money-laundering, counterfeiting, or bomb-making) and/or operational support (i.e. access to smuggling routes and safe havens). In theory cooperation potentially provides significant benefits for both parties involved, including everything from access to previously unobtainable know-how and materials, to the destabilization of political structures (i.e. through corruption and violence) and international counter-terrorism or anti-crime policies through the undermining of trust between state actors. Regardless of the country which hosts a crime-terror connection, mapping the associated dynamics and resultant implications of such interaction often reveals a network that extends from an international to community context. Thus in a policy context,

Figure 1: Interaction in Unstable Environments



the existence of any crime-terror connection merely highlights the fact that law enforcement, homeland security and national security are intrinsically linked together.

In assessing the interaction between criminal and terrorist groups, the available evidence indicates that the depth of collaboration is most often dependent on the nature of the geographic region in which these relations are established. As illustrated in Figure 1, relations in Western democracies are often based on sympathetic feelings which can emerge from loyalties to specific ethnic or religious communities, or it can be established through converts. Relations in transitional states are most accurately described as ad hoc because they are predominantly based on fulfilling immediate operational needs; and, relations which emerge within (post) conflict societies tend to be the ones that are most developed and interactive. In conflict-ridden and conflict-prone environments, the maintenance of instability is in the interest of terrorists because it diminishes the legitimacy of governments in the eyes of the mass populations—the very people terrorists seek to gain support from; and it is in the interest of criminal groups who have learned how to maximize profits within this context. For this reason, the relationship between criminal and terrorist networks are most developed and prevalent in South America, Southeast Asia, the Middle East and Eurasia; however, they are potentially most dangerous in

North America and Western Europe precisely because these ties are less transparent and more adaptive.

Criminal and terrorist networks which have emerged from a state of perpetual conflict and instability blatantly reveal the ultimate danger of the crime-terror connection to international security. Operating within de facto 'safe havens' for illicit operations, weak and failed states foster nefarious collaboration, which subsequently seeks to perpetuate a condition of civil (or regional) war to secure economic and political power. At an extreme end, this is reflected in the conditions of Afghanistan, Angola, Myanmar, Sierra Leone, Tajikistan, and confined territories in Pakistan, Indonesia and Thailand where government control is extremely weak, if existent at all. Although unstable, but not necessarily classified as failed states, conditions in many South American and African states also fall within this category when assessments of relations between criminal and terrorist networks are concerned. In most of these situations conflict/war has provided "legitimation for various criminal forms of private aggrandizement while at the same time these are necessary sources of revenue in order to sustain the war. The warring parties need more or less permanent conflict both to reproduce their positions of power and for access to resources."[2]

Conflict that besets the interaction between criminal and terrorist networks share several common characteristics. To begin with, these conflicts usually have no clear military objective and lack political order. Instead, military units constitute "little more than marauding bands acting quite independently" and "showing no discipline whatsoever in the actions they were committing."[3] Furthermore, it is evident that the perpetuation of conflict, as opposed to victory, becomes a priority in order to create ideal conditions for criminal activities to flourish[4] amongst groups equally motivated by the "accumulation of wealth, control of territory and people, freedom of movement and action, and legitimacy. Together, these elements represent usable power—power

[2] Kaldor, Mary, *Old and New Wars: Organized Violence in a Global Era* (Stanford, CA: Stanford University Press, 1999), p. 110.

[3] Snow, Donald M., *Uncivil Wars: International Security and the New Internal Conflicts* (Boulder, CO: Lynne Rienner Publishers, 1996).

[4] Berdal, Mats and Mónica Serrano, "Transnational Organized Crime and International Security: The New Topography." In Berdal, Mats and Mónica Serrano, eds., *Transnational Organized Crime and International Security: Business As Usual?* (London: Lynne Rienner Publishers, 2002), pp. 197-207.

to allocate values and resources in society."[5] Unlike traditional organized crime, epitomized by the established hierarchical groups such as the Japanese Yakuza, which is dependent on the international financial system and state stability, criminal networks which grew from within unstable environments have no innate loyalty to the state. As a result, the risk calculations which are made prior to engaging with known terrorist networks are extremely open, based more on fulfilling immediate benefits rather than assessing long-term repercussions.

Alliances between criminal and terrorist groups in environments characterized by perpetual instability emerged as early as the 1980s in very specific cases that saw both groups benefit from such a relationship. The first such documented alliances were created in Latin America between terrorist groups such as Colombia's FARC and the Shining Path of Peru, and the infamous drug cartels (i.e. Cali and Medellin). In exchange for securing drug laboratories and airstrips, the terrorist groups collected a local tax from the drug trade. Relations between criminal and terrorist groups in South America evolved over the years, from the Medellin cocaine cartel allegedly hiring the ELN to plant car bombs in 1993,[6] to FARC increasingly taking control over cocaine trafficking operations after the demise of the Cali and Medellin cartels and using cocaine as currency for arms shipments supplied by criminal groups in Mexico[7] and Russia.[8] Although South America is no longer characterized as an unstable environment; pockets of sustained instability, especially in the case of Colombia, set a worthwhile historical precedent against which contemporary examples could be compared.

[5] Manwaring, Max, *Grey Area Phenomenon: Confronting the New World Disorder* (Boulder, CO: Westview Press, 1993). (1993), pp. 7-8.

[6] Clawson, Patrick and Rensselaer Lee, *The Andean Cocaine Industry*, (New York: St. Martin's Press, 1996), p. 53.

[7] "Colombian Rebel Connections to Mexican Drug Cartel," Statement by Richard Boucher, Spokesman for the U.S. Department of State, (November 29, 2000). Available at: http://www.fas.org/irp/news/2000/11/irp-001129-col.htm; Luis Gutierrez Esparza, "La Mafia Rusa en Mexico," *Memorando*, (July 29, 2001). Available at: http://latamcent.org.mx; and, *Organized Crime and Terrorist Activity in Mexico, 1999-2002*, A Report Prepared under an Interagency Agreement by the Federal Research Division, Library of Congress (February 2003); Sam Logan, "Organized Crime, Mexico's Top Threat," *ISN Security Watch* (26 April 2006).

[8] Seper, Jerry, "Mexicans, Russian Mob New Partners in Crime," *The Washington Times*, (August 20, 2001); "Peru: a Spy Story Replete with Arms, Drugs-Dealers and Bears," CNN, (September 8, 2000); and, "Farclandia," a discussion of narco-states, cited in the transnational crime section of the Centre for the Study of International Security website (Washington, DC). Available at: http://www.csis.org.

South America, however, is not a unique case study; on the contrary, other regions provide equally illustrative examples of how crime and terror naturally relate in environments characterized by sustained conflict or perpetual political instability. For example, a similar situation existed in South and Southeast Asia during the 1980s when the Liberation Tigers of Tamil Eelam (LTTE) established ties with the Indian mafia[9] to sell illicit narcotics in exchange for arms. Such relations have existed with criminal groups based in Pakistan and Burma; and groups based throughout South/Central Asia who have provided the LTTE access weapons, training, established smuggling routes and corrupt relations which were used to facilitate the movement of human cargo and narcotics. Other Indian and Pakistani-based criminal groups have also been implicated in 'exchange' relationships with al-Qaeda and Laskhar e-Tayyaba. Similar relations with regional criminal networks also exist amongst the myriad of groups operating in Thailand,[10] and the Indonesian conflict zones of Aceh, Sulawesi and Maluku[11]—with the specific intent of arming terrorist groups.

The most debilitating case for international counter-terrorism initiatives, including those led by the U.S., relates to the persistence of ties between criminal and terrorist networks in Afghanistan. The persistence and evolution of crime-terror collaboration in the face of Coalition forces engaged in counter-terrorism and reconstruction efforts has contributed to sustained instability and an inability of the Coalition forces to make inroads in winning the hearts and minds of the local populations. This has been further exacerbated by the confusion with which the various military missions have been characterized and the Taliban's shifting frontline (i.e. marked by territorial gains and propaganda successes). In this rather complex environment, criminal and terrorist networks have managed not only to maintain their hold over the highly profitable narcotics trade, but they have also evolved the trafficking process into networks which have become increasingly organized and sophisticated in nature. Furthermore, these networks have been facilitated and secured as a result of the importance the

[9] This alliance is discussed in Kshitij Prabha, "Narco-Terrorism and India's Security," *Strategic Analysis*, vol. 24, no. 10 (January 2001).

[10] For comprehensive assessments of these relations, see the work of Anthony Davis published in *Jane's Intelligence Review* between 2002 and 2007.

[11] These allegations were first uncovered by Davis, Anthony, "The Complexities of Unrest in Southern Thailand," *Jane's Intelligence Review*, 14, 9 (September 2002).

drug mafias placed on creating a highly corrupt and conducive government apparatus. Conservative estimates by the U.N. indicate that at least a quarter of the Afghan parliament is involved in the drugs trade, a figure which does not take into consideration the collusion of provincial governors and law enforcement.

Regardless of the Coalitions' focus on eliminating the Taliban and all al-Qaeda remnants in Afghanistan, the existence of a crime-terror nexus inherently undermines any such efforts—least of which because it is politically difficult to explain why it is that senior Afghan government officials are engaged in the very trade which is funding the resurgence of the Taliban and other region groups including the Islamic Movement of Uzbekistan and the East Turkestan Islamic Movement. Furthermore, the same product which continues to finance regional terrorism can arguably still be connected to a centralized recruitment and training base for militants in the Pakistani Tribal areas who have interests in bringing their knowledge to support operations in Western Europe and the U.S. Although the flow of narcotics trafficked from Afghanistan to Pakistan has dissipated in favor of the Northern and Balkan trafficking routes, the fact that three of six key transhipment hubs for Afghan opium and heroin are located in Pakistan (Peshawar, Quetta and Karachi) is significant. The other three are located in Kyrgyzstan (around Osh), and in Iran (around Zahedan and Mashhad)[12]—ultimately using West African, Caucasian, Central Asia, Turkish, Kurdish and Albanian criminal networks to bring narcotics shipments to destinations throughout Eurasia and Europe.

Without considering the complexities which the growing interaction between criminal and terrorist networks in Africa pose to current counter-terrorism initiatives, the South American and South Asian cases are indicative of the blurring lines between homeland and national security. In both cases, attempts made by the U.S. to increase its national security have produced increased threats from terrorism against the U.S. and U.S. interests. In spite of efforts to support Colombia in eradicating coca and eliminating insurgent groups, the interaction between crime and terrorism around the cocaine trade has produced 'back doors' through which foreign-based terrorists could feasibly manipulate to either penetrate the U.S. with operatives, or

[12] Based on confidential discussions with UN personnel.

support cells already entrenched within American society. This is replicated in Afghanistan, where despite U.S. efforts to eliminate terrorist bases, the networks used to traffic opiates to the West are the same networks which could be manipulated by terrorists seeking retribution by targeting U.S. interests in the region and by feeding global anti-American sentiment through propaganda drives which are, in part, supported through drug profits.

Interaction in Transitional States

Transitional states, generally incorporating the former Soviet Union, parts of Eastern Europe, the Americas and the Middle East, provide a different context in which criminal and terrorist networks engage with one another. Unlike criminal and terrorist groups engaged in conflict and post-conflict societies the nexus in transitional states is not necessarily about perpetuating instability, but about maximizing the chances of success for immediate operations. In this environment, illicit actors—regardless if they are characterized as criminals, terrorists or insurgents—have a driving interest in profit maximization as the route to ensure their survival. This is a motivation which is facilitated by poor border security, weak law enforcement, corrupt public officials, and established smuggling networks. As such, transitional states are most often used to provide exchanges of goods, access to established smuggling routes and/or expertise. Interaction thus predominantly follows the trade in high value illicit commodities, such as narcotics and arms.

The former Soviet Union, for example, provided black market access to an arsenal of weaponry (including chemical, biological and radiological materials). In the 1990s their were fears cited by Western governments and academics that these materials could be directed to terrorist groups. Although fears regarding the trade in chemical, biological and radiological materials have been sustained through the years, it is the trade in Soviet-sourced arms on the black market that has proven to be difficult to disrupt. Controlled, in most contexts, by major international arms dealers, terrorists have yet to become a notable direct client of the black arms market. Although an ideological argument could be formed to explain why arms dealers tend not to directly source terrorist groups, the reality is that international arms dealers are not interested in terrorist groups because they generally purchase in small quantities. As a result, terrorist networks interested in acquiring weapons or related materials are reliant, at least in many transitional states, on criminal networks or individual intermediaries who have established relations to the market gatekeepers. This appears to have been the case in 2005 when Italian authorities uncovered an extensive arms trafficking network that supplied known Islamist militants. The ring supplied weapons through a network established between Bosnian criminals and the Camorra, the latter of which simultaneously sought to help the militants enter Europe clandestinely and provide them with arms and explosives.

One of the regions most vulnerable to smuggling of radiological material, more specifically, is the Caucasus where criminal networks have evolved to incorporate relations between state officials, business interests, and terrorist groups. In fact, during investigations into criminal groups operating in the breakaway republics of Abkhazia and South Ossetia in 2005, Georgian authorities uncovered several smuggling networks which were found to support the transit of numerous goods, including radiological materials. With the support of the U.S., a sting operation was orchestrated in February 2006 in which 'buyers' were sent to the breakaway regions. Although no known terrorist interests were implicated in this operation, the fact that orphan and unsecured radiological materials could be accessed confirms the position cited by the FBI in 2005 after they broke up a criminal network planning shipments of various weapons—including a claim of enriched uranium—from Armenia, Chechnya, Georgia or Ukraine to the U.S. At the time, an FBI representative posited that "these individuals may not have been terrorists themselves, but they have showed transparent willingness to do anything with anybody, so long as it generates money for their organization."[13]

The interest of criminal networks in transitional states to maximize profits has also been mirrored in South America; with South American authorities repeatedly expressing concerns regarding the willingness of criminal groups to provide services for foreign-based terrorist groups. For example, since 2005 reports have noted that Mexican and Peruvian groups—with no identifiable state or social allegiance—have attempted to specialize in establishing smuggling rings that trafficked Middle Easterners into the U.S. Concerns emerged when individuals

[13] Discussions with Aleksandr Kupatadze, April 2007.

with alleged ties to militant Islamist groups sought to become involved in these structures.[14] Human smuggling rings with the ability to facilitate the entry of militants into the U.S. were further highlighted with the discovery of a Colombian false-passport ring which involved Colombian nationals and foreign nationals with ties to Jordan and the Palestinian territories.[15] Although it is most likely that the false passports supplied by this criminal network went predominantly to Colombian-based groups such as FARC, the concern does highlight an inherent vulnerability for the U.S. which continues to emanate from its southern neighbors—a vulnerability not only to the various perils of the cocaine trade itself, but from the willingness of groups controlling narcotics smuggling routes to use that control for the benefit (knowingly or unknowingly) of terrorist financing or operations.

Despite the experiences of the regions noted in this section, and support provided by the U.S. government to help strengthen anti-crime and counter-terrorism initiatives, the connections between crime and terror persist. Unfortunately these connections are, in many states, enhanced by the inability to curtail corruption or assert government legitimacy and authority throughout the state. Long histories of political instability, mistrust in bureaucracy and state institutions, have created environments in which people are generally driven by concerns over securing the present, as opposed to concerns regarding the implications of their actions for the future. The cycle which results thus makes stability elusive, and in fact feeds into instability both internally and regionally.

Thus in the case of Colombia, for example, despite all the money channeled through Plan Colombia, the country remains a faltering state that sporadically feeds into regional instability through the relations established between FARC and the Colombian paramilitaries (i.e. AUC) and regional criminal groups to move narcotics to the U.S. and European markets. The continued existence of a narcotics economy and culture within South America will indefinitely undermine the creation of a functioning political system which is not itself implicated in corruption associated with securing, and thus perpetuating, the crime-terror nexus. And in each example cited above, the flawed nature of

[14] These concerns were presented in a succinct analysis provided by the *Jamestown Terrorism Monitor*, 3:22 (November 17, 2005).

[15] "U.S. seeks 8 tied to passport ring," *Associated Press* (January 27, 2006).

national security programs implemented by the U.S. are highlighted in the inherent threats posed to U.S. homeland security through the existence of smuggling networks which, for the right price, can be readily manipulated by terrorist interests.

Interaction in Western Democracies

Connections between criminal and terrorist groups are most readily identifiable in environments characterized by some degree of instability—be it in a state of outright conflict, or suffering from entrenched corruption which fuels the rise of criminal enterprise. In these environments not only is the existence of criminal and terrorist networks expected, but their interaction seems natural—even if only ad hoc in nature. Identifying the connection between criminal and terrorist networks in Western democracies, however, is significantly more complex. To begin with, these societies pose a host of obstacles to illicit operations, making internal group trust and loyalty more sensitive issues. Furthermore, there is a natural ideological divide between criminal and terrorist networks; highlighted by the fact that criminal groups successfully operating in the West have no interest in destroying the fabric of the society from which they prosper. As such, of all types of societies, the crime-terror nexus seems most unwelcome, and thus most unlikely, in Western democracies.

The notion of a connection between criminal and terrorist networks emerging in Western democracies, however, should not be entirely discarded. On the contrary, in addition to monitoring potential avenues of terrorist financing, there is a need to simultaneously monitor points where a potential relationship between crime and terror would be feasible. This is not entirely a scenario-building exercise, but is in fact based on evidence and concerns emanating from completed and ongoing counter-terrorism investigations. For example, in 2002 Italian authorities noted that criminal and terrorist cells were engaged in a reciprocal relationship wherein Italian criminal groups smuggled arms to Palestinian and North African groups in exchange for supporting Italian narcotics smuggling networks. That same year allegations regarding cooperation between the 'Ndrangheta and militant cells based in Italy also emerged, and in 2004 Italian authorities noted concerns regarding Neopolitan mafia converts establishing an arms-for-drugs network on behalf of Italian based terrorist cells. The integration of these ‘types’ of individuals came to a head in 2004 when, following the Madrid attack (3/11), Spanish authorities discovered that drug traffickers were radicalized and integrated into the terrorist cell responsible—thus adding contacts and skill-sets required for successful preparation. A year later, French authorities dismantled an ‘illicit network’ in 2005 which consisted of several individuals including known militants, radicalized delinquents and common criminals.

The driver behind the cases of crime-terror interaction noted above is not believed to be profit-maximization or a desire to secure an unstable operating environment. These connections appear to be based on a more complex equation, combining factors such as loyalties to a specific ethnic or religious community, or the emergence of sympathetic feelings by the criminal/terrorist network—feelings often reflected in converts. These trends appear to be consistent throughout North America and Western Europe, and are most relevant in the context of radicalization and conversion of criminals within prison systems, as was the case with Jose Padilla, John Walker Lindh and Richard Reid. In fact, France, the U.S. and the UK have all admitted that their prisons systems are vulnerable to charismatic radical Islamist leaders inspiring prisoners to join the *global jihad*. The problem of radicalization in respect to the U.S. was succinctly established in a study by George Washington University[16] which identified four main radicalization processes: individual, organized, gang and para-radicalization. Potentially the most problematic in terms of the crime-terror nexus are gang radicalization and para-radicalization. In the former pre-existing prison gangs are exploited to attract converts (thus taking advantage of an established system of trust and loyalty), and para-radicalization referring to a situation when non-radicalized individuals aid radicalized networks. Thus in addition to creating an inherent ‘home-grown’ terrorist threat, the interaction within prison systems also provides terrorist cells in Western democracies with access to the know-how required to conduct criminal activities which remain below the radar of law enforcement because they are naturally high volume and low cost (i.e. various types of fraud and petty crimes).

[16] George Washington University and the Critical Incident Analysis Group, *Out of the Shadows: Getting Ahead of Prisoner Radicalization*, (2006).

Policy Recommendations

Although caution must accompany any assessment focused on identifying points of interaction between very distinct groups, it would be naïve—in the face of solid examples—to conclude that it is not in the interest of criminal and terrorist groups to cooperate. By quoting traditional understandings of motivation and internal aversion to risk as justification for crime and terrorism not to cooperate, merely supports current counter-terrorism policies. After six years of implementation these policies have not significantly altered the terrorist risk environment. In fact, it is through the strategies implemented by Western democracies in their desire for national security that the risks to homeland security are ironically increasing. Although there are numerous examples where this is the case, the most illustrative is evident in debates regarding radicalization of individuals not only throughout the world, but also throughout the Western world. As such, it may be argued that the policies our own governments adopt to enforce security and stability in the international system are having a boomerang effect which can no longer be ignored.

Counter-terrorism is naturally a complex phenomenon which naturally takes time to perfect in environments, and against adversaries, which are by nature flexible and adaptive. However, instead of seeking to entrench our approach to counter-terrorism, the only way to meet the threat as it is evolving, is to ensure that counter-terrorism is itself innately flexible and adaptive. Unfortunately this naturally goes against the way security and defense have been organized in the West. Recommendations therefore need to combine central coordination with the need for specialized agencies to take the lead in identifying, monitoring, and securing the vulnerabilities and gaps within their areas of responsibility. In relation to the interaction between crime and terrorism, this has several implications for counter-terrorism strategy. Using the '5Ds' approach to counter-terrorism, the following are some key recommendations for integrating the threat of a crime-terror nexus into U.S. initiatives:

Deterrence

In theory, the notion of deterrence should be an effective tool which can be employed against states in which the threat from an interaction between crime and terrorism could be detrimental to the security of the U.S. Unfortunately, deterrence is most likely to work in a context in which the target has something to lose—as such, deterrence has historically been successfully employed between state actors, and thus has limited value to non-state actors in unstable and transitional environments, who do not necessarily guide their actions according to our understanding of how a rational state would. Although deterrence is employed on a state level in relation to counter-terrorism, it is ineffectual when pitted against governments which are unable to exert control throughout their territory. Deterrence as a counter-terrorism tool should thus be focused on the contexts in which it is most likely to contribute to an overall strategy: such as on a sub-national level within the U.S. In other words, deterrence could be integrated within a Criminal Justice strategy focused on discouraging prison radicalization, or engaging in document or banking fraud.

Dissuasion

Dissuasion is a policy approach which has not been adequately integrated within counter-terrorism strategies despite its importance in relation to winning the hearts and minds of individuals who may be considered vulnerable to radicalization. As a form of communication focused on influencing a target towards a certain action or inaction through logic or reason, dissuasion highlights the need—especially in relation to circumventing militant Islamist arguments—to enter into a dialogue which does not present issues in black and white, but articulates the complexities and realities of the 'gray'. For example, dissuasion can be used to build a moral argument to the banking sector that it is essential for them to disclose all fraud-related losses to the authorities because fraud is not only a problem of criminality, but fraud provides a natural point of confluence between crime and terrorism. Thus banks could be more willing to share information with the authorities in the knowledge that they may be providing important intelligence. Dissuasion is therefore a strategic tool that can be implemented from a community to federal level, benefiting intelligence-led policing and intelligence-led diplomacy when foreign-based actors are involved.

Denial

In relation to the interaction between crime and terrorism, denial as a strategy presents a catch-22 situation. Although the importance of blocking criminal opportunities is important in both the context of anti-crime and counter-terrorism, the ability to identify crimes which are of interest to both criminal and terrorist networks provides an invaluable intelligence tool. Thus prior to implementing a policy of denial, it is essential to use knowledge of crime-terror interaction to collect more insight regarding organizational design of both groups, including the fundamentals of the acquisition and movement of criminal financing. Such knowledge not only contributes to the building of solid cases for prosecution services, but it also helps develop adaptive forecasting models which allows law enforcement and the security services to focus their resources.

Diplomacy

As with deterrence, diplomacy is a tool which, in a traditional setting, works best when it involves defined state actors. However, diplomacy has been evolving to meet the challenges of the contemporary system, and has application to counter-terrorism when it is conceptualized as a tool that supports the responsible and accountable management of world politics and global interdependence. In the context of the crime-terror nexus, diplomacy is a tool that could be effectively used to (a) initiate and maintain dialogue between stakeholders who have an interest in reducing the opportunities for criminal and terrorist networks to collaborate, and (b) collect and distribute intelligence from/to stakeholders with an ability to contribute to the identification and disruption of criminal-terrorism ties. In other words, there is a need to be creative with diplomacy in a counter-terrorism context, moving away from a reliance on the state system to engage actors with the ability to alter the environment in which they operate (i.e. international business). This is especially true in unstable environments and states who do not exert authority or control throughout their territory.

Defense

Although defense is accepted as an integral component of counter-terrorism, it can not be treated as the a priori approach to national or homeland security when dealing with adversaries who are not easily identifiable. Furthermore, although in theory defense operations can secure an unstable situation, the strategy that guides operational and tactical decisions must be well defined and compliant to an overall counter-terrorist strategy that seeks to diminish the utility of terrorism by undermining its validity to the very people which terrorist groups seek support from. In relation to connections between criminal and terrorist networks, the most relevant implication of defense operations emanates from the fact that defense strategies merely displace or in some cases exacerbate conditions which create opportunities for criminal activity, and potential terrorist reliance and thus willingness to engage with the criminal realm.

Chapter 5

Dissuasion and the War on Terror: What is Meant by Dissuasion, and How Might It Apply to the War on Terror?

Charles D. Lutes and M. Elaine Bunn[1]

The Concept of Dissuasion

The concept of dissuasion, introduced in the 2001 Quadrennial Defense Review (QDR)[2] as one of the four defense goals—along with assurance, deterrence and defeat—is probably the least understood of the strategic goals in U.S defense strategy documents.

As originally conceived, dissuasion was focused on the development of *state* military *capabilities.* The 2001 QDR stated:

> Through its strategy and actions, the United States influences the nature of future military competitions, channels threats in certain directions, and complicates military planning for potential adversaries in the future. Well targeted strategy and policy can therefore dissuade other *countries* from initiating future military competitions [emphasis added].[3]

This implies a narrow definition of dissuasion—discouraging current or potential adversary countries from developing, deploying, augmenting (quantitatively), enhancing (qualitatively) or transferring military capabilities that would threaten the United States, its forces or its

[1] The views expressed in this paper are of Charles D. Lutes and M. Elaine Bunn and do not necessarily reflect the views of the Department of Defense or the National Defense University.

[2] *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, Sept. 30, 2001).

[3] Ibid, p. 12.

interests[4]—rather than a broader interpretation of demotivating threatening ambitions in the first place.

While dissuading states' military capabilities is still the primary focus, the term evolved to include dissuasion against a wider set of actors and a wider range of activities. This broader interpretation is reflected in the 2005 National Defense Strategy:

> Would-be opponents will seek to offset our advantages. In response, we seek to limit their strategic options and dissuade them from adopting threatening capabilities, methods, and ambitions. *We will work to dissuade potential adversaries from adopting threatening capabilities, methods, and ambitions, particularly by sustaining and developing our own key military advantages.*[5]

The 2006 QDR seems to revert to a primary focus on states' military capabilities: to "dissuade major and emerging powers," the United States "will attempt to dissuade any military competitor from developing disruptive or other capabilities that could enable regional hegemony or hostile action against the United States or other friendly countries…"[6] However, in order to examine how dissuasion might apply to the War on Terror, we must look beyond nation states and beyond military *capabilities* only. Therefore, we will use the construct used in the 2005 National Defense Strategy—that of "dissuading capabilities, methods and ambitions."

In addition to this apparent confusion about both whom and what the United States might attempt to dissuade, the distinction between *deterrence* and *dissuasion* is often confused. While deterrence is focused on convincing an adversary not to undertake acts of aggression, dissuasion is aimed at convincing a potential adversary not to compete with the United States or go down an undesirable path. For instance, one *deters* WMD use but *dissuades* acquisition of WMD. More broadly, one *deters*

[4] The authors acknowledge Andrew Krepenevich's work on dissuasion at the Center for Security and Budgetary Affairs in influencing this definition.

[5] *The National Defense Strategy of the United States of America* (Washington, DC: Department of Defense, March 2005), p. 7.

[6] *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 6, 2006), p. 30.

aggression but *dissuades* the acquisition (or improvement) of the means of aggression, and more broadly, the hostile ambitions in the first place.

However, both deterrence and dissuasion are focused on influencing the decisions of others, and both require "getting into the heads" of these others. The most cogent current definition of deterrence is in the Deterrence Operations Joint Operating Concept (DO JOC),[7] written in 2004 and revised in 2006. The DO JOC states that the objective of deterrence operations is "to decisively influence the adversary's decision-making calculus in order to prevent hostile actions against U.S. vital interests…."[8] An adversary's deterrence decision calculus focuses on their perception of three primary elements: the *benefits* of a course of action; the *costs* of a course of action; and the *consequences of restraint* (i.e., costs and benefits of not taking the course of action we seek to deter).[9] Likewise, dissuasion involves influencing an adversary's decision calculus about the costs, benefits, and consequences of restraint regarding whatever path we seek to dissuade them from going down —whether that involves ambitions, methods or capabilities.

Since it is aimed at influencing the decisions of potential adversaries, dissuasion (like deterrence) is context specific. It depends on whom the United States is trying to dissuade, what it its trying to dissuade them from doing, how they see their stakes, how they see our stakes, how they weigh risks and gains, how they filter information, how they

[7] U.S. Strategic Command, "Deterrence Operations Joint Operating Concept," Final Draft, Version 2.0, August 2006. Available at: www.dtic.mil/futurejointwarfare/concepts/do_joc_v20.doc.

[8] With regard to "vital interests," the Deterrence Operations Joint Operating Concept (JOC) states that:

> "Consistent with the NSS, enduring U.S. vital interests include: maintaining the integrity of U.S. territory; preserving basic political and societal integrity within the U.S.; preventing mass casualties among the U.S. population; securing critical U.S. and international infrastructure (energy, telecommunications, water, essential services, etc.) that support our basic standard of living and economic viability; and supporting the defense of U.S. friends and allies. Because of the uncertain future security environment, additional vital interests may arise that are identified by senior national leadership. Deterrence strategy and planning must be sufficiently robust and flexible to accommodate these changes if and when they occur. Flexibility in our deterrence construct also hedges against the possibility that an adversary might incorrectly perceive their actions to be "below the radarscope" of U.S. resolve and response."

[9] U.S. Strategic Command, 5.

make decisions, their regional situation, their internal organization and decision making—all the "local conditions."[10] The types of information and the understanding of a group and its leaders necessary for deterring that actor would also be useful for developing dissuasion strategies for that actor. But even if we reduce our ignorance in these areas, it is difficult to predict whether our dissuasion strategies will have the effect we want.

Without influencing an opponent's decision, we could still try to *prevent* or *disrupt* his *acquisition* of threatening capabilities, or *defeat* or *defend against use* of them. But in those cases, we may have physically kept the potential aggressor from taking action, but we have not changed his mind; thus, our actions are not dissuasion or deterrence. That is not to say that the United States should stint on its efforts to prevent, deny, disrupt, or defeat; those are valuable capabilities in and of themselves, since some adversaries may not be dissuaded from acquiring or improving capabilities or deterred from using them. Indeed, U.S. ability to do those things (prevent, deny, defeat, disrupt) may well influence the calculations of potential adversaries and contribute to dissuasion and deterrence.

In order to examine how the concept of dissuasion might apply to the War on Terror, it may be instructive to break it down a bit and look more precisely at what the United States may want to dissuade—that is, terrorist ambitions, methods and capabilities.

Dissuading Ambitions

Changing the ambitions of adversaries, both state and non-state, is the most difficult challenge for dissuasion as an instrument of policy. Influencing an actor's desires, motivations, goals, and objectives requires a deep understanding of the ambitions of the actor and the context in which the actor operates. Even more difficult is determining the factors that created such ambitions and what influence strategies would be effective in altering them. To influence ambitions, time and patience are the most important commodity for the dissuader.

In some contexts, it may be difficult to determine just who the target of dissuasion should be. In these cases, it may be useful to delineate two

[10] See Payne, Keith B., *The Fallacies of Cold War Deterrence and a New Direction* (Lexington, KY: The University Press of Kentucky, 2001), Chapter 5.

types of dissuasion—direct and indirect. Direct dissuasion would consist of those activities and capabilities designed to influence the ambitions of the adversaries themselves, especially those key decision-makers that direct their actions. Indirect dissuasion would instead be aimed at actors who provide support (such as a population, financiers, weapons suppliers) without which the adversaries could not carry out their ambitions.

For the War on Terror, direct dissuasive strategies may be the least effective approaches. An example strategy might be *to convince radical Islamic leaders that strategic competition with the West is not in their best strategic interests.* The global jihadist movement has arisen as a challenge to the progressive western vision based on democratic values. A stated goal of Osama bin Laden—to create an Islamic caliphate—would be in strategic competition with Western vision and values. The ambitions of its leaders would change only if they perceive that there is greater value in ending the strategic competition than in continuing it. This might occur if they reach some accommodation with the West; feel an imminent existential threat; or are unable to maintain support for their vision. However, the degree of radicalization among the leaders of this movement makes it highly unlikely that any current methods or capabilities would directly affect the ambitions of the Islamic movement. Another direct strategy would be to target the terrorist foot soldiers themselves for dissuasion, in a sense "de-radicalizing" them. However, that cannot be done effectively on an individual basis but only in the context of dissuading the populace as a whole.

The challenge of direct dissuasive approaches has led to the adoption of several types of indirect approaches in strategies of the U.S. and the broader international community. The combination of these with other preventive and deterrent actions over time may provide the dissuasive effect that does in fact directly influence the movement and its ambitions. In the U.S. National Strategy for Combating Terrorism, this dissuasive effect is captured in one of the prongs of a dual-pronged vision: "the creation of a global environment inhospitable to violent extremists and all who support them."[11] The challenge becomes one of developing a set of viable strategies to attain that goal.

[11] *National Strategy for Combating Terrorism*, (Washington, DC: The White House, September 2006), p. 7. Available at: http://www.whitehouse.gov/nsc/nsct/2006/sectionIV.html. Editor's note: the other prong is: "the defeat of violent extremism as a threat to our way of life as a free and open society."

A mixture of several types of indirect strategies has been adopted in policies of various players in the War on Terror. The first approach is to *offer an alternative ideology to radical Islam.* The United States has made clear that its long term solution for winning the War on Terror is "the advancement of freedom and human dignity through effective democracy."[12] The target audience for this strategic approach is the general Islamic population and would-be recruits in order to directly counter the competing vision of radical Islam. Ultimately, it will be the struggle for legitimacy among competing ideologies that will determine the final outcome.

Another approach would be to *eliminate the conditions creating violent extremism.* This would directly attempt to mitigate some of the root causes of violent extremism in order to dissuade the populace from supporting terrorism, similar to the previous approach. It is different in that the mechanisms employed to address these conditions or grievance would not be tied directly to a specific ideology or political process. The United Nations, in its report from the Secretary-General, suggests that the international community must address these conditions conducive to exploitation by terrorists: extremist ideologies and dehumanization of victims; violent conflict; poor governance, lack of civil rights, and human rights abuse; and religious and ethnic discrimination, political exclusion, and socio-economic marginalization.[13] The mechanisms for conducting this approach were outlined by former UN Secretary Kofi Annan:

> We must dissuade the would-be-perpetrators of terror by setting effective norms and implementing relevant legal instruments; by an active public information campaign; and by rallying international consensus behind the fight against terrorism. To achieve effective dissuasion it is essential to remember that the fight against terrorism is above all a fight to preserve fundamental rights and to sustain the rule of law.[14]

[12] Ibid, p. 9.

[13] United Nations General Assembly, *Uniting Against Terrorism: Recommendations for a Global Counter-Terrorism Strategy. Report of the Secretary-General* (New York: United Nations, April 27, 2006), p. 3. Available at: http://www.un.org/unitingagainstterrorism/sg-terrorism-2may06.pdf.

[14] Kofi Annan, Address to the United Nations Security Council, October 4, 2002. Available at: http://www.un-ngls.org/documents/text/go.between/gb94a.htm.

A final indirect approach that will be considered here is to *influence supporters and sponsors of terrorism to withdraw support.* As opposed to the generally positive inducements of the previous approaches, this one is more oriented to imposing costs on the supporters of terrorism. Economic sanctions, interdictions, or physical punishments that impose unacceptable risks to supporters and sponsors could dissuade them from enabling terrorist activities. Without such support, terrorist leaders would be forced to reconsider their ability to achieve stated goals and would likely be influenced to moderate them.

Several challenges limit the likely effectiveness of strategies designed to dissuade the ambitions of our adversaries in the War on Terror. The first, as previously alluded to, is the difficulty in gaining the deep understanding of adversaries' decision-making and thought processes required to influence them. In attempting to influence the populace, the perceived legitimacy of alternative approaches is another challenge. To the extent that radicalization has occurred as a result of the perception of Western influence, attempts to create Western-style democracies may fall short. Additionally, the ongoing problems of the U.S. in dealing with other Middle East challenges further exacerbates the perception of legitimacy. Finally, the greatest challenge is that dissuasion of ambitions requires altering deep-rooted fundamental motivations, a process that can take a generation or more to accomplish, yet the time and patience required is essential for a complete solution to the problem of radical violent extremism.

Many of these approaches are addressed in various comprehensive strategies to combat terrorism (e.g. the U.S. and UN strategies). The problem is in the details. It is not a trivial task to develop capabilities and operations designed to accomplish the goals of dissuasion. As dissuasion is the product of an accumulation of multiple actions, the effects of individual actions are not usually measurable. Causal linkages to U.S. actions are often impossible to determine.

Despite the challenges, there are several areas which should be emphasized in such a dissuasion strategy. A well-designed and implemented strategic communication strategy is essential. On May 31, 2007, the interagency Policy Coordinating Committee led by Under Secretary of State Karen Hughes unveiled the first-ever National

Strategy for Public Diplomacy and Strategic Communication.[15] The strategy's objectives include offering a vision of hope and opportunity to the world, and isolating and marginalizing violent extremists. However, any public diplomacy and communication plan can be undermined by seemingly unrelated events. Partnering with regional and local nations and NGOs to address the underlying conditions is also important. Finally, as dissuasion is not usually the primary objective of most U.S. actions, a careful evaluation of the positive and negative dissuasive effects of planned operations and statements is warranted.

Dissuading Methods

Another form of dissuasion would be to influence the adversary to change his methods to those that are more benign than ones currently employed. The primary means of accomplishing this is to reduce the benefits to the enemy of his selected actions. Cost imposition in terms of denial of the means to carry out his selected method will be discussed in the next section on dissuading capabilities.

Reducing the benefits of adversary methods requires the dissuader to develop capabilities and means to deny the enemy the ability to carry out his attack or to mitigate the consequences if it occurs such that the attacker gains no, or negative, value from the attack. Thus, preventive and denial methods not only thwart individual attacks, they may eventually drive the enemy to abandon that approach. For instance, the increased airport security since 9/11 and success at stopping several hi-jacking or airplane bombing attempts may have influenced terrorists against targeting air traffic. Unfortunately, it will be hard to gauge whether dissuasion has occurred and thus the security measures must stay in place indefinitely.

At least two types of approaches to dissuade methods have been addressed. The first is to *de-legitimize terrorism as a method.* This is a long-term approach that, much like efforts to dissuade ambitions, will require patience and time. The U.S. first unveiled this strategy in its

[15] Strategic Communication and Public Diplomacy Policy Coordinating Committee (PCC), *National Strategy for Public Diplomacy and Strategic Communication*, June 2007. See also Walters, Caroline, "Hughes Releases First-ever Comprehensive National Strategy for Public Diplomacy," University of Southern California Center on Public Diplomacy, June 8, 2007. Available at: http://uscpublicdiplomacy.com/index.php/newsroom/pdblog_detail/070608_hughes_releases_comprehensive_national_strategy_public_diplomacy/.

2002 National Security Strategy which states as an essential element in waging a war of ideas to win against terrorism by:

> …using the full influence of the United States, and working with allies and friends to make clear that all acts of terrorism are illegitimate so that terrorism will be viewed in the same light as slavery, piracy, or genocide: behavior that no respectable government can condone or support and all must oppose.[16]

To accomplish this, the U.S. goal has been to create a global antiterrorism consensus by persuading the world community that extremist violence against innocent non-combatants is an evil method regardless of the political cause.

The UN has also seized upon this notion that terrorism as a method must be made unacceptable:

> The United Nations should project a clear, principled and immutable message that terrorism is unacceptable. Terrorists must never be allowed to create a pretext for their actions. Whatever the causes they claim to be advancing, whatever grievances they claim to be responding to, terrorism cannot be justified. The United Nations must maintain the moral high ground in this regard.[17]

Attempts to create this global antiterrorist environment have focused on public diplomacy and strategic communication. Unfortunately, the results have been mixed at best as perceptions and beliefs are difficult to change through such methods, particularly if those beliefs are not well understood.[18]

A second, more tactical, approach to dissuading methods has focused on prevention of terrorist activity through *defense in depth*. Developing a strong homeland security posture is designed not only to prevent

[16] *National Security Strategy of the United States of America* (Washington, DC: The White House, 2002), p. 6.

[17] United Nations General Assembly, p. 3.

[18] For a thorough treatment see McMillan, Joseph, ed. *In the Same Light as Slavery: Building a Global Antiterrorist Consensus*, (Washington DC: National Defense University Press, 2006).

and deny terrorist tactics but also to force them to abandon certain avenues of approach. Such a strategy is designed primarily to defeat terrorists overseas and prevent them from attacking the homeland.

A line of argument has been made that U.S. operations in Iraq have altered the target set of al-Qaeda away from the U.S. homeland and toward Iraq. Although it is difficult to assess whether this is the case or not, the idea that U.S. actions may have channeled al-Qaeda to change the location and object of its attacks would points to a possible dissuasive by-product of the Iraq war.

A more direct dissuasive effect can be designed into a strong homeland security posture. The increased security and vigilance at critical nodes deters a would-be attacker, making it too difficult to carry out his operations and thus increasing his risk by raising the costs and possibly reducing the rewards of his actions. To the extent that terrorists are deterred from conducting a certain action across a broad range of targets, they may rethink the efficacy of the act itself and ultimately abandon it in favor of a different tactic. In this “dissuasion through deterrence” process, the terrorist’s intent is unlikely to be affected, however his methods will change. To the extent that the methods change to something more easily prevented or mitigated, this dissuasion will have a positive effect. Unfortunately, determined terrorists will seek alternate methods that may be harder to defend against.

This raises one of the most serious challenges to dissuasion of methods: the ability of the adversary to adapt and develop new innovative methods. The U.S. recognizes this limitation in its counterterrorism strategy: “Our effective counterterrorist efforts, in part, have forced the terrorists to evolve and modify their ways of doing business. Our understanding of the enemy has evolved as well.”[19] Channeling the adversary to adopt certain methods requires a deeper understanding of the adversary than is realistically possible. The dissuader’s influence as to which methods the adversary will adopt is limited. As a result, the dissuader must be highly adaptable to be able to again deter, prevent, or defeat the new methods.

[19] *National Strategy for Combating Terrorism*, p. 5.

Dissuading Capabilities

The concept of dissuasion was originally derived from the concept of "competitive strategies" which had as its focus the development of overwhelming and superior capabilities to dissuade an adversary from competing directly with those capabilities. As the notion of dissuasion has broadened, so should its relationship to capabilities. In the War on Terror, there is no danger that violent extremists will seek to match our capabilities through strategic competition, but they may try to challenge the U.S. through asymmetric competition. Thus, dissuasion should be focused on preventing the adversary from acquiring certain asymmetric capabilities.

In the War on Terror, the major focus should be on dissuading terrorist acquisition of weapons of mass destruction (WMD).[20] The destructive capacity of nuclear, biological, chemical, and radiological weapons would have a catastrophic effect on the U.S. or its allies if used by a terrorist organization. In this case, once a terrorist has the capability, it will be difficult to deter him from using it. Thus, preventive actions are required to make sure he does not acquire such a capability. To the extent that these actions alter the terrorist's decisions to obtain certain weapons, then dissuasion has occurred as well. A number of actions, ranging from interdiction to securing material of concern, are being conducted to prevent and dissuade terrorists from obtaining WMD. The targets of such efforts are more likely to be the criminal networks and black markets to dissuade the providers of such material from dealing in these illicit materials. As the costs and difficulty of obtaining WMD are raised, at some point terrorists may have to abandon pursuit of this capability in favor of a more cost-effective and easier-to-obtain alternative.

Terrorists tend to develop capabilities such as Improvised Explosive Devices (IED) from simple, rudimentary, or widely available technology. Therefore it is unlikely that any effective strategy or capability, short of the ability to neutralize these capabilities, will be effective in dissuading terrorists from acquiring them.

[20] For a discussion on various issues surrounding dissuasion of WMD capability, see Lutes, Chuck, "The Role of Dissuasion in Combating WMD," *Strategic Insights*, Vol III, Issue 10 (October, 2004).

In a general sense, one could consider suicide bombers as a terrorist "capability." While we cannot prevent terrorists from acquiring the material for suicide bombs—and thereby dissuade future theorists from attempting to do so—we may be able to dissuade the would-be bomber from enlisting in the cause in the first place. As discussed in previous sections, changing the attitudes and mindset of the population will go a long way to drying up this resource and denying this capability.

Conclusions

Dissuasion is a tricky concept and one should not get caught up in debates about what distinguishes dissuasion from prevention, or deterrence. In the War on Terror, these differences blur even more. In reality, actions designed for one purpose have secondary and tertiary effects. The key is to consider what those effects might be, and in the case of dissuasion, to understand how certain actions might change the mindset of the adversary. Actions determined to have positive dissuasive effects should be continued, while actions with negative dissuasive effects should be examined more closely. Unintended consequences can have disastrous results.

The U.S. has employed a variety of strategies that will have some dissuasive effect on terrorists' ambitions, methods, and capabilities. These effects may not be realized for a long time, and we may never be able to determine their full extent. However, dissuasion is a useful conceptual tool in considering new strategies, methods, and capabilities for countering terrorism and protecting the U.S. homeland.

Chapter 6

Trade Security: Stovepipes In Motion

Robert Quartel

Solving the complex issue of national maritime security policy requires that we bridge the gap between, first, the requirements of homeland security (essentially a policing activity) and national security (embodied in the national intelligence architecture) and, second, between these governmental functions and the operational needs of both domestic and global commerce for speed and efficiency at a reasonable price. The decision requirements of each sector independently are insufficient to solve the aggregated, overlapping problem of global maritime security.

Moving forward in a meaningful way, however, is impeded by a widening gap between the public, partisan political, and commerce-driven expert's point of view about what the security issue really is in the maritime domain. A growing number of maritime security experts have in fact begun to arrive at the view that *the public process directs us to look for the wrong things at the wrong time in the wrong direction in the wrong place with the wrong mindset and with the wrong resources.*

If almost any expert in maritime security were to be asked what the most important events of 2006 and early 2007 were that have both illustrated and affected our collective view of the national maritime security problem, he would no doubt first answer the Dubai Ports World fiasco. He would do so not because the proposed financial takeover of a number of American port facilities by Dubai Ports World (DPW), the second largest operator of terminal facilities in the world, was—as much of the public and Congress perceived it to be—a threat of any kind to national security, but because a legitimate international business transaction was derailed by Congressional and public hysteria about a fictional "Arab takeover" of "America's ports," stoked primarily to foster short-term tactical partisan goals of the now majority party in the Congress. Experts in trade and intelligence alike have in fact described this purely political theater as an event which damaged not only commercial but national security interests of the United States.

Others might well suggest for second and third place two other events: First, the arrest in Miami in the summer of 2006 of seven said-to-be early-stage conspirators plotting to damage the port and, second, a truck incident which occurred there in January 2007 in which a case of mistaken identity, an unknown cargo, and a language miscommunication fostered a severe but reasonably appropriate reaction of security forces. A few might include a fourth answer, the use of chlorine trucks in bombings in early 2007 in Iraq. All of these would be correct but the chlorine trucks might well today be better put at the head of the list of what should inform us most going forward.

What do these several apparently unconnected events—the DPW fiasco, a squishy FBI sting, the highly public capture of a not innocent, but certainly non-threatening truck and driver in Miami, and now binary chlorine weapons in Iraq have to do with the way we should be thinking about maritime security in its whole and its parts, whether for national security or the maintenance of global commerce? Everything and nothing.

Everything because maritime security and now "port security" have dominated Washington rhetoric in recent years—including not only the 2004 Presidential campaign but the last session of the 109th Congress in which over 100 new pieces of legislation were dropped in the congressional hopper, all purporting to make American ports "secure." The so-called SAFE Port Act, passed at the end of 2006 and which some might say was the epitome of doing everything and nothing—including making internet gambling illegal which the cynical have said was as germane to safe ports as the rest of the law—was neither the least nor the last of this flurry of activity generated out of the lies of the DPW controversy. Today the 2006 SAFE Act is itself being supplanted by the so-called Fulfilling the Mandates of the 9/11 Commission Act in which congressional partisans have invented out of whole cloth a fictional Commission mandate to physically scan all containers in movement to the U.S.

And *nothing* because almost everything the Congress and the public think they know about maritime security and the maritime domain—*about both the actual threats and the actually threatened*—are wrong as are not surprisingly the solutions demanded from this lack of knowledge. That extends most certainly to their lack of understanding of the technologies associated with whatever risks there may be.

It would be reasonable that most people both in the public and on Capitol Hill would seem to believe that maritime security is all about ports and water. In fact, it is not just about either. In many respects, American ports may well be the least important part of the international supply chain and the most overrated potential victim of our maritime insecurities.

The Miami incidents are important and have an ironic relevance because they *should* serve to remind all of us that if we spend all of our time and energy and money looking out the front door we are going to miss what is happening in our backyard. That's true of the maritime domain and the intelligence activities associated with it too.

Maritime security is not just about the water and what is on or abuts it, but about the context in which maritime events occur.

Nor is maritime security likely to be about containers with nuclear bombs or ships blowing up in the Port of New Jersey or any other port as is the focus of so much congressional legislation and associated conversations about technology.

It is really mostly about process—the intersection of intermodal transportation and finance and people. That suggests that the solution should be about getting more information and intelligence on those processes and transactions.

The U.S. Department of Homeland Security has developed a myriad of programs to deal with the process issue in the international maritime trade arena, imposing on the commercial sector process requirements having little to do with traditional compliance: The Customs-Trade Partnership Against Terrorism (CTPAT) aims to tighten up supply chain processes through voluntary process security; the Container Security Initiative (CSI) inserts scanning machines into the loading process overseas; the 24-hour rule pushes some of the content data at us before a vessel sails for the U.S.; and recently the initial phase of Secure Freight, in response to the so-called SAFE Port Act, combines a variety of measures to attempt to create a holistic and secure trade process. Nevertheless, while many of these programs are justified (for essentially political reasons) as having both a security and an efficiency component—in the eyes of trade and security experts the first would be modest and through the lens of the business community the latter largely fictional.

Irrespective of their utility, CTPAT and the 24 Rule and new trade data rules requiring even more information early will not make us safe—although the latter will certainly help because it is mainly about data, not necessarily all that we need or could get, but an important start nonetheless.

Likewise, there is no question that better security seals, tracking devices, "smart boxes" and the myriad of technologies including offshore monitoring devices are generally good things and will all at some future point be a part of what we all like to call a "complete solution" covering both the commercial and governmental requirements in the broader question of supply chain and maritime domain vulnerability to terrorist infiltration and use. They will, that is, if the commercial devices ever get to a price that falls below the insurance/cost curve and therefore finally make a business case for voluntary adoption—the path it seems that we are by-and-large following.

But smart boxes and electronic seals and RFID tags and field monitoring devices will not make us safe. Nor are they going to happen soon in a significant way.

Targeting high-risk containers and running them through VACIS (scanning) machines at CSI ports and past radiation monitors is a nice thing too, because we might catch an occasional stowaway, and we may well deter the casual terrorist.

But is it worth the cost—either directly as a public investment or indirectly in the cost of moving goods? Probably not, because, despite the widespread belief outside the industry that physical inspection is better than intelligence, *CSI and VACIS machines and radiation portals—whether applied to 5 percent or 100 percent of all containers—will not make us safe either.*

For a bit of perspective, consider this: Airport screeners have, according to the Government Accountability Office (GAO) a failure rate of from 15-20 percent on suitcases and carry-ons—little boxes if you will—that average between 4 and 6 cubic feet of volume. Over half the containers in the world are boxes containing some 2600 cubic feet of widely varying goods. Scanning machines still have to be operated by human beings who, even aided by intelligent decision software (a necessity given the high volumes of data and complex decision rules), still make the final decision.

Nor will knowing what is in the box, the traditional U.S. Customs view—or believing you know—keep us safe. The typical international trade moving for a part of its existence in the maritime domain—that is, on a ship over water—consists of the activities of some 20-25 parties, 30-40 documents, hundreds of data elements most of which are entered repetitively and often incorrectly. Not to mention, of course, the activities and vulnerabilities associated with the ship, the crew, the ports, the trains and the trucks and facilities associated with all of it before and after a cargo ever hits a terminal.

But while it all sounds complex and vulnerable and it is—it is probably easier and more likely to turn a perfectly legal cargo, one the origin of which you know, that you know for a fact is what it says it is—into a lethal weapon than it is rationally to penetrate a supply chain in motion with a WMD.

The knowledge of *context*—intelligence—will make us more secure than will supposed knowledge of *contents.* Why is this? Because, when we are sure that we know the contents, we probably do not. When we think we know the context, we might. But intelligence alone will not make us safe either.

Why then does this discussion begin by saying that we are looking in the wrong place for the wrong thing in the wrong direction at the wrong time with the wrong resources? The answer lies in the questions that both transportation and WMD experts ask themselves against the knowledge they have gained from experience. The broad conclusion that many of us draw from this analysis is that we probably spend altogether too much time and energy on ports, contrary to widespread public and political opinion.

A study published in 2006 by the Public Policy Institute of California illustrates among many other points the flaws in the logic of looking out, not in, for danger. In this study, the authors considered the ease and impact of a truck bomb attack on the Ports of Los Angeles and Long Beach. They note first, again contrary to public opinion, the relative un-attractiveness of ports as a target: "[T]he sheer physical scale of the facilities"[1] makes it clear that neither a conventional weapon nor a dirty bomb could have more than a minimal impact on the capability of the port to operate. Even a nuclear bomb, they note—the only device that could take out the whole facility for any extended period of time—would be more likely to target a large population rather than the thinly populated port. Ports have too few bodies to be bloody enough to be attractive.

Nevertheless, they conclude that four truck bombs strategically placed at the four bridges connecting the ports and their terminals to mainland domestic distribution systems could take this port complex offline for anywhere from three months to two years—at a cost ranging from "mild" to as high, perhaps, as $45 billion over that period.

More importantly from the standpoint of institutional resilience (recovery from an incident) they go on to say in other chapters that the economic damage is in fact likely to be minimal because, irrespective of the damage to a single port complex, the carriers and shippers are flexible and agile even if the port is not. Ships and trains and trucks and their cargoes and the workers associated with these facilities will rapidly find another place to go.

The key points are:

- Ports are physically more vulnerable to a truck than they are to a ship, and
- The maritime domain is not just about the water.

It is about the nexus in which it is embedded—the much greater system of transportation transactions, technologies, financial activities, people intersections and movements and more, some public, some private, some governmental—the myriad of activities that make up the broad system of international trade and commerce and trade movements. Ships do not stand or operate alone. They stand at the middle of a system that is fundamentally anchored on land, not in the water.

Thus, approaching the maritime domain as solely about ships, water, and ports misses the larger point—which is that ports and ships on the

[1] Haveman, John and Howard J. Shatz, eds., *Protecting the Nation's Seaports: Balancing Security and Cost*, (San Francisco: Public Policy Institute of California, 2006).

water ride the leading edge of a great wake of data and transactions, some 90 percent of which took place—in a data sense—before any ship ever left the dock and a large piece of that post-purchase order and before a product was ever manufactured. Unfortunately, we've tended so far to focus on the bow wave of data instead.

All of that being said, then what is the threat and where should our activities focus in the future?

Policy Going Forward: Revising the Forward Face

When the public or the government think about maritime security, they seldom think about trucks, trains, or hazardous materials moving into or out of that environment. Some of that is related to the peculiar institutional stovepipes in which all of commerce, transportation security and the intelligence and law enforcement activities associated with them are executed. Nevertheless, the use of chlorine and possibly other hazardous materials in the past in terrorist bombings in Iraq as a secondary—and additionally destructive—element underscores the broad range of vulnerability to this type of attack and produces today in the case cited above the conventional equivalent of what I would call the "new dirty bomb."

Yet, in the course of an average day, hundreds of thousands of trucks and railroad tank cars *knowingly* transport millions of tons of hazardous chemicals and products across the United States, in and out of ports, off and on ships, some totally within the domestic context and others at the end or beginning of an international pipeline of cargoes. Unknown amounts of hazardous cargoes move *unknown to or undeclared* by their (truck) drivers or the companies associated with the move. Some 3 billion tons of regulated hazardous materials—including explosive, corrosive, poisonous, flammable, and radioactive materials —traverse the country annually in a system of over 26 million trucks, nearly 3 million certified for full container loads, driven by some 3.3 million men and women with commercial truck driver's licenses—carrying nearly 70 percent of all domestic commerce. Another 30 million carloads, 8 million containers and almost 3 million trailers move over 121,400 miles of railroad track in some 473,000 rail cars, pulled by 22,000 locomotives, and manned by over 157,000 employees.

It should thus be easy for the reader—and certainly for an opportunistic terrorist—to imagine the theft and diversion of a gas or propane truck. But, if terrorists (domestic or foreign-grown) were to strike inside the United States, they would likewise be certain to learn from the lessons so ably demonstrated daily in Iraq and to integrate some form of lethal or toxic material into any form of bombing—from a suicide attack in a mall to a truck bomb on a bridge. The threats that planners have imagined range from the use of explosives both of the nuclear and non-nuclear sort; dirty bombs using radioactive material widely available across the nation; the release of toxic chemicals that can cause significant injury or death; and many other scenarios.

Despite this, we have spent literally hundreds of millions of dollars on port security—some $800 million or more—looking at the ships and containers coming in by water and almost nothing on the containers and non-containerized cargoes entering the maritime domain from the domestic side by truck or rail.

So that takes care of the "wrong place" part. Now how about the "wrong thing"—beyond the potential for domestic chemical weapons? What about the what—that is, what is or is not likely to be thrown at us through the maritime domain from overseas?

To address that, look at the issue of ports as funnels, that is, as a way-station for a weapon on the way to somewhere else—the container as a Nuclear-Bomb-Casing-Scenario, the one that drives so much of political rhetoric.

Being among the first to suggest the possibility that a terrorist could put a bomb in a box coming from a foreign country, I acknowledge that as starting point. But every WMD or transportation expert knows that that would in reality be the hard way to do it—either to create a WMD or to move a weapon through the supply chain without its discovery. First, every weapon of mass destruction but one is more easily built right here at home. Why then go to the trouble of attempting to sneak a weapon in from overseas with all of the attendant difficulties of process control? Biological weapons can be produced with materials and equipment bought off the web. Potential chemical weapons surround us: a tipped chlorine tanker passing by the Department of Agriculture in Washington, a gasoline truck detonated in downtown Chicago, any of these constitute a potentially lethal weapon of mass destruction.

A dirty bomb—a psychological device—requires only explosives and low-grade radioactive material stolen from a hospital or a watch factory.

This is where the Miami arrest comes in as a helpful reminder that even we Americans—as the Canadians, Spaniards, Londoners, Indonesians and others before us have tragically learned—potentially have our own home-grown terrorists who are willing to contemplate these relatively easy paths to death and destruction. And the truck incident reminds us that ports have both an in and an egress gate.

The exception to all of this is the fissile material or even some of the components needed to create a nuclear device, which almost certainly have to come from a source overseas. But are terrorists—who we know aren't stupid and who have spent now some 20 years trying to steal the bomb (or fissile material)—really going to put it in a box once they get one and just let it go? Most of the terrorism and transportation experts I talk to believe the logical answer is "No." Most transportation experts would argue that the best course is to smuggle it into the U.S. in an oil tanker, the hold of a grain or chemical ship, the bowels of a car carrier, or even in the Captain's cabin on a liner vessel.

Perhaps the terrorists might even want, instead, to put it on a tramp from the Caribbean and load it onto something like a private boat, take it from there to a dock—not a port—and deliver it just about anywhere they wanted to up or down the East Coast. Of course, that same boat, docked on an island surrounded by farms, could hold about a ton of phosphate fertilizers too—to my earlier point about home-grown terrorists and the weapons they can create in our own backyards.

Shielded as it would have to be to prevent contamination of the terrorists themselves, it would be undetectable at more than a short distance by any radiation detectors we now have. The great volumes of these ships would require vast armies of inspectors who would still prove to be virtually useless. That boat, no surprise, is the Coast Guard's greatest fear.

So, if securing the container, knowing the content, checking the players, battening down the ships and our ports, implementing RFID and electronic seals, and getting in the face of our friends and allies is not the solution, then what are we missing?

If we cannot seal ourselves off from these threats, what can we do?

The short answer is that we need to continue our efforts to better connect the dots. We need more data on what goes on in the commercial trade process and we need better and more far-reaching intelligence on what goes on and around the maritime domain. For a fifth of what we have spent on Operation Safe Commerce and the Port Security grants we could have the information we need to truly ascertain risk, probability, and security. New systems being evaluated for food safety and air cargo risk assessment bear this out.

We also need better data collection capabilities and more money to create and buy the technology to connect the dots of the data we already have. The private sector spews data on the supply chain, worldwide. The web—open source—leaks facts and information like a torrent on everything that moves. The government collects millions of pieces of data on people and goods, not only on transportation but on the transactions underlying commerce. The global financial system manages billions of transactions daily, which we now know we monitor. We should spend the money to pull it all together. The core elements of a robust common operating picture for maritime security and trade intelligence are there today, spread across the Navy, TSA, the Coast Guard, and even in some small part at U.S. Customs and Border Protection.

We need to involve the trade profession, because the people who actually move goods will always know more about the process than almost anyone sitting there in Washington on Capitol Hill.

We need to focus more on shipments and less on containers, intermodal more than just ships, dock and terminal workers more than just mariners.

We need to look in and not just out, at trucks, trains, and people—not just at ports, ships and sailors.

We need to continue to break down the information barriers both between defense and national security systems and between these systems and the commercial system of trade.

Most importantly, from an operating standpoint, we need to put maritime intelligence under an umbrella that intersects intermodal commerce and we need to separate compliance from security. DHS, Defense, the Navy and the U.S. Coast Guard are all parts of that complete solution.

We should husband and spend our scarce dollars on the problem—not the innocents, whether we are talking about containers or ships or sailors or just plain old border security. That means that we should automate almost all of the big processes and actually process everything that moves—people, goods, equipment—again, whether it is about logistics or people or trucks that want to cross the border. And it means that we use these automated processes to refine and target and assess the risk to which we should actually apply our limited resources—again, whether VACIS machines, tags, or people—rather than waste them on people and goods that are almost certainly not part of the threat.

Finally, none of this is not to say we should not continue to tighten up our supply chains, monitor container traffic, look at ships, etc. We should do that too—but our expectations for the value of these limited actions should itself be limited as should our federal dollars. This is largely the responsibility of the private sector.

The biggest problem of all, however, continues to be the failure to focus on what constitutes a real and probable threat—the public and political uproar over Dubai Ports World illustrating this in spades—and the larger societal problem which is that the public likes gadgets and the Hill likes pork. We are spending too much of our scarce money and too much time on both. What we should be doing instead is spend more money and time and effort on the cost effective things that matter—intelligence, process, people, information, response.

Chapter 7

Deterrence and Homeland Security: A Defensive-Denial Strategy Against Terrorists

James H. Lebovic

Terrorists are allegedly difficult to deter because they are hard to punish. But terrorists are *punished* when they are *denied* their objectives with defenses that cause an attack to fail. When their attacks fail, terrorists must accept costs (punishment) in the form of a lost capacity to attack alternative targets or the same target, at some future point, under more favorable conditions. The costs of failure are prohibitive when the success of an attack depends upon surprise and the defender is now on alert. Then, the "next" attack will be harder to engineer than the last. The costs of failure are also high when a current operation will expend valuable—and, perhaps, irreplaceable—offensive assets such as the trained commercial pilots that were essential to the 9/11 attacks. Given these costs, terrorists might choose not to attack, might choose to attack a less consequential target, or might delay an attack giving the defender time to pick up signs that an attack is forthcoming and to prepare accordingly. *All three outcomes are desirable from a deterrence standpoint.*

What Targets Require Defending?

A defensive-denial strategy must respond to a simple question, "what targets require defending?" The answer is complicated, however, because a wealth of available attack choices permit terrorists to strike not just unusually vulnerable or valuable targets but especially vulnerable *and* valuable ones. For example, the exclusive screening of carry-on luggage at airports would allow terrorists to smuggle bombs onto planes in the cargo hold. The quandary for the defender is knowing what to protect, then, when it cannot protect everything. More specifically, the issue is what to select for protection and what to exclude from protection given two complications.

First, lesser defensive priorities are still inviting targets. In fact, it is hard to conceive of a target that offers at least some political dividends to a terrorist if attacked successfully that is not also valued by the targeted government or society. Thus, from the defender's perspective, everything appears vulnerable. For instance, attacks on any of a large number of buses and trains are useful to an attacker that seeks to convey that everyone, anywhere, at any time, is susceptible to attack—that people risk their lives doing the ordinary. Even isolated attacks on anonymous individuals can have enormous terror-producing effects, as the 2002 sniper attacks in Washington, D.C. show convincingly. As always, the problem for the defender is that it can try to protect what it values most but this is wasted effort if the attacker's interests center on another target, that the defender also values.

Second, terrorists can choose to attack less protected targets when defensive commitments create offensive opportunities. By defending certain targets at the expense of others, the defender redirects the terror threat toward "softer" targets. This target shift is evidenced in Iraq when insurgents moved from attacking less vulnerable U.S. targets (e.g., bases, convoys, and targets in Baghdad's walled green zone) to Iraqi civilians, recruiting centers, police stations, diplomats, government officials, and Shiite mosques.

When evaluating its capabilities and setting its priorities, then, the defender encounters the long-recognized international dilemma for states seeking to deter attacks on their interests. By designating areas of the world that are in the national interest to defend, a state implicitly excludes other portions of the world from protection and invites attacks on those lesser interests. Conversely, by claiming lesser interests as "vital," a state risks depreciating the credibility of its promises to defend any and all of these vital interests if attacked. The credibility of the defender's claims are at issue in part because of what can be described as a "commitment" problem. The defender can "signal" its terrorist adversaries that it will remain vigilant against any and all terror attacks, as the U.S. did by establishing the Department of Homeland Security and adopting various security reforms. But ambitious commitments invite challenges. The more the defender commits to defend, the greater the challenger's willingness to test the defender's resolve and/or capabilities.

Even if terrorists believe that the defender has the *intention* to defend its interests—most certainly true of the defense of targets on national soil—the defender's credibility is in question when the attacker doubts the defender's *capability* to respond successfully to an attack. Because the defending government cannot do everything and be everywhere at once, the government cannot devote resources to the protection of targets in proportion to their value. The sheer number of places where large numbers of people congregate—among them, the most vulnerable and sympathetic portions of the population (e.g., school children)—make a universal defense strategy impossible—and dangerous. By attempting to defend more than it can, the defender risks undermining its ability to deter attacks.

Yet the options for the attacker are constrained, as well, given its desire to strike targets of value to a government or society. This limits the range of available choices to targets that governments have a strong interest in defending. Symmetries in value between the attacker and defender are arguably more the rule than the exception when terrorists desire to hit societies "where they hurt" and to magnify the political, social, and/or economic effects of an attack. Indeed, the evidence is that the impact of so-called spectaculars reverberates beyond the limited threat those attacks present—that people tend to exaggerate the chances that they, too, will be victimized. Because of these very consequences, governments can focus their defenses on what terrorists want to attack. For example, these symmetries arguably abet the U.S. strategy of protecting nuclear power plants more than oil refineries, airline transportation more than bus stations, and the U.S. capital more than other U.S. cities. It also played to the U.S. strategy, immediately after 9/11, of concentrating protective resources upon the disarming of airline passengers—preventing them from boarding planes with potential weapons—over screening stowed aircraft luggage for explosives. Assuming that terrorists had less interest in killing hundreds of people when, by hijacking an aircraft and using it as a weapon, they can kill hundreds (perhaps, thousands) of people, destroy a physical structure, and receive credit for pulling off *another* 9/11 style attack, the U.S. could focus upon what it regarded as a costly attack scenario.

Although the defender might still be unable to offer a robust defense of the numerous targets that terrorists want to strike, the defender can benefit, as well, from important capability and informational advantages (asymmetries). These limit what the attacker can gain from an attack and/or force the attacker to accept risks and costs in planning and executing an attack. These advantages can boost the credibility of a defender that can capitalize on a variety of (denial-based) strategies.

First, the defender can rely upon a *limited defense*. A limited defense is meant to concede ground—given the prohibitive human and financial costs of a robust defense—and only contain the damage that is suffered in an attack. Viewed from a deterrence standpoint, a limited defense attempts to reduce the value of an attack. The current enforcement of flight restrictions around Washington DC illustrates this. With the high costs of around-the-clock patrols by military aircraft, an identification zone and narrower flight-restricted zone within which aircraft are closely monitored concentrically encircle the U.S. capital. Because it is unlikely, however, that the implementation sequence will unfold within the time period available to shoot down an approaching aircraft or that the order will be given barring extraordinary evidence of hostile intent, the system is best suited to stop a *second attack*, not a first. This limited defense aids deterrence by reducing the value of an attack, that is, by thwarting the catastrophic outcome (i.e., multiple planes crashing into multiple buildings) that motivates the attacker.

Second, the defender can resort to a *partial defense* to boost the costs and risks of an attack. For instance, by reducing key vulnerabilities in high value targets, the defender can deprive the attacker of easy victories and force it to adopt more expensive and dangerous tactics to accomplish its objectives. Simply reinforcing and locking the door to the airplane cockpit, and keeping the door locked under all circumstances, dramatically increases the challenge for an attacker that seeks to gain control of a passenger aircraft. Indeed, the defender can adopt single measures that reduce the value of an attack *and* increase the costs to an attacker. Protecting critical nodes (e.g., in the electric power grid) or choke points (e.g., railway or highway tunnels) that could produce highly disruptive effects if attacked reduces the payoff from attacking those sites (by offering a limited defense) and forces the attacker to adopt cost-ineffective methods to achieve attack objectives (e.g., attacking electric transmission towers and lines rather than substations).

Third, the defender can utilize a *flexible defense* by allocating resources as needed to blunt an anticipated or actual attack. Consequently, local defenses can be designed only to limit damage from an attack through a "holding action" until reinforcements arrive in the form of light, mobile quick-response military forces, special weapons and tactical (SWAT) teams within police departments, or emergency responders such as hazardous materials teams, medical personnel, fire departments, and help arriving from other municipalities, states, or countries. Flexible defense is also embodied in organizational and/or technological systems that permit a coordinated and informed response to an attack.

Fourth, the defender can resort to a *selective defense* in which resources are allocated to combat more damaging threats rather than less damaging ones. For instance, security is often disproportionately tight at sports events that attract tens of thousands of people. Smaller groupings of people are attractive targets, but the possibility that terrorists could kill and injure a large number of people in a single incident—in a celebrated venue—makes these events important to defend. Likewise, security can focus on more over less damaging modes of attack. For example, U.S. officials can worry more about a destructive car and truck-bomb threat to homeland civilians and structures than the threat from dismounted suicide bombers.

Fifth, the defender can engage in *defensive screening* efforts in which populations are "filtered," as they pass through key access points. The intent is to locate those who fit a suspect demographic or behavioral profile and to subject them to additional screening (i.e., searching and/or questioning). Profiling will not work if the size of the suspect population is too large to target for rigorous screening, government agencies focus on physical characteristics at the expense of useful behavioral markers, and members of a "suspect population" retain useful information out of fear that they will inadvertently incriminate themselves, family members, or friends, or damage their community. In principle, though, screening underlies all efforts to monitor the flow of people or goods at some distance from possible targets. For instance, a "profiling" of sorts underlies the U.S. monitoring of container shipments into the U.S. U.S. customs inspectors focus their scrutiny on "untrusted" shipments from problematic areas of the world and/or that involve importers that have not built a record for clearing customs.[1]

[1] Flynn, Steven, *America the Vulnerable: How Our Government is Failing to Protect Us from Terrorism*, (New York: Harper Collins, 2004), p. 90.

Sixth, the defender can construct a *triggered defense*. The defender need not stay on maximum alert all of the time but can husband resources and go on alert when a possible threat is identified. Once mobilized, the defender is better able to combat the threat and to appreciate its actual dimensions. Signs of a prison break can trigger a general “lock-down” to counter both the immediate threat (e.g., prisoners who are trying to escape) and unknown other—perhaps, bigger—threats to which the precipitating incident is linked. Similar triggering occurs when a security violation in some U.S. airports leads to an order to “dump the concourse” which requires the re-screening of all airline passengers.[2] Triggering is also involved in decisions to shut-down a subway system when some trains are attacked, to heighten security precautions for all forms of public transportation when one mode is attacked, and to heighten security in U.S. public transportation when the subway system in another country (e.g., Britain) is hit.

Seventh, the defender can engage in a *random defense*. Just as bargaining theories of deterrence relied upon a “threat that left something to chance,” the defender can choose to protect some targets or take some actions periodically and/or unpredictably to increase the risk to the attacker. The logic of risk manipulation supported the random screening of U.S. airline passengers in the aftermath of 9/11. Random screening—let alone the screening of but 1-in-10 passengers—appears to make little sense from a defensive perspective given the severity of the threat should terrorists take control of an airliner. It does make sense from a deterrence perspective (especially if it is assumed that the 10 percent chance of being screened combines with other uncertainties with which the attacker must contend). The 10 percent detection probability is that much more effective as a deterrent if attackers in a group (the 19 hijackers) each have a 1-in-10 chance of being screened and the detecting and detaining of any one attacker will impair or compromise a terror operation. Then, random screening serves a selective defense that focuses on combating a (9/11 style) multiple-attack scenario.

Eighth, the defender can employ the *spatial defenses* that were used in the Cold War era to strengthen nuclear deterrence. One aspect of

[2] Ibid, p. 77.

these defenses is *mobility*. Just as the nuclear powers relied upon mobile submarines and land-based missiles to keep nuclear forces secure from attack, governments can harness mobility to protect government leaders from assassination. The schedule and movements of the U.S. president are often kept secret and, in times of emergency (e.g., 9/11), the president can remain mobile (e.g., Air Force One) or be taken to an undisclosed, fortified location for protection. Another aspect of these defenses is *dispersion* to reduce the value of a *target* (in contrast, a limited defense reduces the value of an *attack*). Just as the nuclear powers chose not to co-locate all of their nuclear resources—creating an inviting target for attack—the U.S. president and vice president currently avoid attending the same public events. The logic of dispersal underlies recommendations that dangerous chemical facilities be distanced from population centers and that trains carrying dangerous cargos be routed away from urban areas.

Finally, the defender can rely upon *defensive uncertainty*. Despite al-Qaeda's legendary ability to obtain information on targets (through open sources and active surveillance), not all of the strengths and vulnerabilities of a target will be known to an attacker. Available floor plans and maps might be incorrect, dated, or lacking fine details (e.g., the location and capabilities of an alarm system). Or else, uncertainty could arise from unresolved engineering or practical issues that are implicit in an attack scenario. Illustrating this is the considerable controversy about whether the reactor core of a nuclear power plant could survive a direct hit from an aircraft. Uncertainty could also result from a deliberate policy of defensive concealment. For example, security units seek to multiply their effectiveness by reducing the predictability of their patrol schedules and staffing and by withholding information about their counter-terror tactics and procedures. Inevitably, all partial and flexible defenses have some amount of useful uncertainty built into their performance, unintentionally or by design. A visible airport security presence—though for passenger screening—offers some protection against any and all attacks on airline transportation because the defender *could* stumble onto an attack.

Thus, deterrence can be strengthened when the defender creates favorable capability and informational asymmetries using a number of defensive approaches, alone or in combination. Indeed, deterrence effects could multiply enormously through a packaging of approaches—

as illustrated by security at a hypothetical gathering attended by a government leader. The leader can be protected through a selective defense in the form of bodyguards, a full screening of people in close contact with the leader, a partial defense (against certain kinds of attacks) through screening with metal detectors or explosive-sniffing dogs, random screening of all people in attendance, and uncertainty about where the leader will be sitting and how and when the leader will be entering and departing the venue. In combination, these imperfect approaches offer the deterrent advantages of a *layered defense*. The variety of possible combinations of defensive approaches is too large to discuss in full. Suffice it to say that which combinations are usefully employed depends on available defensive resources, the nature and intensity of the threat, and the defender's tolerance for error. Random screening makes little sense if an assassin is known to be in a crowd just as random screening or selective defense of urban targets make little sense if terrorists are known to possess a nuclear weapon that can devastate an entire city.

It is easy, then, to understate the range of options available to the defender and to overstate the options available to terrorists. Certainly, deterrence is likely compromised should terrorists acquire weapons of mass destruction. The ability of a single atomic bomb to produce widespread destruction at a national point of entry allows an attacker to overcome challenges (e.g., moving the bomb to a distant city) that could undermine operational success. Likewise, a terrorist possessing the anthrax or smallpox virus is arguably positioned to realize a worst nightmare in Western societies and to attack with ease because a biological strain can be introduced surreptitiously into a population. But terrorist groups have not taken full advantage of opportunities to exercise "high-end" options (i.e., spectacularly destructive attacks) or even "low-end" ones that are well within these group's capability and promise a considerable return. If terrorists have rejected either set of options based on their cost or value, the capabilities of the attacker are inadequate given its objectives, and deterrence is in effect, at some level. Policymakers can magnify these effects with appropriate defensive strategies.

Policy Implications

The principles underlying a denial-based, deterrence strategy are straightforward: "instead of trying to protect every conceivable target against every imaginable form of attack,"[3] the defender seeks to cause the attacker to accept greater costs and risks and/or a reduced prospect of gain in planning and executing an attack. When governments accept these principles, a number of useful policy guidelines emerge.

First, governments must safeguard their priorities by protecting against *possible* worst-case attacks on national citizens—their lives, livelihood, and property—and *probable* attacks that reflect the goals of the attacker (e.g., the World Bank buildings or Wall Street). In selecting their protective priorities, governments must distinguish the practical value of a target from its patriotic or sentimental value, likely effects from less-likely ones, and short-term consequences of an attack from long-term effects. Thus, a viable strategy could center on protecting transportation links—and airlines in particular given their unique vulnerability—and places in which large numbers of people congregate.

Second, governments can protect targets by conceding their vulnerability. Governments must draw a distinction between tolerable and intolerable levels of destruction. In all likelihood, people will die and/or property damage will occur in a terrorist attack regardless of what governments and private interests do to prevent it. The operative question must be how best to expend resources to contain and otherwise limit the consequences of an attack.

Third, governments can protect targets by not increasing their vulnerability. Through regulatory efforts aimed at hardening, zoning, transporting, or policing, governments must defend facilities and vehicles that can have devastating collateral effects when struck. Chemical plants and trucks and trains carrying hazardous materials are inviting targets when proximate to urban areas, and these potential "weapons" must be "distanced" from lucrative value targets.

Fourth, governments can protect targets even when doing so incompletely. Defensive measures succeed, controlling for cost, if

[3] Jenkins, Brian Michael, *Countering al Qaeda: An Appreciation of the Situation and Suggestions for Strategy*, (Santa Monica, CA: RAND Corporation, 2002), p. 29.

reducing casualties and damage below levels that would otherwise have occurred.

Fifth, governments must respond, but not over-respond, to threats. Flexible defenses rely upon scarce and depletable resources, and the danger should flexible defenses become static or overused (e.g., through frequent "alerts") is that they will be unavailable for other contingencies.

Sixth, governments must control national gateways and key corridors of attack. By screening traffic through immigration offices and airports, governments can increase the overall risk to a terror operation that involves large numbers of personnel. Governments must also act to impose risks late in the attack plan. It is one thing to deny entry into a country of an operative whose papers are not in order; it is quite another to nab an attacker at the preparation stage (when guns or explosives are being purchased or specialized training is being sought) or (at a checkpoint) during the execution of an attack. Attackers should not be permitted to assume all risks up front when the security of a terror operation is least likely to be compromised and the penalties for participants are relatively mild (e.g., deportation rather than death in a failed attack).

Seventh, government must adopt covert measures signaled overtly. Covert surveillance can trap a suspect, but a security presence can deter an attack only when advertised. Visible defenses need not be *transparent* defenses: signaling the full capabilities of a defense is advisable only when defenses are impenetrable. Visible devices and procedures that allude, somehow, to the existence of hidden ones are perhaps the best deterrent, for example, in the form of an occasionally strong, albeit somewhat unpredictable, security presence.

Eighth, governments must anticipate new threats but can focus on established ones. Imagining what terrorists *could* do is a useful exercise; but terrorists might have neither the desire nor capability to do what we fear most. This means that governments can capitalize on the learning curve, as terrorist behavior becomes more predictable with time.

Admittedly, a deterrence strategy might not stop all attacks; in fact, it might not stop attacks in which relatively simple devices are used to kill many people. Unfortunately, deterrence could also cause the attacker to change targets and/or methods resulting in a more damaging attack than the one that had been deterred. But the success of a defense-based deterrence strategy is not assessed by summing the costs; instead, it is assessed by whether, over the long term, the defender is better off with the strategy than without it.

Chapter 8

Creating a National Homeland Security Plan

Bruce Davis

It is time to create a National Homeland Security Plan (NHSP) on par with the National Response Plan (NRP). The National Strategy for Homeland Security; Homeland Security Act of 2002; and Homeland Security Presidential Directive-5 (HSPD-5), Management of Domestic Incidents, establish objectives for a national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur.[1] The NRP was created to establish a single, comprehensive approach to domestic incident management to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. By its very nature it tends to focus on coordinating the activities of the signatory Federal agencies during the response phase with less application to preventing the terrorist attack. This leaves a gap in National Security preparedness. This analysis paper addresses the intersection between homeland security and national security in the context of homeland defense and how a NHSP will help bridge that gap.

U.S. Northern Command (USNORTHCOM) is in the final steps of getting version 2.0 of the Department of Defense Homeland Defense and Civil Support Joint Operating Concept (DOD HD & CS JOC) approved by the Secretary of Defense. As part of Department of Defense (DOD) transformation, the family of Joint Operating Concepts (JOCs) describes how the Joint Force is expected to operate in the future and guide the development of future Joint capabilities. The DOD HD & CS JOC proposes that creating an NHSP is one way to strengthen National Security by defining roles and responsibilities at all levels of the government to address all threats to the nation.

[1] National Response Plan December 2004.

The Homeland is confronted by threats ranging from national security threats (for example, ballistic missile attack) to law enforcement threats (for example, bank robbery) (Figure 1). This is a conceptual spectrum with clear definitions of both ends and less clarity in the middle where the two blend together. In the middle is a "seam" of ambiguity where threats are neither clearly military wartime threats (requiring a military [DOD] response capability) nor clearly criminal type threats (requiring a non-military response capability from the Department of Homeland Security (DHS), the Department of Justice (DOJ), or other agency).[2] Within this overlap area are threats such as transnational terrorist groups that challenge the delineation of responsibility between DOD and DHS, DOJ, or other agencies because it is sometimes difficult to label them as either a national security threat or a law enforcement threat.

Defense of the Homeland involves a global, multi-domain battlespace. Within the context of a global battlespace (Figure 2) the joint operations area (JOA) is a multi-domain space with the Homeland at its core. The JOA expands and contracts in relation to the Joint Force Commander's ability to acquire and engage the adversary. Since the strategy is to engage adversaries before they gain access to the Homeland, areas of the JOA are often either in the Forward Regions or in the Approaches, or both.[3] The joint area of interest is the multi-domain space beyond the boundary of the JOA that is the source of indirect influence on the Joint Force Commander's mission.

Reducing uncertainty requires use and integration of existing and developing policy and guidance to clarify and codify roles, responsibilities, and an interagency concept of operation between DOD and non-DOD partners. A recommended approach is that DOD actively engage non-DOD partners using existing and developing policy and guidance to help develop a NHSP similar in concept to the NRP, but addressing detect, deter, prevent, or if necessary defeat versus post-attack roles and responsibilities.[4] The DOD HD & CS JOC also recommends that development and implementation of a NHSP would help cover the seam of uncertainty through the integration and coordination of

[2] Department of Defense Homeland Defense and Civil Support Joint Operating Concept V2.0.

[3] Strategy for Homeland Defense and Civil Support, June 2005.

[4] DOD HD & CS JOC.

Figure 1 National Challenge

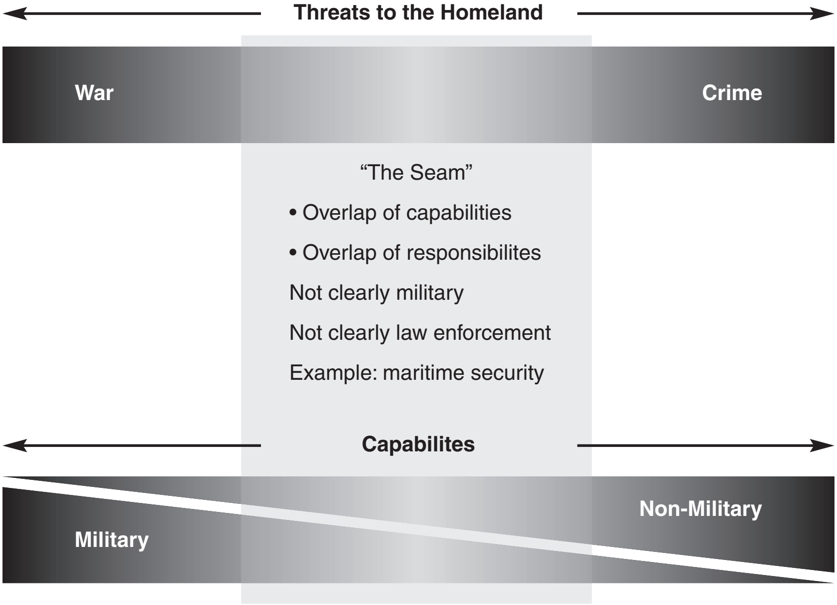
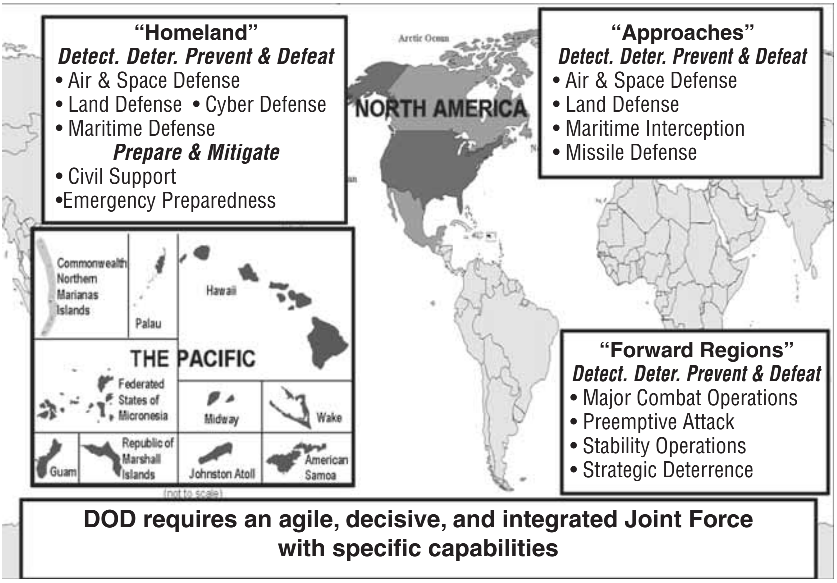

Threats to the Homeland
War
Crime
"The Seam"
• Overlap of capabilities
• Overlap of responsibilites
Not clearly military
Not clearly law enforcement
Example: maritime security
Capabilites
Military
Non-Military

Figure 2 DOD Strategic Concept, Active, Layered Defense



"Homeland"
Detect. Deter. Prevent & Defeat
- Air & Space Defense
- Land Defense • Cyber Defense
- Maritime Defense

Prepare & Mitigate
- Civil Support
- Emergency Preparedness

"Approaches"
Detect. Deter. Prevent & Defeat
- Air & Space Defense
- Land Defense
- Maritime Interception
- Missile Defense

"Forward Regions"
Detect. Deter. Prevent & Defeat
- Major Combat Operations
- Preemptive Attack
- Stability Operations
- Strategic Deterrence

DOD requires an agile, decisive, and integrated Joint Force with specific capabilities

planning, exercising, training, and operations with interagency partners to achieve desired outcomes.

The global war on terrorism (GWOT) requires a greater degree of interagency involvement and coordination than does conventional warfare. A challenge to achieving a wartime footing for DOD in terms of the GWOT is that many of the key “wartime” activities involve coordination and planning with other federal departments and agencies. In Homeland Security Presidential Directive (HSPD)-5, the President directed development of the NRP to align federal coordination structures, capabilities, and resources into a unified, all discipline, and all-hazards approach to domestic incident management. While preparations and plans for DOD to support civil authorities in the event of an attack are outlined in the NRP, there is no similar overarching national level plan that specifically coordinates the pre-attack actions of the U.S. government.

Development of an NHSP, that operationalizes the National Security Strategy (NSS) and helps define roles and responsibilities for DOD and non-DOD partners, would help clarify how operations will be conducted in the “seam” of overlapping responsibilities and capabilities. The NRP and National Incident Management System (NIMS) allow DHS to coordinate authorities, tasks, and procedures for all federal departments and agencies for post attack response measures. An NHSP would enable a coordinated national effort to do the same for pre-attack national security measures to detect, deter, prevent, or if necessary defeat external threats and aggression.[5]

This concept from the DOD HD & CS JOC does not specify the details of a NHSP. It is likely that in some areas, such as ballistic missile defense, DOD will be the lead and operate more or less autonomously. In other areas, such as maritime defense of the U.S., DOD may lead in some geographic areas and functions, while coordinating closely with one or more non-DOD agencies (for example the U.S. Coast Guard). In yet other areas, such as the GWOT where the National Counter Terrorism Center is responsible for developing an integrated national strategic-operational plan, DOD will contribute to an integrated national planning effort and may lead in some areas and support in other areas as that plan is implemented.

[5] DOD HD & CS JOC.

USNORTHCOM offers three different campaign frameworks[6] as fundamental to the discussion of the NHSP. All three campaign frameworks are founded on the central idea and strategic objective of this concept—dealing with threats to the U.S. as early and as far forward from the Homeland as possible, and in the event of successful attack or natural catastrophe, to support an integrated national response that occurs as quickly and effectively as possible. DOD plays a vital role in each campaign. The first campaign framework is the "Homeland Defense (HD) and Civil Support (CS) Campaign Framework" with DOD missions performed in each of the three regions to produce an active, layered defense of the Homeland. The second campaign framework is the "Homeland Security (HS) Campaign Framework" wherein the DHS, DOJ, or other non-DOD agency is designated as the lead or primary agency in conducting HS missions across several critical mission areas. The third campaign framework is the "National Security Campaign Framework" which encompasses the roles, missions, and actions of federal, state and local authorities, and other Government agencies at all levels in addressing threats to the Homeland.

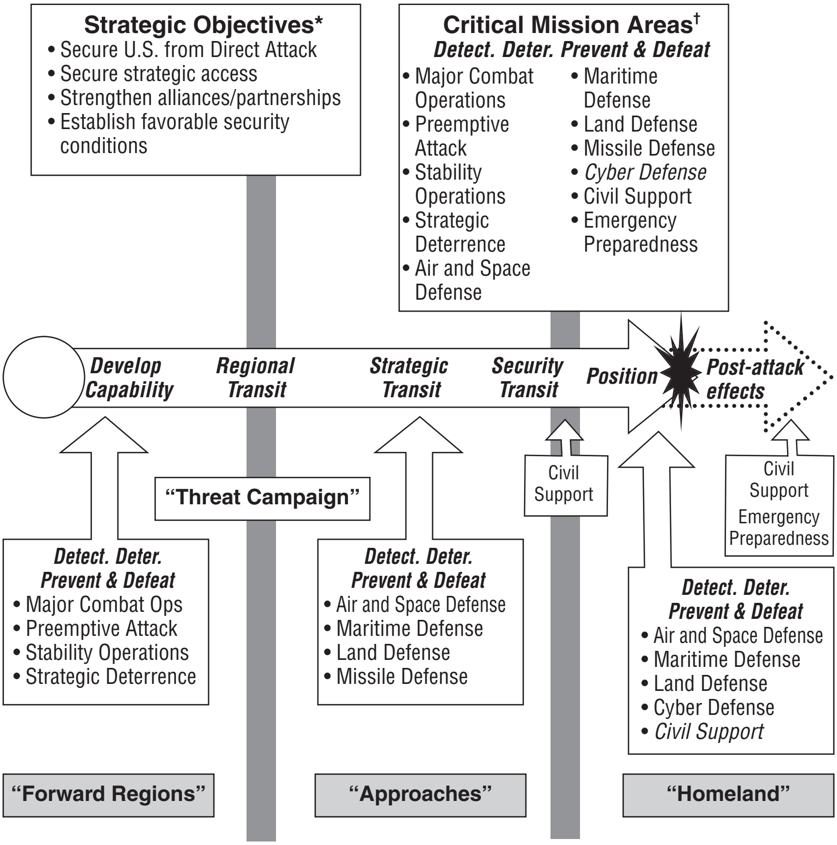
Homeland Defense and Civil Support Campaign Framework

The HD and CS Campaign Framework of an active, layered defense builds upon the National Defense Strategy strategic objectives and serves to conceptually depict how DOD will accomplish its HD and CS missions, and Emergency Preparedness planning activities across the threat spectrum in the Forward Regions, Approaches, and the Homeland.[7] This framework (for illustrative purpose only in Figure 3) emphasizes the critical importance of preventing attacks on the Homeland and mitigating and/or managing the consequences of the effects should they occur. To meet this complex challenge, planning and execution of military operations need to be integrated and synchronized within a larger national security strategy construct and conducted in coordination with other government agencies, allies,

[6] The figures associated with each of the three campaign frameworks are conceptual examples and are not all inclusive of DOD HD and CS actions and the overlap of those actions with non-DOD partners.

[7] DOD HD & CS JOC.

Figure 3 Homeland Defense and Civil Support Campaign Framework



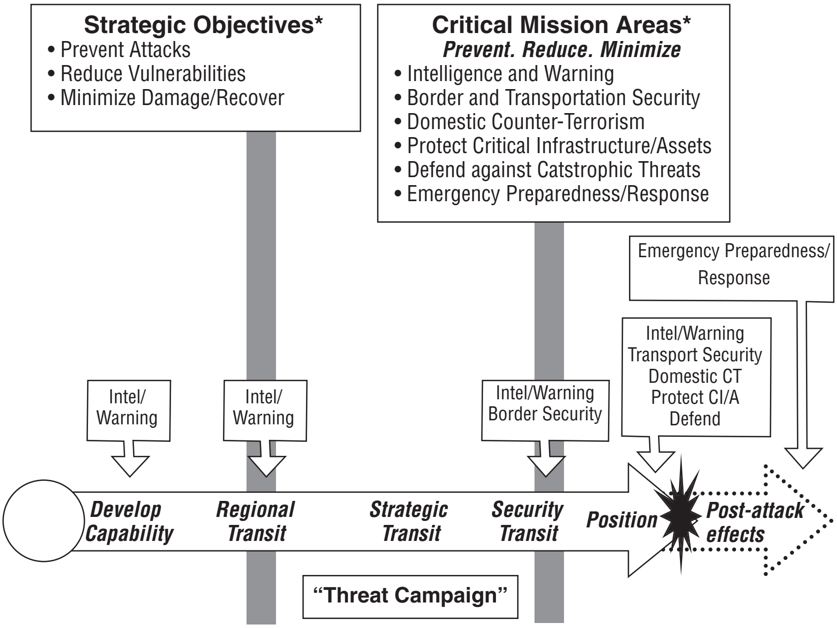
*from the National Defense Strategy. †from the DOD HLS JOC 1.0

and international partners in a broader "National Security Campaign." Integration and synchronization of HD operations and HS activities within the context of the National effort assure maximum and optimum resources against any designated threat.

Homeland Security Campaign Framework

The purpose of a HS campaign, as expressed in the National Strategy for Homeland Security (NSHS), is to mobilize and organize the Nation to secure the U.S. Homeland from terrorist attacks.

Figure 4 Homeland Security Campaign Framework


Strategic Objectives*
• Prevent Attacks
• Reduce Vulnerabilities
• Minimize Damage/Recover
Critical Mission Areas*
Prevent. Reduce. Minimize
• Intelligence and Warning
• Border and Transportation Security
• Domestic Counter-Terrorism
• Protect Critical Infrastructure/Assets
• Defend against Catstrophic Threats
• Emergency Preparedness/Response
Emergency Preparedness/ Response
Intel/Warning Transport Security Domestic CT Protect CI/A Defend
Intel/ Warning
Intel/ Warning
Intel/Warning Border Security
Develop Capability
Regional Transit
Strategic Transit
Security Transit
Position
Post-attack effects
"Threat Campaign"

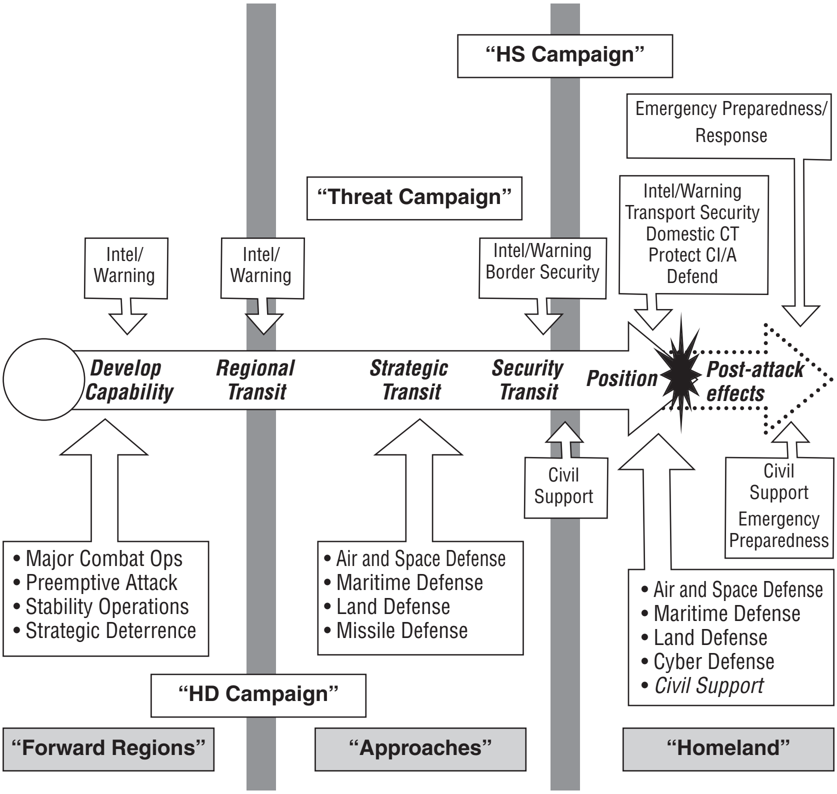
*from the National Strategy for Homeland Security

The NSHS establishes a foundation upon which to organize HS efforts and delineates the strategic objectives of HS; prevent terrorist attacks within the U.S., reduce America's vulnerability to terrorism and minimize damage and recover from attacks that do occur.

The NSHS also aligns and focuses HS functions into six critical mission areas: intelligence and warning, border and transportation security, domestic counter-terrorism, protecting critical infrastructure, defending against catastrophic threats, and emergency preparedness and response. The first three mission areas focus primarily on preventing terrorist attacks; the next two on reducing the Nation's vulnerabilities; and the final one on minimizing the damage and recovering from attacks that do occur. In this way, the NSHS provides a conceptual HS campaign framework to align the resources directly to the task of securing the Homeland.

Figure 4 displays, in general terms, an HS Campaign Framework based on the strategic objectives and the critical mission areas defined

Figure 5 National Security Campaign Framework



in the NSHS and imposed upon a generic threat campaign.[8] The critical mission areas are conceptually aligned with the major threat events (threat capability development through post-attack effects). This campaign framework applies when DHS, DOJ, or another non-DOD agency is the designated lead or primary agency. While not the lead in this campaign, DOD must maintain cognizance of the situation and leverage critical situational intelligence/warning.

National Security Campaign Framework

Threats such as transnational terrorist groups challenge the delineation of responsibility between DOD and DHS, DOJ, or other agencies

[8] DOD HD & CS JOC.

because it is difficult to label them as either a national security threat or a law enforcement threat. Determining whether a particular threat is one or the other will depend on circumstances such as current law, authority to act, magnitude of the threat, response capabilities required, and asset availability. A coordinated, integrated, and coherent national effort will be essential to secure the Homeland against all threats. The absence of a clearly defined border between the overlap of DOD and DHS, DOJ, or other agency capabilities and responsibilities allows latitude in determining which threats are best met by law enforcement and which will require military response, and conceptually substantiates the importance of a National Security Campaign Framework.[9]

Figure 5 illustrates how both DOD and non-DOD campaigns would work together to establish unified action against common threats and hazards in the Forward Regions, the Approaches, and the Homeland.

Having been part of discussing the need for a National Homeland Security Plan and later coordinating on its development within the DOD HD & CS JOC, the concept is sound and the product is feasible. For DOD conducting HD and CS operations, the strategic and operational context of integrated planning and conducting missions inside a broader National Security Campaign in coordination with non-DOD and international partners has significant implications. The first is the acknowledgement of other actors conducting parallel efforts to protect the U.S. and the challenges and opportunities this national security partnership presents. The main challenge is coordinating and integrating, through formal and informal agreements, the activities of multiple federal, state, and local actors involved and operating in the same battle space. Because the structure of the government makes unity of command impractical with this coalition of actors, coordination must be accomplished at all levels through formal and informal agreements. However, this spectrum of actors and capabilities also presents the opportunity for DOD and the Joint Force Commander to leverage cooperation to increase situational awareness, mitigate capability gaps in the Joint Force, and synchronize a more effective response to emerging threats. Interoperability and interagency coordination are key considerations in maximizing these opportunities.

[9] DOD HD & CS JOC.

It is also important that it not be primarily a DOD plan. That could be problematic with the other federal agencies. It will succeed as a coordinated national effort to harness the 32 signatory agencies into one unified national effort to shape the security environment with unity of effort providing unity of results. It must be a global approach for integrating U.S. capabilities to promote the active layered defense, defeating threats as far from our shores as possible. The NHSP will need to clearly identify and define roles and responsibilities to avoid overlap and identify gaps in strategy, policy and capabilities. As contained within the USNORTHCOM concept it will be a plan for detecting, deterring, preventing, and defeating external threats and aggression. National security requires national actions and agencies that traditionally played only a domestic role increasingly have a role to play in our foreign and security policies. This requires us to better integrate interagency activity both at home and abroad. Finally the National Homeland Security Plan must be an overarching plan to coordinate all elements of national power, addressing challenges with the appropriate tools, to ensure the best mix of Diplomatic, Information, Military, and Economic power.[10]

The USNORTHCOM recommendation, as articulated by Admiral Timothy J. Keating in his December 6, 2006 memo to the Deputy Secretary of Defense continued to advocate that the "best way forward is through an NHSP Working Group jointly established by the National Security Council and the Homeland Security Council. This Working Group would be chartered to develop a draft National/Homeland Security Presidential Directive (NSPD/HSPD) that assigns roles for creating an NHSP."[11] The importance of this interagency group is to establish the interagency buy-in and build a sense of urgency. As conceptualized by USNORTHCOM, an NHSP would facilitate interagency coordination and collaboration by defining roles and responsibilities for detecting, deterring, preventing and defeating threats and aggression to carry out the NSS as an integrated national effort between DOD and non-DOD partners in homeland defense.

[10] USNORTHCOM Point Paper on the National Homeland Security Plan (NHSP) Initiative V2.6.

[11] Admiral Timothy J. Keating memo to the Deputy Secretary of Defense, December 6, 2006.

Chapter 9

The Case for a New Guard Operational Model

Lawrence J. Korb and Sean E. Duggan

The controversy in mid-May 2007 over whether the Kansas National Guard had sufficient troops and equipment at their disposal to deal with the tornado that devastated Greensburg exposed the National Guard's looming personnel and equipment crisis. While the corresponding predicament in the Army's active component has received a great deal of attention prior to the Kansas disaster, the crisis in the reserve component has gone largely unnoticed. Lt. General Steven Blum, the chief of the National Guard, summarized the situation when he said the Guard is "in an even more dire situation than the active Army, but both have the same symptoms; I just have a higher fever."[1]

To maintain the continued occupation of Iraq and our increasing military commitment to Afghanistan, the Pentagon has had to dramatically increase its reliance on the reserve forces (both the National Guard and Reserves). In 2005 alone, 14 of the Guard's 38 brigades (including nine of the Army National Guard's 16 Enhanced brigades) were deployed either to Iraq or Afghanistan; seven Guard brigades served in Iraq and another two served in Afghanistan — for a total of more than 35,000 combat troops. That same year, 46 percent (or about 60,000) of the troops in Iraq were from the reserve component.[2]

Moreover, to continue the current policy the Department of Defense will have to continue to rely on the reserves, most likely increasing the involvement of the Army National Guard in the coming year.[3] Four more Guard brigades—more than 13,000 troops—were deployed to Iraq in early 2008, shortening their time between deployments to meet

[1] "General: Guard Units not Ready for Combat," *USA Today*, August 1, 2006.

[2] Scott Tyson, Ann, "Possible Iraq Deployments Would Stretch Reserve Force," *Washington Post*, November 6, 2006.

[3] Congressional Budget Office, "The Effects of Reserve Call Ups on Civilian Employers," May 17, 2007.

the demands of the latest escalation. Ground troop levels in both theaters of war could not be sustained at the current rate without the numbers and skills provided by the men and women of the Army National Guard.

The current predicament of the Army National Guard reflects the changing role of the force itself—shifting the reserve component's dual-purpose balance between domestic commitments and overseas imperatives decisively toward the latter. The heavy reliance on the Army National Guard, its combat units (Enhanced Separate Brigades) in particular, for overseas operations represents a fundamental change from the Guard's planned role as a strategic reserve force whose wartime function was to deploy in the later stages of a major conflict if needed.

The current transition from a strategic to an operational reserve has not only drastically altered the role of the National Guard but has also devastated its personnel and equipment readiness. As former Defense Secretary Melvin Laird has noted, the Guard and the all-volunteer force are in uncharted waters as we prosecute the long war.[4] Frankly speaking, the Guard cannot perform both its domestic and overseas missions at this pace. As long as the Guard's concurrent domestic and overseas responsibilities stretch the force thin, a new operational model for the reserve component is needed.

After outlining the current overuse of the reserve component and its consequences on our national security and homeland defense, we will then make the case to establish a non-deployable 'Home Guard' to ensure that the states are never left without adequate military resources. To do any less would be endangering our national security at home and abroad.

Overburdened and Overused

While the total Army (comprised of the Active, Guard and Reserves components) consists of 1.1 million men and women, nearly half of these troops are in the selected reserves. Of these 1.1 million, the

[4] Laird, Melvin, "National Guard Needs Adequate Funding," *The Milwaukee Journal Sentinel*, May 12, 2007.

authorized end strength for the Army National Guard is 350,000 and the reserves, 200,000.

When the all-volunteer force was created, the National Guard was designed to act as a strategic reserve for the active component, which would serve as the ready force. The reserve component was meant to act as a bridge to conscription should a protracted conflict occur. With the Pentagon straining to keep force levels high in Iraq, the Guard is being used as an operational reserve, alternating deployments with the active force. The nation's current reliance on the Guard to fight two major ground wars is unprecedented.

Consider that since the attacks of September 11: every National Guard enhanced brigade has been deployed overseas at least once and two have already been deployed twice; one brigade combat team from Minnesota, the 34th Infantry Division, has been in Iraq since March 2006 and did not return home until summer of 2007; all told the total number of reservists called up through March 2007 exceeded 580,000,[5] of those more than 417,000 National Guard and Reservists—or about 80 percent of the members of the Guard and Reserve—have been deployed to Iraq or Afghanistan; of the 417,000, 84,200 troops (or 20 percent) have been deployed more than once.[6]

Moreover, the President's latest escalation has forced the Pentagon to recall to active duty several thousand Guard personnel who have already served in Iraq and Afghanistan. To do this, the Bush Administration announced in January 2007 that it was revising rules that limited call-ups of Guard members. The Pentagon's previous policy limited involuntary mobilizations of Guard members to no more than 24 months every five years.

Units that have recently returned include the 39th Infantry Brigade from Arkansas, the 45th Infantry Brigade from Oklahoma, the 76th Infantry Brigade from Indiana, and the 37th Infantry Brigade Combat Team from Ohio. According to standard practice of no more than one deployment every five years, none of these units should have been redeployed before 2010 at the earliest. To maintain this latest escalation,

[5] Congressional Budget Office, "The Effects of Reserve Call Ups on Civilian Employers," May 17, 2007.

[6] Website of House Majority Leader Steny Hoyer, see: http://majorityleader.house.gov/docUploads/Iraqbythenumbers031907.pdf.

however, none of these four units was home more than three years and one unit, the 76th Infantry Brigade from Indiana, received only two and a half years between deployments. Violating the Pentagon's own rule will undoubtedly have adverse consequences for the men and women of these units.

In fact, some of these effects have already surfaced. Lengthy and repeated tours of duty that violate longstanding deployment policy have taken a grave toll on the people of the Guard and Reserve as well as the families that they leave behind. As Michael Evans, Regional Family Program Manager for the U.S. Army Reserve Command, noted before Commission on the Guard and Reserve, "we recruit soldiers, but we retain families."[7] Due to these unexpectedly long periods of separation, recruitment and retention are bound to suffer. The National Military Family Association released a survey on deployment cycles that concluded that, "Army National Guard and Reserve families reported the greatest stress concerning deployment length. Their service members typically experience family separations of close to 18 months."[8]

Echoing this concern, the Commission on the National Guard and Reserve recently concluded, "overall, if the reserve component, including the National Guard, continues its high operational tempo, current indicators cast considerable doubt on the future sustainability of recruiting and retention, even if financial incentives continue to increase."[9] Not surprisingly the Army National Guard fell short of its recruiting goals in 2005 and 2006.[10]

The case of the 39th Infantry Brigade is illustrative of this phenomenon. This unit of the Arkansas National Guard, which returned from Iraq in March 2005 after a one-year tour in country and 18 months on active duty, deployed to Iraq in December 2007, about two and a half years after returning. Of particular concern to Capt. Christopher Heathscott, a spokesman for the Arkansas National Guard, is that the reality of going to Iraq next year could cause some Arkansas reservists not to re-enlist this year. "Over the next year roughly one-third of the

[7] http://www.cngr.gov/May%2015-17/Evans%20Testimony.pdf.

[8] National Military Families Association, "Cycles of Deployment," see: http://www.nmfa.org/site/DocServer/NMFACyclesofDeployment9.pdf?docID=5401.

[9] Commission on the National Guard and Reserves, "Strengthening America's Defenses in the New Security Environment," March 1, 2007.

[10] Hall, Kristin, "Numbers Up for Guard Recruitment," *Associated Press*, May 15, 2007.

soldiers in the 39th will have their enlistment contracts expire or be eligible for retirement," Captain Heathscott noted.[11]

Further compounding these problems, unpredictable and irregular reserve deployments have had a significant impact on reservists' civilian employment. As a recent Congressional Budget Office report noted, small businesses that employ reservists and those troops who are self-employed are logically the most impacted by current Guard and Reserve deployments. The report went on to note that as many as 28,000 reservists hold key positions in small businesses and an additional 53,000 reservists are self-employed. "Many reservists, when they joined the military, probably did not anticipate the increased frequency and duration of the activations that have occurred during the past several years," CBO reported, "and may be finding those mobilizations more disruptive than they might have expected."[12]

Underequipped and Underprepared

The equipment situation for the National Guard is also in tatters. The Army Guard began the wars in Afghanistan and Iraq with its units short tens of thousands of soldiers, or about 15 percent to 20 percent, and equipped with only 65 percent to 70 percent of their required wartime needs. Those shortages have deepened as people and equipment are borrowed from units staying home to fill out those about to go overseas—a process known as "cross-leveling."[13]

"Our issue is that we are shortchanged when it comes to equipment," said Col. Jon Siepmann, a California Guard spokesman. "We have gone from a strategic reserve to a globally deployable force, and yet our equipment resources have been largely the same levels since before the war."[14] According to Lt. General Blum, current equipment levels are in fact much worse than before 2001. Today, the Army National Guard presently has on hand only 30 percent of its essential

[11] Cloud, David S., "Units of National Guard May Return to Iraq Early," *New York Times*, February 22, 2007.

[12] Congressional Budget Office, "The Effects of Reserve Call Ups on Civilian Employers," May 17, 2007.

[13] GAO, "Reserve Forces Army National Guard's Role, Organization, and Equipment Need to be Reexamined," October 20, 2005.

[14] Saulny, Susan and Jim Rutenburg, "Kansas Tornado Renews Debate on Guard at War," *The New York Times*, May 9, 2007.

equipment here at home while 88 percent of the Army National Guard that is in the United States is very poorly equipped.[15] Nearly 9 out of every 10 Army National Guard units that are not in Iraq or Afghanistan have less than half the equipment needed to respond to a domestic crisis and less than 45 percent of the Air National Guard's units have the equipment needed to deploy.[16]

This is "the first time such a shortfall in equipment readiness has occurred in the past 35 years," according to Lt. General Blum.[17] He estimated the total cost of the shortfall at about $36 billion.[18] Guardsmen lack training on even the most essential equipment, including those in units about to deploy. Cases in point: one-third of the Oklahoma National Guard is lacking M-4 rifles and the Arkansas National Guard is short 600 rifles for the state's 39th Brigade Combat Team.[19]

Troop Siphoning

The process of cross-leveling is not isolated to equipment. Historically the Army National Guard has had more combat units than it has had personnel to man them, resulting in undermanned units. A recent Congressional Budget Office (CBO) report outlines the consequences of this "overstructure." In 2002, for example, the Guard's divisions and separate brigades required a total of nearly 200,000 personnel and were authorized to have almost 195,000 personnel, but they had only 172,000 personnel assigned to them—resulting in an 88 percent "fill rate" compared with the authorized level.[20] This degree of overstructure is equivalent to about six separate brigades that could not be manned. While this gap was spread out over all the Guard's combat forces, over time, the shortages created have resulted in grave consequences.

To understand overstructure's ramifications, one needs to understand that upon mobilization, units must be brought to at least 100

[15] Brown, Drew, "Wars are Depleting the National Guard's Equipment Stocks at Home," *McClatchy Newspapers*, January 31, 2007.

[16] Ibid.

[17] Ibid.

[18] Free Market News Network, "Chief: National Guard Funds Lacking," May 15, 2007.

[19] Cloud, David S., "Units of National Guard May Return to Iraq Early," *New York Times*, February 22, 2007.

[20] Congressional Budget Office, "Issues that Effect the Readiness of the Army National Guard and Army Reserve," May 16, 2007.

percent of its authorized strength before deployment. In fact, units are frequently deployed with 105 percent of its authorized strength to hedge against loss of troops due to sickness, injury, hardship or other reasons. As a result of overstructuring, the 100-105 percent requirement necessitates transferring additional personnel from other units into the new unit. To illustrate this practice, the CBO report outlined:

> A hypothetical force of 10 brigades, each having 1,000 authorized positions but only 900 assigned personnel. In order to deploy one brigade, it would be necessary to cross-level 100 personnel from a second brigade (or combination of brigades, although for simplicity, this example assumes only a single donor). Deploying the first unit at its full authorized strength of 1,000 personnel would thus mean reducing another brigade to only 800 personnel. The second brigade would eventually receive 100 personnel back, but they would be ineligible for another deployment. To deploy that second brigade, 200 personnel would have to be cross-leveled into that unit, leaving a third brigade with only 700 personnel available, and so on. Ultimately, the 10th brigade would be unable to deploy because it would have no personnel available.[21]

While cross-leveling troops has enabled commanders to lead fully manned units in both Iraq and Afghanistan this process not only causes a loss of cohesion in the receiving unit but, perhaps more significantly, it also causes the donor unit to become even more undermanned than before; thus creating a vacuum throughout the entire Guard.[22]

Leaving Homeland Security Vulnerable

Even as significant numbers of personnel and equipment are cross-leveled to forwardly deployed troops in Iraq and Afghanistan, the Army National Guard's responsibility for homeland defense and civil support has remained constant. As a result, the Guard's evolving role from a strategic reserve to an operational reserve has had a significant impact on its ability to perform its domestic missions, something both

[21] Ibid.

[22] Ibid.

Republican and Democratic governors have complained about to the president and the secretary of defense in recent years.

In the pre-9/11 security environment, it was assumed that the National Guard could perform its domestic roles with the personnel and equipment it was supplied with for its war fighting missions.[23] Even a cursory examination of the Guard's equipment situation demonstrates that the force's current operational model for performing both its domestic and international roles is unsustainable.

As noted above, in order to address equipment requirements for current operations in Iraq and Afghanistan, the Army now requires that reserve (and active) units leave behind certain essential items that are in short supply. These key items include tanks, trucks, up-armored humvees and as well as long-range surveillance and communications systems.

This process is meant to assure that follow-on units are 100 percent equipped. The procedure also reduces the amount of equipment that has to be transported from the United States to Iraq or Afghanistan, better enables units to meet their deployment dates, and maintains stocks of essential equipment in theater where it is most needed.[24] But as a 2005 Government Accountability Office report notes, "while this equipment approach has helped meet current operational needs, it has continued the cycle of reducing the pool of equipment available to nondeployed forces for responding to contingencies and for training."[25]

The response to Hurricane Katrina revealed these serious shortcomings in the equipping of Guard units for the Homeland Security and Defense departments. According to WGNO, a Louisiana ABC affiliate, four weeks before the hurricane struck the Gulf Coast, Lt. Colonel Pete Schneider of the Louisiana National Guard complained that when guard members left for Iraq in October 2003 they took a lot of needed equipment with them. Specifically, they took dozens of high-water vehicles, Humvees, refueling tankers, and generators.[26]

[23] GAO, "Reserve Forces Army National Guard's Role, Organization, and Equipment Need to be Reexamined," October 20, 2005.

[24] DOD Directive 1225.6, Equipping the Reserve Force, April 7, 2005.

[25] GAO, "Reserve Forces Army National Guard's Role, Organization, and Equipment Need to be Reexamined," October 20, 2005.

[26] Block, Schatz, Fields, Cooper, "Behind Poor Katrina Response, A Long Chain of Weak Links," *Wall Street Journal*, September 6, 2005.

Like Lt. Colonel Schneider's warnings, similar reports of critically depleted equipment stocks by the Louisiana Army National Guard were ignored. As of July 2005, the Louisiana Guard reported that it had less than 5 percent of the required amount (or a quantity of fewer than five each) of more than 220 critical items. Among these 220 high-demand items were generators, trucks, and radios—items that would become invaluable in the wake of Katrina.[27]

As a Congressional Research Service report released in the wake of the disaster noted, the inability to carry out relief operations centered as much upon the unavailability of equipment as personnel. The report notes that:

> National Guard units responding to Katrina did not have adequate numbers of tactical radios or High Mobility Multi-Wheeled Vehicles adapted for high water operations because this equipment was in Iraq. Another example noted is that of the 101st Air Assault Division, based in Ft. Campbell, KY. This division, which has the largest number of transport helicopters of any Army unit, was not deployed to Katrina operations because it is in the process of deploying to Iraq.[28]

Contrary to official statements by the Bush Administration, a dearth of ready troops was also to blame. Had a substantial number of essential Guard units been readily available, logistical gaps that occurred during Katrina operations would have been mitigated. Fort Polk—which is about 270 miles northwest of New Orleans—is home to the 4th brigade, 10th Mountain Division. Immediately after Katrina struck, the 4th brigade could send only a few dozen soldiers manning purification equipment and driving half-ton trucks filled with supplies and equipment. According to *The Wall Street Journal*, a week after Katrina hit, the Army was reluctant to commit this active unit because the 4th brigade, which numbers several thousand soldiers, was in the midst of preparing for an Afghanistan deployment in January 2006.[29]

[27] GAO, "Reserve Forces Army National Guard's Role, Organization, and Equipment Need to be Reexamined," October 20, 2005.

[28] Congressional Research Service, "Hurricane Katrina: DOD Disaster Response," September 19, 2005.

[29] Block, Schatz, Fields, Cooper, "Behind Poor Katrina Response, A Long Chain of Weak Links," *Wall Street Journal*, September 6, 2005.

Instead, the Pentagon chose to send some 7,500 soldiers from the active Army's 1st Cavalry Division at Fort Hood, TX and the 82nd Airborne Division from Fort Bragg, NC, along with Marines from California and North Carolina—a factor that lengthened their arrival time on the ground in Louisiana by several days (soldiers from the 82nd Airborne Division—nicknamed the ready division—are meant to be able to deploy anywhere in the world in 18 hours).[30]

Moreover, at the time of the disaster over a third of the total Guard of Louisiana and Mississippi, some 5,900 troops, were deployed to Iraq or Afghanistan. And according to Dave McGinnis, former Chief of Staff of the National Guard Association of the United States, the problem for Louisiana and Mississippi was not how many troops were in Iraq at the time but rather the kind of soldiers who were there. As McGinnis noted, "It's combat brigades, which are the types of units you need in these situations," that were overseas, he said.[31]

Unfortunately, symptoms of the pre-Katrina equipment shortages are already beginning to reappear elsewhere. Efforts to rebuild the tornado-ravaged community of Greensburg, Kansas have revealed that reconstruction and crisis management has been constrained by a lack of National Guard equipment. According to Kansas Governor Kathleen Sebelius, the state's National Guard has only about 40 percent of the equipment it is allotted because much of it has been sent to Iraq.[32]

Much of the state's Guard equipment that is normally positioned around Kansas to respond to emergencies and natural disasters is gone. As Sebelius noted, a lack of immediate access to things like tents, trucks, and semi trailers will really handicap the rebuilding effort.[33] According to Kansas Adjutant General Maj. Gen, Tod Bunting, normally the Kansas Guard would have about 660 Humvees and more than 30 large trucks to traverse difficult terrain and transport heavy equipment. When the tornado struck the Guard had a mere 350 Humvees and 15 large trucks.[34] As State Senator Donald Betts Jr. put

[30] Ibid.

[31] Moniz, Dave, "Pentagon to Send 10,000 National Guard Troops," *USA Today*, August 31, 2005.

[32] "Iraq War Hampers Kansas Cleanup," May 6, 2007, see: http://www.kcbs.com/pages/424076.php?contentType=4&contentId=472199.

[33] Ibid.

[34] Saulny, Susan and Jim Rutenburg, "Kansas Tornado Renews Debate on Guard at War," *The New York Times*, May 9, 2007.

it: "We should have had National Guard troops there right after the tornado hit, securing the place, pulling up debris, to make sure that if there was still life, people could have been saved. The response time was too slow, and it's becoming a trend. We saw this after Katrina, and it's like history repeating itself."[35]

Sadly the problems plaguing the Kansas Guard are not unique. Despite a signed a letter by all 50 governors to President Bush asking for the immediate re-equipping of Guard units sent overseas the Guards of California, Florida, Arizona, New Jersey, Idaho, Louisiana, South Carolina, Oklahoma, Michigan, New Mexico, Oregon, and Arkansas also have less than half the equipment they need to deal with natural disasters. As Defense Secretary Robert Gates has acknowledged, Army National Guard equipment levels are the lowest they have been since 9/11. In fact, the Commission on the National Guard and Reserves reported in March 2007 that nearly 90 percent of National Guard units are not ready to respond to crises at home and abroad.[36]

Faced with shortages, states have been forced to rely more on existing compacts with their neighboring states in order to mitigate the dangers of being caught off guard by a natural disaster, terror attack, or civil disturbance. Such compacts represent mutual assurances of aid, relief, and troop commitments should a contingency occur. Yet as Major General Melvyn Mantano, the former head of the New Mexico National Guard, notes, "these compacts are practically nullified now because all states have people in" Iraq. "If you have four or five states around you, where are they going go get their equipment from? Because they all have been deployed."[37]

Toward a New 'Home Guard'

This situation clearly cannot persist without serious adverse consequences to our national security and our National Guard. According to Arnold L. Punaro, Chairman of the Commission on the National Guard, "we cannot sustain the [National Guard and Reserves] on the course we're on."[38] As this nation conducts what the

[35] Ibid.

[36] Commission on the National Guard and Reserves, Second Report to Congress, March 1, 2007.

[37] Spiegel, Peter, "Guard Equipment Levels Lowest Since 9/11," *Los Angles Times*, May 10, 2007.

[38] Ann Scott Tyson, "Shortages Threaten Guard's Capability," *The Washington Post*, March 2, 2007.

administration refers to as the global war on terrorism, the stress on the Guard will not change. It is therefore necessary to construct a new model to establish in each state an adequately trained and equipped, non-deployable Home Guard.

Such a force would consist of volunteer doctors, nurses, construction workers, firefighters, police officers, communications experts, city planners, engineers and social workers, among others. While President Bush has recognized the need for such a force, he has not followed up effectively on his 2002 State of the Union initiative to create a major new citizen service corps, the USA Freedom Corps, which would call on all Americans to serve their nation for the equivalent of two years (4,000 hours) over their lifetimes.

Fortunately, models for such a non-deployable corps of volunteers already exist. Twenty-three states and Puerto Rico have federally authorized military reserve forces, or State Military Reserves, consisting of thousands volunteer citizen-soldiers. These state reserves, which are called by different names in every state, are essentially Home Guards. They consist of several thousand volunteer citizen-soldiers who are subject to be called to state active duty by their respective state adjutant general. Generally, volunteers have previous military experience, some however, enlist to share their professional skills attained in civilian careers.

Units in Virginia and California are exemplary. The California State Military Reserve (CSMR) provides services for its National Guard including training, preparation for mobilization and deployment, and medical assistance. State reservists also fill in for the National Guard in its defense support to civil authorities during state emergencies such as natural or manmade disasters and civil disorders in case the Guard is mobilized overseas. California volunteers are a non-expeditionary force and thus cannot be called on for service outside of the country. However, members of the CSMR were mobilized to provide emergency building damage assessments in the wake of Hurricane Katrina; such cooperation provides an ideal alternative to traditional state to state relief compacts.

The 7,000 plus strong Virginia Defense Force (VaDF) is another example. Like the National Guard, VaDF is a branch of the Virginia Department of Military Affairs, trains monthly at Virginia National

Guard armories, and is under the overall command of Virginia adjutant general. Unlike the National Guard, VaDF troops are reserved for in-state duty to ensure Virginia is never left without adequate military forces in the event of partial or full mobilization of the Virginia National Guard to federal service. While these troops are paid if called to state active duty, they are volunteer personnel who do not receive pay for monthly training or annual field exercises. Last year, the VaDF provided 69,000, or $1.3 million worth of free man-hours—performing eight homeland-security measures, including crowd control and catastrophic disaster response planning.

With no end in sight for the Army's reliance on the National Guard for its overseas missions, the president should ask the Congress to increase the budget of the Department of Homeland Security by at least $10 billion, the cost of one month's operations in Iraq. This would provide adequate funding for training and equipping Home Guards in every state. The cost of one month's operations in Iraq is a small price to pay to protect the homeland in the event of another catastrophic natural disaster or terror attack while making the American people feel that they are a part of this long war.

Chapter 10

Homeland Security and the Protection of Critical Energy Infrastructures: A European Perspective[1]

Heiko Borchert and Karina Forster

Homeland security is about the nexus between new national and international security risks, the way our states prepare themselves to deal with these risks and the resulting political leeway. States that remain vulnerable at home cannot assume a global leadership role.

The European Union (EU) assumes to be a global player. Despite ongoing efforts to improve the national security of EU member states, the region remains vulnerable. There is no better issue to illustrate Europe's vulnerability than energy security in general and energy infrastructure security in particular.

EU member states are energy-import dependent and rely on the stability of those countries, that harbor energy resources and critical energy infrastructures. Extracting energy resources, refining and transporting them to consumer markets and distributing energy products depends on a functioning energy infrastructure. For example Europe transports 85 percent of its gas imports by pipeline.[2] This energy infrastructure becomes even more important as the EU tries to diversify its energy resource imports and turns to suppliers that are further away. Finally, the EU aims at establishing a common European market for gas and electricity. In this context the creation of a cross-border emergency management framework to deal with infrastructure-related incidents becomes indispensable but remains to be established.

[1] This paper was extracted from the authors' study on energy infrastructure protection commissioned by the Swiss Ministry of Foreign Affairs and does not necessarily reflect the official position of the Swiss government.

[2] Energy Sector Inquiry. DG Competition Report, SEC(2006) 1724, Brussels, January 10, 2007, p. 25.

There is thus a clear link between energy infrastructure security and European homeland security. So far, however, energy issues are a matter of competition and environmental policy, rather than security policy. This is a serious problem for Europe.

This paper argues that Europe's current competition-based approach is insufficient to address the homeland security tasks posed by energy infrastructure security. The EU should acknowledge that the global energy supply chain is dominated by power and monopolies that benefit producing countries rather than competition and market liberalization. Therefore the EU should engage in creating an appropriate international set up to address energy infrastructure security.

With regard to the regulatory environment, the EU should harmonize and further develop existing safety and security standards. These standards should also receive more attention when providing stimuli for energy infrastructure investments. Finally, the EU must back its soft power approach to energy security by credible hard power and improve cross-border emergency management for energy infrastructure-related incidents.

The paper starts with a brief outline of current European activities in the field of critical infrastructure protection (CIP). Then we portray energy infrastructure security as a European homeland security challenge. We conclude by submitting concrete proposals for EU action to advance energy infrastructure security.

Europe's Approach to Critical Infrastructure Protection

According to the European Commission critical infrastructures "consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States."[3] The Commission has identified energy, nuclear industry, information and communication technologies, water, food, health, the financial sector, transportation, the chemical industry, space and

[3] Critical Infrastructure Protection in the fight against terrorism, COM (2004) 702, Brussels, October 20, 2004, p. 3.

research facilities as critical infrastructure sectors.[4] To advance their protection the Commission has proposed the European Program for Critical Infrastructure Protection, a directive for identifying European critical infrastructure, the creation of a new information network, funding alternatives, and new research opportunities.

- *European Program for Critical Infrastructure Protection (EPCIP)*
  The Commission presented the EPCIP in December 2006 after two years of preparatory work. The EPCIP provides a methodology to identify European critical infrastructures. These are infrastructures "which are of highest importance for the Community and which if disrupted or destroyed would affect two or more Member States or a single Member State if the critical infrastructure is located in another Member State."[5] The EPCIP also includes an action plan and addresses the role of contingency planning and CIP cooperation with third countries.

- *Directive for European Critical Infrastructure*
  The directive sets out criteria to identify European critical infrastructure. It is up to the member states to identify critical infrastructure on their own territory and outside their territory. Based on their compilation, the Commission will propose a list of European critical infrastructures.[6] In addition, the directive asks member states to make sure that owners and operators of European critical infrastructure establish and update operator security plans.

- *Rapid Alert Information Exchange*
  To complement existing networks for emergency management information exchange, the European Commission has proposed the critical infrastructure warning information network (CIWIN), "which could stimulate the development of appropriate

[4] Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, COM (2006) 787, Brussels, December 12, 2006, p. 21. In addition, many EU members also identify government structures and emergency responders as critical infrastructure sectors.

[5] European Program for Critical Infrastructure Protection, COM (2006) 786, Brussels, December 12, 2006, p. 4.

[6] It remains open, however, how genuine European aspects will be taken into account in this process.

protection measures by facilitating an exchange of best practices." Right now, a team led by Unisys Belgium, which had won the contract,[7] is conducting interviews in order to identify EU member states' expectations *vis-à-vis* CIWIN.

- *Funding*
  Under the program "Prevention, Preparedness and Consequence Management of Terrorism" the Commission provided €3.7 million in 2005 mainly for preparatory actions. On February 6, 2007 the Commission launched a new call worth €3 million for projects to enhance protection measures for critical infrastructure, risk mitigation strategies, the development of contingency plans or the development of common security standards.[8]

- *Research*
  As part of the new 7th Research Framework Program[9] security research has a dedicated CIP focus. In addition, other program areas such as information and communication technologies (e.g. intelligent infrastructures), energy (e.g. smart energy networks), transport (e.g. support for the European global satellite navigation system Galileo and EGNOS) or space (e.g. development of satellite-based and in-situ monitoring and early-warning systems) are relevant for CIP as well.[10]

Energy Security and European Homeland Security

Oil and gas are dominating Europe's energy mix. In 2000, 38 percent of Europe's primary energy needs were satisfied by oil and around 23 percent by gas. This is likely to change until 2030 when oil is expected to account for 34 percent and gas for 27 percent.

[7] See: http://ec.europa.eu/justice_home/news/tenders/2006_S044_045852/invitation_tender_en.pdf http://www.dgmarket.com/eproc/np-notice.do?noticeId=1512748.

[8] See: http://ec.europa.eu/justice_home/funding/epcip/funding_epcip_en.htm#.

[9] Seventh Framework Program of the European Community for research, technological development and demonstration activities (2007-2013), Decision No. 1982/2006/EC of the European Parliament and of the Council, December 18, 2006, OJ L 412, December 30, 2006, pp. 14-27.

[10] Before launching the 7th Research Framework Research the Commission used the Preparatory Action on Security Research to launch infrastructure relevant projects such as the VITA project (Vital Infrastructures Threats and Assurance) to analyze threats to and assurance and protection of highly networked infrastructures. See http:// ec.europa.eu/ enterprise / security/doc/project_flyers/766-06_vita.pdf.

More important, Europe's energy import dependence is projected to grow. In 2000 Europe imported around half its energy needs from abroad with Russia, Norway, North Africa and the Persian Gulf as the key suppliers. The spur in gas demand is very likely to increase gas import dependence from around 50 percent in 2000 to over 84 percent in 2030. By then 93 percent of Europe's oil demand will be satisfied by imports compared to about 76 percent in 2000.[11]

The projected shift in Europe's energy mix towards increased gas demand has strategic consequences. On the one hand, it means that key gas suppliers such as Russia and Algeria, which have formed a strategic partnership in mid-2006 between Gazprom and Sonatrach, will gain in relative importance *vis-à-vis* oil suppliers and are likely to become Europe's most important gas suppliers. On the other hand, it can be speculated how the influence of these suppliers will affect the transatlantic partnership.[12]

The Complexity of Energy Infrastructure Security

Energy infrastructure security must be understood as a holistic approach that looks at ends, ways and means to detect and explore natural energy resources and to refine, store, transport, and distribute the relevant products. As our model of analysis (Figure 1) makes clear several analytical dimensions need to be taken into account:

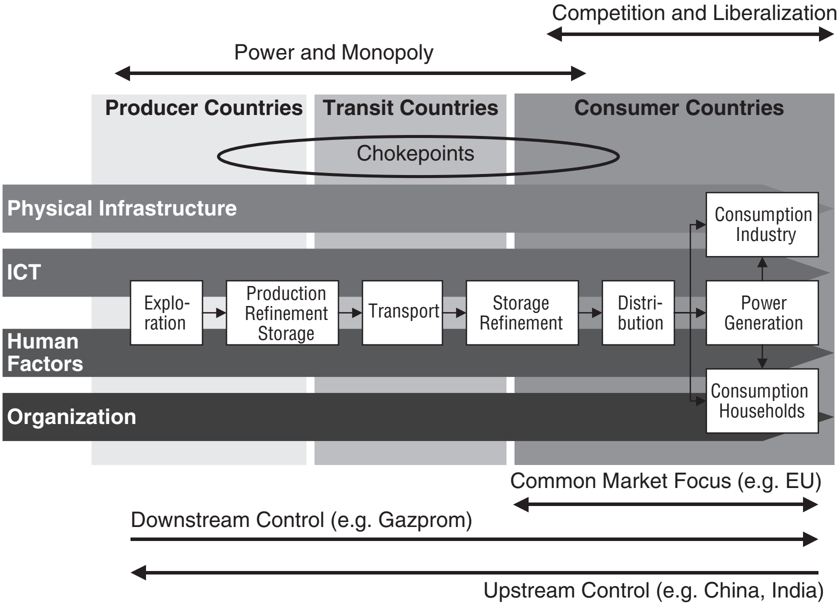
- *Energy Supply Chain*
  The energy supply chain at the center of Figure 1 illustrates the relevant steps to bring energy recourses to consumer markets. Most importantly, the supply chain highlights the interconnectedness of all stakeholders involved: individual firms or nations depend not only on their own choices to guarantee infrastructure security, but also on those of others.[13]

[11] *European Energy and Transport. Trends to 2030—update 2005* (Luxembourg: Office for Official Publications of the European Communities, 2006), pp. 26-27.

[12] Belkin, Paul and Vince L. Morelli, *The European Union's Energy Security Challenges,* CRS Report RL33636 (Washington, DC: Congressional Research Service, 2007), p. 29.

[13] Heal, Jeffrey et. al., "Interdependent Security in Interconnected Networks," in Auerswald, Philip E. et. al., eds., *Seeds of Disaster, Roots of Response. How Private Action Can Reduce Public Vulnerability* (Cambridge: Cambridge University Press, 2006), pp. 258-275, here p. 258.

Figure 1 Energy Infrastructure Security—Model of Analysis



- *Production, Transit, and Consumption Countries*
  Energy infrastructures cross various countries and are thus subject to regulatory differences. Today, important production and transit countries lack energy infrastructure security concepts or strategies. If safety and security standards exist at all, they are not delineated from an overall concept. Given the logic of the supply chain, this directly weakens the security of supply of consuming countries.

  Furthermore there is the crucial role of chokepoints, i.e. narrow geographic bottlenecks through which energy supplies are channeled. For example, 88 percent of all Persian Gulf oil exports need to pass the Strait of Hormuz.[14] If the Strait is blocked, there are alternative routes, but delivery takes longer which increases supply costs.

[14] Jean-Paul Rodrigue, "Straits, Passages and Chokepoints. Maritime Geostrategy of Petroleum Distribution," *Cahier de Géopgraphie du Québec*, 48:135 (December 2004), pp. 357-374, here p. 367.

- *Risks*
  Physical infrastructure risks describe vulnerabilities of assets such as pipelines or pumping stations. Protecting and hardening these elements can improve physical security. Information and communication technology (ICT) refers to the dependence of energy infrastructure on networks and control systems. This makes energy infrastructure security even more complex as risks that can endanger the proper functioning of ICT can also affect energy infrastructures.

  Human factors illustrate that human activity can pose security risks either by deliberate attacks (e.g. in case of terrorists) or occasional malfunctions. Finally, organizational aspects need to be taken into account in order to address interfaces between the various actors along the energy supply chain.

Analyzing energy infrastructure security on the basis of our model yields five distinct problems, which illustrate the complexity of this important homeland security task:

- *Power Asymmetry in the Supply Chain*
  It is estimated that around 85-90 percent of the world's oil reserves fall under direct government control. Governments receive at least 45-90 percent of the net value of crude oil over the lifetime of around 40 years of an oil field. State players also account for about 78 percent of world oil and 74 percent of world gas production, leaving the rest to corporate actors such as Exxon Mobil, Royal Dutch Shell, BP or Total.[15]

  This means that the EU's competition-based regulatory approach is seriously limited. In fact, competition only works on the European home market, and even there serious problems exist. As all other stages of the supply chain are dominated by power and monopolies, there are serious power asymmetries: Europe's market focus collides with the desire for upstream control of leading energy resource consumers such as China

[15] GAO, *International Energy: International Forums Contribute to Energy Cooperation with Constraints* (Washington, DC: GAO, 2006), p. 20; Harel, Xavier, "La pétro-politique rebat les cartes," *La Tribune*, June 12, 2006, p. 36; Shankelman, Jill, *Oil, Profits, and Peace. Does Business Have a Role in Peacemaking?* (Washington, DC: United States Institute of Peace Press, 2006), p. 40.

and India and the striving for downstream control followed by leading producers such as Gazprom.

- *Insufficient Network Management*
  The European desire for "green energies" from renewable sources collides with existing network capacities. Wind power, for example, is hard to control. Overcapacity of power from wind parks can thus lead to critical power grid situations in particular in neighboring regions used to diverge surge capacities. So far investments and planning procedures are insufficient to tackle this problem, which means that inadequate network design can pose serious risks to energy infrastructures.

- *Manifold Vulnerabilities*
  More attention needs to be paid to the security repercussions of deregulation. Stimulating competition can lead to cuts in reserve building, reduction of storage capacity and lower spending on training and maintenance.[16] Furthermore, interdependencies between energy infrastructures and other critical infrastructures need much more attention. Electronic control systems, for instance, have been called an "inroad to critical infrastructure disaster" as information security for these elements lags behind general information security.[17]

- *Underinvestment*
  The European Commission estimates that Europe needs to invest up to €1.8 trillion in its energy infrastructure until 2030 in order to meet the requirements of the common European market for gas and electricity. Around €310 billion are forecasted for investments in oil and gas infrastructure. Of the roughly €1.4 trillion needed for Europe's electricity infrastructure around €900 billion alone are required for power generation.[18]

[16] Thomas, Stephen and David Hall, *Restructuring and Outsourcing of Electricity Distribution in EU* (London: Public Services International Research Unit, 2003), p. 28; Buchan, David, "The Threat Within: Deregulation and Energy Security," *Survival*, 44:3 (Autumn 2002), pp. 105-116, here p. 113.

[17] E Luiijf, Eric A. M., "SCADA: An Inroad to Critical Infrastructure Disaster," Presentation to the 4th EAPC/PfP Workshop on Critical Infrastructure Protection and Civil Emergency Planning, Zurich, August 24-26, 2006.

[18] EU Energy Policy Data, SEC(2007) 12, Brussels, January 10, 2007, p. 17.

The sums currently available are nowhere near these benchmarks. The European Investment Bank, for example, provides around €0.5-1 billion annually until 2013 for trans-European energy network projects.[19] Whereas electricity transmission operators earned €334 million in 2005 from maintaining cross-border interconnectors, they have only reinvested €25 million between 2002 and 2005.[20]

- *Regulatory Deficits*
  Regulatory deficits result from the lack of a common regulatory area for energy infrastructure security and from power asymmetries. Europe, it is said, is a world-leading gas consumer and could thus influence producers. But as long as European countries prefer bilateral agreements with key suppliers it will not be possible to leverage European buying power. Furthermore, the quest for downstream control by leading producers poses the risk of interference of foreign actors into national and European critical energy infrastructures. So far there seems to be a regulatory hole for dealing with foreign companies investing in Europe's critical infrastructures. The problem needs to be solved on a national basis which opens the door for diverging approaches.

Current European Energy Regulation

Energy infrastructure-related aspects were addressed before the above mentioned directive was proposed. Based on the key directives launched in the second half of the 1990s to establish common rules for the internal market in electricity and natural gas two directives in particular addressed measures to safeguard security of natural gas supply as well as electricity supply and infrastructure investments.[21]

[19] EIB, *EIB Financing of the Trans-European Networks* (Luxembourg: EIB, 2006), p. 6.

[20] Kopp, Gudrun, "Grenzüberschreitende Stromnetze ausbauen," FDP im Deutschen Bundestag, Presseinformation Nr. 12, 5 January 2007.

[21] Directive 2004/67/EC of the European Parliament and of the Council of 26 April 2004 concerning measures to safeguard security of natural gas supply, OJ L 127, April 29, 2004, pp. 92-96; Directive 2005/89/EC of the European Parliament and of the Council of January 18, 2006 concerning measures to safeguard security of electricity supply and infrastructure investment, OJ L 33, February 4, 2006, pp. 22-27.

In addition European energy associations also engage in defining safety and security regulations. For example, the Union for the Coordination of Transmission of Electricity (UCTE) has set up regulations for electricity transmission to be followed by the respective national associations, and Marcogaz has developed guidelines and performance indicators for pipeline integrity management systems (PIMS).[22]

Overall, however, Europe's quest for energy security is not driven by security issues. In principle Europe's energy policy rests on competitiveness, environmental issues and security of supply.[23] In practice, the European Commission's emphasis on market liberalization is strongest. As of July 1, 2007 Europe's gas and electricity markets should be fully opened for competition, but EU member states are far from achieving this goal.[24]

Examples of Critical European Energy Infrastructures

Transportation and energy are the first sectors for which the Commission proposed criteria to identify critical infrastructures. The document is confidential[25] and not available publicly. However, possible candidates for this list can be identified by approximation and could include:

- Projects of high-priority identified under the Priority Interconnection Plan to realize the common European market for gas and electricity (e.g. Nabucco pipeline);
- Interconnectors which link foreign energy supply infrastructures with the European network, for example in Belgium, the Netherlands, Poland or Slovakia;
- Intra-European interconnectors which link supply lines with intra-European transmission pipelines, for example between Slovakia and Austria or Slovakia and the Czech Republic;

[22] For more information, see: http://www.ucte.org, http://marcogaz.org.

[23] A European Strategy for Sustainable, Competitive and Secure Energy. Green Paper, COM (2006) 105, Brussels, March 8, 2006, pp. 5-17.

[24] Prospects for the internal gas and electricity market, COM(2006) 841, Brussels, January 10, 2007.

[25] http://ec.europa.eu/dgs/energy_transport/security/infrastructure/index_en.htm.

- Oil refineries producing oil-based products which are key for European industry sectors and are not easily offset by other refineries;
- Liquefied natural gas (LNG) receiving terminal capacity which will be mainly concentrated in Spain and Italy. A growing portion of the new LNG terminal capacity under construction will be held by non-EU producers;[26]
- Shipping capacity to deliver LNG to Europe (already today 25 percent of the total existing shipping capacity that serves European markets with LNG is held by Bonny Gas Transport, a 100 percent subsidiary of Nigeria LNG Ltd).[27]

Possible Next Steps

There is a need for institutional reform to address energy infrastructure security at the global and at the European level. The International Energy Forum could provide a global umbrella to start discussing the issue, and the EU could appoint a special Coordinator as a focal point for activities in different policy areas. With regard to the regulatory framework there is a need to take stock of existing safety and security standards and to advance them commensurate with ongoing threat assessments and the needs of Europe's common energy market. Safety and security standards should also receive more attention when thinking about stimuli for energy infrastructure investments. Finally, energy policy and security and defense policy need to be brought together. The EU should address the potential role of hard power in energy infrastructure security and should step up its efforts to strengthen cross-border crises and consequence management for infrastructure-related incidents.

Create an Appropriate Institutional Setting

Although discussions on energy infrastructure security take place in different formats, there is no overall umbrella to bring the different work strands together. This void could be filled by the International

[26] Energy Sector Inquiry, p. 269-270.

[27] Ibid, p. 268.

Energy Forum (IEF) which involves 60 states and almost every relevant international organization.[28]

Given the sensitivity of the subject matter confidence- and security-building by exchanging information is key. This could be the starting point for the IEF, inter alia, by looking at different definitions of and approaches to energy infrastructure security, debating responsibilities and competencies of state and private actors, comparing existing safety and security standards, conducting joint risk assessments and discussing possible joint approaches to identify and protect critical energy infrastructures with cross-border impact.

To complement this global approach the EU should appoint a European Energy Infrastructure Security Coordinator.[29] The new Coordinator would have to raise awareness, create a trustworthy environment for information exchange, stimulate dialogue among public and private actors, serve as a point of contact, identify best practices, coordinate safety and security activities in the energy sector, and make sure that the issue receives the necessary attention as a cross-sector item in Europe's different policy areas.

As a first priority the new Coordinator should focus on European critical energy infrastructures identified in the EPCIP framework. In doing so, the Coordinator could establish an Energy Infrastructure Security Platform involving all relevant public and private stakeholders in Europe. The work of the Platform should be coordinated with other international institutions and should mirror IEF activities.

Take Stock of Existing Safety and Security Standards

The lack of common energy infrastructure safety and security standards along the energy supply chain is a problem for cross-border energy flows. As a first step to solve this problem, an overview of existing national and international safety and security standards should be compiled in order to identify needs for action.

[28] For more on this, see: Borchert, Heiko and Karina Forster, "Energy Infrastructure Security: High Time for a Networked Public-Private Governance Approach," *Middle East Economic Survey,* 50:21 (May 21, 2007), pp. 32-36.

[29] This builds on the idea of European coordinators for key European infrastructure projects. See: Priority Interconnection Plan, COM(2006) 846, Brussels, January 10, 2007, p. 10.

In this context safety and security standards for priority infrastructure projects that connect Europe with key supply regions or provide major intra-European interconnections should be scrutinized. Performance requirements will need to be discussed with the respective production and transit countries and companies involved. If these requirements cannot be met, European financial or technical assistance may be required.

In addition, mutual interdependencies between the energy sector and other critical infrastructure sectors such as ICT and transportation need to be addressed. Following the assessment of these critical interdependencies it will be important to identify what should be done at the international, regional, and national, and sub-national levels and how responsibilities and tasks should be shared between public and private actors.

Finally, there is a need to deal with ICT safety and security standards, in particular for Supervisory Control and Data Acquisition systems (SCADA) used in the energy sector. Given the lack of awareness of SCADA problems, there is a need to identify and document best practices and to standardize safety and security norms. This could be done, for example, by conferences and publications launched by the European Energy Infrastructure Security Coordinator.

Pay More Attention to Safety and Security in Europe's Regulatory Framework for Infrastructure Investments

A regulatory framework for energy infrastructure investments that takes into account safety and security spending requires market-based incentives for increased spending in combination with monitoring and regulatory oversight.

Market-based stimuli could include tax incentives for safety and security investments, preferential deduction of safety and security investments during the life-cycle of an infrastructure project, or tax incentives for research and development into infrastructure safety and security technologies. The level of these incentives should be commensurate with energy infrastructure risk assessments. This helps avoid that incentives are tilted away from safety and security towards other purposes when threats vanish.

Safety and security spending needs to be monitored. This could be done by the European Commission (for European critical energy infrastructure projects) or by national energy market regulators. Possible investment categories that should be tracked could include new investments, spending on operation and maintenance, recruitment, training, safety and security in general, ICT safety and security in particular, and life extension upgrades.

As safety and security matters along the supply chain, the EU should consider how these ideas could be addressed as part of Europe's external energy dialogue with production and transit countries. For example programs such as the EU-Africa Partnership on Infrastructure Initiative and overseas development aid could be targeted more directly at energy infrastructure safety and security.

Address the Role of Hard Power in Energy Infrastructure Security

So far, hard power plays no role in Europe's energy policy. NATO, by contrast, has engaged in dialogue with oil and gas producing companies and countries about how the alliance could help provide energy infrastructure security and has identified critical infrastructure protection as a future task for NATO forces.[30]

Military capabilities relevant for homeland security can also advance energy infrastructure security. This is true for intelligence gathering and assessment or surveillance for example with unmanned aerial vehicles, networked sensor applications or radar systems. In addition, armed forces could help provide physical protection of infrastructures and support the stabilization of areas in which infrastructures are situated. Passive and active electronic warfighting capabilities could be used to assure ICT security. Finally, armed forces could provide emergency assistance in case an infrastructure-related incident involves the use of weapons of mass destruction.

First of all, the EU should bring in line its ambitious external energy policy agenda with the European Security and Defense Policy

[30] Bergin, Tom, "NATO Eyes Naval Patrols to Security Oil Facilities," *The Scotsman*, May 14, 2007. Available at: http://news.scotsman.com/latest.cfm?id=748442007; Comprehensive Political Guidance, endorsed by NATO Heads of State and Government on November 29, 2006, Para. 16(c). Available at: http://www.nato.int/docu/basictxt/b061129e.htm.

(ESDP). The Long-Term Vision which outlines future capability requirements for EU armed forces only makes very general references to energy security.[31] However, as long as there are no explicit energy infrastructure related requirements, possible tasks for the armed forces will not enter national capability planning. The EU should thus address potential ESDP contributions to energy infrastructure security and adapt existing scenarios for the European Headline Goal 2010.

The EU and NATO could advance energy infrastructure security through joint science and technology projects involving key energy production and transit countries. Joint projects would be most suitable in the fields of ICT security, situational awareness, command and control, human factors, detection and protection technologies, material science, and modeling and simulation.

Regional military cooperation with key partners in the Greater Middle East, the Caucasus and in Central Asia should be envisaged as well. Both organizations have outreach programs that help advance dialogue with these regions. Together they could launch regional military training programs designed to bolster local security and military capabilities for energy infrastructure security tasks. Given the strategic interests of Russia and China in energy security, thought should be given as to how these countries could be involved as well.

Strengthen Cross-Border Crises and Consequence Management

Cross-border cooperation to protect critical infrastructures in Europe suffers from the lack of mutual understanding of each other's crisis management systems and responsibilities, information about existing capabilities, training on joint operations, and mutual understanding between private and public crisis management centers.[32]

Emergency management depends on situational awareness and situational understanding. To this purpose a common energy sector operation picture (COP) could provide an information umbrella for

[31] European Defense Agency, An Initial Long-Term Vision for European Defense Capability and Capacity Needs, October 3, 2006, Para. 11.

[32] Luiijf, Eric A. M., "The VITA Project: Results and Recommendations," Paper prepared for the 4th EAPC/PfP Workshop on Critical Infrastructure Protection and Civil Emergency Planning, Zurich, August 24-26, 2006, pp. 5-7.

private energy companies and network operators as well as police forces, other emergency responders, armed forces and intelligence services. It would make sense to start building such a COP in those European countries where cross-border exchanges of energy flows are highest and which are thus key for the common European energy market.

Furthermore there is a need for bi- and multilateral pre-arrangements for cross-border emergency support that allows for the mutual exchange of aid among public and private actors of different countries. This interaction needs to be trained in advance. To this purpose the European Commission, for example in cooperation with the Euro-Atlantic Disaster Response Coordination Cell (EADRCC), could establish a joint exercises agenda. In all of these activities key external energy partners of the EU should be included.

Chapter 11

The Use of Economic Sanctions to Maintain International Peace and Security and Combat International Terrorism[1]

Chantal de Jonge Oudraat

United Nations Secretary-General Kofi Annan has called economic sanctions a "vital tool" in dealing with threats to international peace and security — "a necessary middle ground between war and words."[2] Sanctions are also favored by most UN member states.

Since the end of the Cold War, the UN Security Council has imposed economic sanctions more than two dozen times to deal with violent conflicts and terrorism (see Table 1 on page 193). The use of sanctions has undergone dramatic changes over the course of this period. Two phases can be distinguished.

The first phase dates from the end of the Cold War to the mid-late 1990s. The sanctions regimes of this period were directed primarily at intra-state and inter-state conflicts. These sanction efforts had ambitious goals: their strategic objective was compellence—the reversal of policies that provoked or sustained violent conflict. In addition, they were comprehensive in scope and encompassed the totality of the target's economy. The effectiveness of these sanctions regimes was poor. They led to tremendous economic costs to the target countries, but often not to changes in the political behavior of the leaders of those countries. The economic impacts on the countries in question also had damaging social and humanitarian effects, leading many

[1] This chapter is derived from Oudraat, Chantal de Jonge, "Economic Sanctions and International Peace and Security," in Aall, Pamela, Chester Crocker, and Fen Osler Hampson, eds., *Leashing the Dogs of War: Conflict Management in a Divided World* (Washington, DC: USIP, 2007), pp. 335-355.

[2] See Kofi Annan, *In Larger Freedom: Towards Development, Security and Human Rights for All* (New York: United Nations, 2005), para 109.

commentators to question the morality of economic sanctions as policy instruments.[3] These sanctions often hurt innocent neighboring countries as well.

The second phase started in the mid-1990s. Policymakers recognized that the adverse humanitarian effects of comprehensive sanctions regimes undermined political support for these actions. They also acknowledged the poor track record of sanctions. In the search for more effective policy instruments, they increasingly turned to targeted sanctions—measures that target specific people, resources, or services and that would reduce harmful humanitarian effects.[4] The shift to targeted sanctions was accompanied by more modest and achievable goals. Starting in the mid-1990s the strategic objective of most sanctions regimes shifted from compellence to denial—withholding the means that could lead to threatening policies or behavior—and to deterrence—discouraging the adoption of threatening policies or behavior. In addition, sanctions were increasingly used to fight terrorism. This fight became a top priority for the UN after the September 11, 2001 terrorist attacks in the United States.

The mid-late 1990s saw a fundamental shift in the use of sanctions along three dimensions: strategic objectives, instruments, and focus. The change in the strategic objectives of sanctions to deterrence and denial, combined with the shift to targeted sanctions and an increased focus on terrorism improved the sanctions record in this second phase from poor to fair.

[3] See, for example, Gordon, Joy, "A Peaceful, Silent, Deadly Remedy: The Ethics of Economic Sanctions," *Ethics and International Affair*s, Vol. 13 (1999), pp. 123-150; Mueller, John and Karl Mueller, "Sanctions of Mass Destruction," *Foreign Affairs*, Vol. 78, No. 3, (May-June 1999), pp. 43-53; Thomas G. Weiss, David Cortright, George Lopez and Larry Minear, *Political Gain and Civilian Pain: Humanitarian Impacts of Economic Sanctions*, (Lanham: Rowman and Littlefield, 1997). On how sanctions criminalize societies, see also Andreas, Peter, "Criminalizing Consequences of Sanctions: Embargo Busting and its Legacy," *International Studies Quarterly*, Vol. 49, No. 2, (June 2005), pp. 335-360.

[4] Targeted sanctions are sometimes also called smart sanctions. They usually consist of travel bans, asset freezes, and embargoes or regulations on strategic goods such as diamonds and timber. Targeted sanctions are not panaceas and they can also hit innocent people hard. To reduce this collateral damage, the UN Security Council started to request the UN Secretariat to draw up humanitarian assessment reports either before or shortly after the imposition of sanctions. A first report of this nature was prepared in 1997 and concerned the proposed sanction regime on Sudan. It led to the decision by the Security Council not to impose an aviation ban.

First, the new strategic objectives helped improve the record. For starters, compellence is inherently difficult.[5] Deterrence is easier for several reasons. First, deterrence does not require immediate action from those who are deterring. In addition, deterrence requires no public action by the one being deterred. Finally, deterrence aims to maintain the status quo, which is generally easier than challenging the status quo.[6] Denial is also easier than compellence. When the goal is denial, actors seek to isolate the offending party and limit its ability to threaten international peace and security. The key to successful denial action is third-party compliance, especially from neighboring states—international assistance can bolster third-party compliance.

Second, the shift to targeted sanctions also helped to improve the track record of sanctions efforts. Targeted sanctions, by virtue of their limited nature, are easier to implement than comprehensive sanctions. In addition, political support for targeted sanctions is easier to mobilize since these sanctions target only those directly responsible for dangerous behavior.

Third, the improved track record of sanctions was brought about because sanctions efforts were redirected from the problems of violent conflicts to terrorism. Violent conflicts are inherently difficult policy problems. Those who are involved in these conflicts are highly motivated and difficult to influence. International actors usually have weaker motivations. Coordinated international actions are difficult to organize and sustain. Mobilizing international support for counter-terrorist actions is much easier. All of the permanent members of the UN Security Council have an interest in this issue, and all have been the object of terrorist attacks. The Security Council has recognized terrorism as an unlawful activity and a threat to international peace and security. It is consequently easier for the United Nations to organize sanctions efforts with respect to the threat of international terrorism.

[5] See Schelling, Thomas C., *Arms and Influence* (New Haven, Conn: Yale University Press, 1966); George, Alexander L., *Forceful Persuasion: Coercive Diplomacy as an Alternative to War* (Washington, DC: USIP Press, 1991); and Art, Robert J. and Patrick M. Cronin, *The United States and Coercive Diplomacy* (Washington, DC: USIP Press, 2003).

[6] Given these strategic dynamics, it is not surprising that the threat to impose sanctions has had a relatively good track record.

The scholarly literature on sanctions is abundant.[7] However, most scholars have failed to recognize the fundamental changes that took place in sanctions efforts the mid-1990s. They have failed to recognize how the shift in strategic goals (from compellence to deterrence and denial), the shift in sanctions instruments (from comprehensive to targeted sanctions), and the shift in focus (from violent conflicts to terrorism) changed the sanctions equation.[8] Most assessments of post-Cold War sanctions are based on the track record of the early 1990s and are consequently negative. Scholars have not given adequate consideration to developments that have taken place since the mid-1990s. This has led to misguided policy recommendations about the use of economic sanctions.

In this chapter I do four things. First, I review the mechanics of UN sanctions. Second, I examine UN sanction regimes in the early 1990s —the first phase of post-Cold War sanctions. I focus on the sanction regimes imposed on Iraq, the Former Republic of Yugoslavia (FRY) and Haiti. Third, I examine UN sanction regimes imposed since the mid-late 1990s, focusing on sanctions efforts to combat terrorism. Fourth, I define the parameters of a successful sanction strategy.

[7] For a very critical view see, for example: Pape, Robert, "Why Economic Sanctions Do Not Work," *International Security*, Vol. 22, No. 2, (Fall 1997), pp. 90-136; and Pape, "Why Economic Sanctions Still Do Not Work," *International Security*, Vol. 23, No. 1, (Summer 1998), pp. 5-65. For a more nuanced view see Elliot, Kimberly Ann, "The Sanctions Glass: Half Full or Completely Empty," *International Security*, Vol. 23, No. 1, (Summer 1998), pp. 66-77. See also Hufbauer, Gary Clyde, and Jeffrey J. Schott, and Kimberly Ann Elliot, *Economic Sanctions Reconsidered* (Washington, DC: Institute for International Economics, rev. ed., 2 vols. 1990); and Baldwin, David, "The Sanctions Debate and the Logic of Choice," *International Security*, Vol. 24, No. 3, (Winter 1999/2000), pp. 80-107.

[8] Notable exceptions in this regard are David Cortright and George Lopez. See David Cortright, and George A. Lopez, *Sanctions and the Search for Security: Challenges for UN Action* (Boulder: Lynne Rienner Publishers, 2002); and David Cortright, George A. Lopez, et al., *The Sanctions Decade: Assessing UN Strategies in the 1990s* (Boulder: Lynne Rienner Publishers, 2000). Targeted sanctions have been the object of three main policy seminars. See the proceedings of the Interlaken seminars organized by the Swiss Government, available at: www.smartsanctions.ch/start.html; the proceedings of the first expert seminar on smart sanctions organized by the Bonn International Center for Conversion and the Foreign Office of the Federal Republic of Germany, Bonn, November 21-23, 1999, available at: www.bicc.de./general/events/unsanc/papers.html; and the proceedings of the Stockholm process in: Wallensteen, Peter and Carina Staibano and Mikael Eriksson, *Making Targeted Sanctions Effective: Guidelines for the Implementation of UN Policy Options* (Stockholm: Uppsala University, 2003), also available at: www.smartsanctions.se.

The Mechanics of UN Sanctions

Economic sanctions are non-military measures that restrict or stop normal international economic exchanges with a state or a non-governmental group, for the purpose of compelling, denying or deterring political or military behavior by the targeted government or group.[9] Economic sanctions are different from trade wars, in which governments restrict or stop international economic exchanges in order to gain more favorable terms of trade.

Underlying the theory of sanctions is the expectation that economic costs will translate into political effects—that economic deprivation will produce public anger and politically significant protest. It is expected that this, in turn, will lead to changes in the behavior of trouble-making elites, or their removal from power.

UN sanctions are coercive measures intended to restore or maintain international peace and security. They are elements of a bargaining strategy that includes measures ranging from the severance of diplomatic ties to interruption of economic relations to the threat and use of military force.[10]

Chapter VII of the UN Charter provides the legal authority for the imposition of UN economic sanctions. It outlines the actions the UN Security Council can take to deal with threats to international peace

[9] Embargoes and export controls limit and ban exports. Boycotts limit and ban imports. Arms embargoes are not to be confused with export controls. Arms embargoes generally have a triggering event—such as, the outbreak of violent conflict. An arms embargo also tends to be of temporary nature—it will be lifted once the armed conflict has stopped. Arms embargoes may have unintended effects. In internal conflicts, they tend to favor the warring factions that have access to governmental stockpiles and industries. In such cases, arms embargoes can undermine the abilities of others to organize and defend themselves. Arms embargoes can thus favor one side over the other and may permit one side to win, rather than pushing both sides toward a military stalemate and political settlement. See Spear, Joanna, "Arms Limitations, Confidence Building Measures, and Internal Conflict," in Brown, Michael E., ed., *The International Dimensions of Internal Conflict* (Cambridge, MA.: MIT Press, 1996), pp. 377-410.

[10] See UN Charter, Chapter VII, articles 39, 40, 41, and 42. UN sanctions are not intended to punish targets. Sanctions imposed by the Security Council are political, not legal, instruments. They are discretionary measures decided upon by the Council outside of any legal or disciplinary context. As such they are unlike sanctions to enforce international or national law. See Sur, Serge, *Security Council resolution 687 of 3 April 1991 in the Gulf Affair: Problems of Restoring and Safeguarding Peace*, (New York: United Nations/UNIDIR Research Papers, No. 12, 1992), pp. 15-16. See also Gowlland-Debbas, Vera, *Collective Responses to Illegal Acts in International Law: United Nations Action in the Question of Southern Rhodesia* (Dordrecht: Martinus Nijhoff, 1990), pp. 461-485.

and security. The Charter gives the Council tremendous latitude in defining threats to international peace and security, and the Council has shown great creativity in the post-Cold War era in defining these threats. Indeed, it has increasingly identified internal conflicts, gross violations of human rights, and terrorism as justifications for international action and the imposition of sanctions.

A decision to impose mandatory sanctions needs affirmative votes of nine members of the UN Security Council, including the votes of China, France, Russia, the United Kingdom and the United States—the five permanent members of the Council. Once the Council has decided to impose economic sanctions under Chapter VII of the Charter, all UN member states are required to implement them.[11] The Security Council usually establishes a Sanctions Committee to facilitate implementation of a new sanctions regime.[12] In recognition of the importance of implementation, the Council may also establish panels of experts to monitor implementation of the regimes. It has done so increasingly since the end of the 1990s.

Phase I: Sanctions and Violent Conflicts in the Early-Mid 1990s

Sanctions regimes tended to be ambitious and broad in scope in the early 1990s. Three sanctions regimes defined this phase: the comprehensive sanctions imposed on Iraq in 1990, because of its invasion and illegal occupation of Kuwait and, subsequently, to ensure compliance with the ceasefire resolution and disarmament provisions; the FRY in 1992, in response to the FRY's involvement in the war in Bosnia-Herzegovina (and in 1994 on the Bosnian Serbs); and on the military junta in Haiti in 1994, because of its reversal of the 1991 elections.[13]

[11] Indeed, when states join the United Nations they accept to carry out the decisions of the Security Council. See UN Charter Articles 41, 25 and 27.

[12] It may be recalled that the interpretative guidance of the Sanctions Committees is not binding on UN members.

[13] In addition to these comprehensive regimes, the Security Council also imposed in this first phase stand-alone arms embargos on: Somalia, Liberia, and Rwanda. An arms embargo and targeted sanctions were imposed on UNITA. All these sanction regimes were poorly implemented. It is only in the late 1990s that the Council started paying serious attention to these regimes. For details, see Oudraat, Chantal de Jonge, "UN Sanction Regimes and Violent Conflict," in Crocker, Chester, and Fen Osler Hampson and Pamela Aall, eds., *Turbulent Peace: The Challenges of Managing International Conflict* (Washington, DC: USIP, 2001), pp. 323-351.

In all three cases, sanctions quickly led to deterioration in the economic and social conditions in the countries concerned. However, they did not lead to changes in the behavior of the political leaderships. On the contrary, these leaders generally became more repressive. Iraqi President Saddam Hussein managed to convince large segments of the Iraqi population that the UN and outside powers were responsible for the humanitarian consequences of the sanctions regime.[14] Profound differences among UN Security Council members developed by the late 1990s. Some believed that sanctions should be lifted because of their dire humanitarian consequences. Others argued that sanctions could contain Iraq, prevent it from becoming a threat to the region, and keep it from developing new weapons programs. Sanctions, they believed, had an important denial function. A third group, comprised of the U.S. and the UK, had hoped that sanctions would lead to the overthrow of Saddam Hussein. Once it became clear that sanctions reinforced rather than weakened the Hussein regime, this group concluded that sanctions had run their course and that forceful removal of the regime was the only viable option. The debate in the UN Security Council over this issue resulted in a rift among UN Security Council members. In March 2003, the U.S. and the UK brought the debate to an end when they invaded Iraq without UN Security Council imprimatur.

Comprehensive sanctions were also imposed on the FRY in 1992 in response to the FRY's involvement in the war in Bosnia-Herzegovina. These sanctions were extended in 1994 to the Bosnian Serbs. However, a lack of clear strategic objectives and disagreements among the Western allies undercut the sanctions effort. Ultimately, it was direct military action in 1995 that ended the war in Bosnia.

[14] UN Security Council members had tried to mitigate the humanitarian consequences of the sanction regime by adopting the Oil-for-Food program. Under the terms of this program, adopted in 1991, revenues from the sale of Iraqi oil could be used to pay for food and medicine. However, it was not until 1996 that Baghdad accepted the conditions of the program and even then it would frequently order insufficient food and medicines, hoard them in warehouses, illegally re-export humanitarian supplies, or simply stop oil exports. The apparent strategy was to increase the misery of the Iraqi people, thereby putting pressure on the Security Council to lift sanctions altogether. In 2000, UN Secretary General Kofi Annan warned the members of the Council that they were losing the propaganda war about who was responsible for the situation in Iraq—Iraqi President Saddam Hussein or the United Nations. Annan also acknowledged that the program established to mitigate the humanitarian effects—the Oil-for-Food program—had not met its objectives. See UN Press Release SC/6833, March 24, 2000 and UN SC document S/2000/208, March 10, 2000.

The UN Security Council imposed comprehensive sanctions on Haiti after the military ousted the democratically elected President of Haiti, Jean Bertrand Aristide. Here, too, divisions among UN Security Council members undercut the effectiveness of the coercive strategy to restore Aristide to power. The junta, bolstered by a weak and disjointed adversary, believed it could weather the storm even when the Security Council imposed a total trade ban on Haiti in May 1994. By this time, the Council had lost much of its credibility. Only the threat of military force, delivered in person by Chairman of the U.S. Joint Chiefs of Staff Colin Powell, U.S. Senator Sam Nunn, and former U.S. President Jimmy Carter and backed up by U.S. forces on high alert, persuaded the junta to budge.

The poor sanctions record of the early 1990s generated four policy lessons.

First, broad international support for sanctions is a key to their success. Unfortunately, this support was often lacking during this period, either because of disagreement over the objectives to be achieved or because there was no country that would take the lead and provide a sharp focus to UN Security Council action.

Second, many sanctions regimes were hindered because they were stand-alone measures that were not integrated into comprehensive coercive strategies that included the threat or use of force. This is one of the main reasons why sanctions were ineffective as instruments of compellence during this period.

Third, the comprehensive sanction regimes of the early 1990s produced great social and human costs that were politically difficult to sustain over a long period of time. This fuelled the search for targeted sanctions. Starting in the mid-1990s, several international workshops were organized to assess and refine the notion and scope of targeted sanctions.[15] The use of targeted sanctions shifted the focus of sanctions from compellence to deterrence and denial—from ambitious to more limited goals. The new objective was to deny ruling and warring elites access to resources, and thereby reduce their ability to wage war.

[15] See footnote 8.

Fourth, for targeted sanctions to work, third-party compliance and implementation are key. This lesson spurred the creation of monitoring groups and investigative expert panels.[16] These groups developed important insights into sanction-busting behavior. This led the Security Council to pay greater attention to the behavior of third parties and neighboring countries, and to focus on the deterrence and denial functions of sanctions. Naming and shaming and the imposition of secondary sanctions were part of this effort.

Phase II—Sanctions and the Campaign Against Terrorism Since the Mid-1990s

The sanctions imposed against Libya in 1992, accused of involvement in the terrorist attacks in 1988 and 1989 on an American (Pan Am) and French (UTA) airliner, spearheaded the UN Security Council concern with terrorism.[17] The Council went on to impose mandatory Chapter VII sanctions to fight terrorism on two other occasions in the 1990s—in 1996 against Sudan and in 1999 against the Taliban regime in Afghanistan.

By imposing sanctions in the 1990s—on Libya, Sudan, and the Taliban in Afghanistan—the Security Council had two main counter-terrorism objectives: to compel—to change the behavior of state-sponsors of terrorism and make sure that individuals believed to be responsible for specific terrorist attacks were extradited; and to deter—to discourage states from providing support to terrorist groups.[18]

In the case of Libya, UN sanctions were fairly effective. Even before sanctions took effect, Libya offered to surrender the suspects of the UTA bombing to a French court and those responsible for the Pan Am explosion to an international court. However, the broader

[16] See Vines, Alex, "Monitoring UN Sanctions in Africa: The Role of Panels of Experts," in *Verification Yearbook 2003* (London: Vertic, 2003), pp. 247-263. The March 2000 Security Council report on sanctions violations of the Angola/UNITA sanctions regime was a first in this regard. See S/2000/203.

[17] For details see Oudraat, Chantal de Jonge, "The Role of the UN Security Council," in: Boulden, Jane and Thomas G. Weiss, eds., *Terrorism and the UN: Before and After September 11* (Bloomington, IN: Indiana University Press, 2004), pp. 151-172.

[18] Washington recognized "this type of concerted multilateral response to terrorism… as an important deterrent to states considering support for terrorist acts or groups." See A/48/267/Add.1, September 21, 1993, para 6.

security objective—weakening Libya's support for terrorist groups—required the continuation of sanctions. By the late 1990s, this broader objective was largely achieved. In 1996, the U.S. State Department noted that Libya's support for terrorism had been sharply reduced.[19] Maintaining UN sanctions consequently became difficult to justify. In addition, international support of the sanctions regime was crumbling. These developments led the United States and the UK to develop a proposal whereby the two Libyan suspects would be tried under Scottish law in a court in the Netherlands. The Libyan government accepted the plan early 1999, and sanctions were suspended on April 8, 1999—three days after the two Libyan suspects had arrived in the Netherlands.

In the case of Sudan, travel sanctions were imposed on Sudanese government officials in April 1996, after Khartoum refused to extradite three suspects in the assassination attempt of Egyptian President Hosni Mubarak. Although Sudan subsequently expelled a number of Egyptians, Palestinians and "Arab Afghans"—including Osama bin Laden—sanctions were kept in place. The United States argued that Sudan continued to be used as a safe haven by terrorist groups such as al-Qaeda. The Security Council agreed and imposed an air embargo on Sudan. However, the embargo was never implemented. Council members feared the humanitarian consequences of such an embargo, particularly on a country already ravaged by civil war. Even so, the adoption of the air embargo sent a message—that support of terrorist activities was not acceptable and could provoke a reaction by the international community.[20]

Members of the Security Council—the United States, in particular—became increasingly concerned about the changing nature of the terrorist threat in the 1990s. Terrorist groups seemed to be operating more and more as part of a global network. In addition, the 1995 sarin nerve gas attack in the Tokyo subway by Aum Shinrikyo increased fears that terrorists might one day use chemical, biological or nuclear weapons.

[19] See *Patterns of Global Terrorism 1996*, U.S. Department of State.

[20] UN sanctions were lifted in September 2001 after Sudan pledged its full support for the global anti-terrorist campaign.

The September 2001 attacks showed how difficult it was to compel regimes such as the Taliban and transnational groups such as al-Qaeda.[21] UN sanctions had no noticeable effect on the Taliban mainly because of their isolated economic position.[22]

Although the UN sanction regimes of the 1990s failed to stop worldwide terrorist activities, they helped to change at least the declared attitudes of states towards terrorist groups, particularly the attitudes of state sponsors of terrorism.[23]

Sanctions Since September 11, 2001

The terrorist attacks of September 11, 2001 made terrorism a top priority for the UN Security Council. Two weeks after the attacks, the Council adopted UNSC Resolution 1373 (1002), obligating all 191 UN member states to take far-reaching domestic legislative and executive actions in order to prevent and suppress future terrorist activities.[24] To monitor implementation, the Security Council established the Counter-Terrorism Committee (CTC), whose goal was "to help the world system to upgrade its capability, to deny space, money, support, haven to terrorism…."[25] In 2004, the CTC's capacity was increased by the establishment of a small, dedicated secretariat—the Counter-Terrorism Executive Directorate (CTED).

[21] The Taliban had been struck by financial and aviation sanctions in October 1999 when they refused to hand over bin Laden, who was accused of involvement of the bombings of the U.S. embassies in East Africa. Bin Laden had been indicted by the United States, in November 1998, for his involvement in the bombings of the U.S. embassies in East Africa and had found refuge in Afghanistan, after having been expelled by Sudan.

[22] The Taliban had limited funds abroad, and the extent of Taliban-controlled air traffic was negligible. The Taliban, moreover, was not active in the above-board global economy; much of its money came from the illegal opium and heroin trade. A strengthened sanctions package adopted in December 2000 did not change these economic fundamentals. An additional sign of the Taliban's intransigence is that the prospect of a U.S.-led attack, which grew in the wake of September 11, 2001, did not change the regime's policy. The Taliban still refused to hand over bin Laden.

[23] The U.S. State Department recognized this transformation in the late 1990s and again in 2001 when it noted the continuation of a slow trend away from state sponsorship of terrorism. See *Patterns of Global Terrorism 2001*, U.S. Department of State.

[24] UNSC resolution 1373 (2001) globalized the ban against terrorism and required states to change and/or adopt domestic legislation to: Criminalize terrorist acts, including the support and financing of such acts; Deny safe haven to terrorists and prohibit any other support for terrorists, such as the provision of arms; Cooperate with other states in the implementation of these measures.

[25] See Press Briefing by the Chairman of the CTC, October 19, 2001.

Five problems have hindered the Council's effort to deny and deter terrorist activities.[26] Some of these problems were familiar in that they had been encountered in previous sanctions regimes.

First, states often have different interpretations of key terms and sanctions provisions. For example, the financing of terrorist activities and groups is frequently equated with money laundering and dealt with within that context. However, money used to finance terrorism is not necessarily generated by illegal business transactions; much of this money is legal and is acquired by legitimate means. Similarly, there is confusion about freezing, seizing, confiscating, and suspending bank accounts.

Second, many states lack the legislative and administrative capacity to implement resolution 1373 (2001). An informal analysis conducted in the fall of 2003 revealed that seventy states were willing to comply with resolution 1373 (2001), but were unable to do so.[27] Denying terrorists access to financial resources has proven to be very difficult.[28] The UN group monitoring sanctions on the Taliban and al-Qaeda noted serious shortcomings in identifying and blocking al-Qaeda assets other than bank accounts.[29] A further complication is that many terrorist attacks since 9/11 have involved relatively small amounts of money.

[26] See for example the briefing for member states on April 4, 2002 by Walter Gehr. See: www.un.org/Docs/sc/committees/1373/rc.htm.

[27] Some sixty states were very gradually moving into compliance, and among the thirty states considered to have achieved "a considerable degree of compliance" inadequacies remained—particularly with respect to the prevention of illegal financial transfers. The study identified twenty states as "inactive"—that is countries "that for a variety of reasons have chosen not to comply with resolution 1373." Cited in Cortright, David, George Lopez, Alistair Millar and Linda Gerber, *An Action Agenda for Enhancing the United Nations Program on Counter-Terrorism* (Goshen and Notre Dame, Indiana: Fourth Freedom Forum and Joan B. Kroc Institute for International Peace Studies, September 2004), pp. 7-8.

[28] For example, while $112 million was frozen in the first three months after the September 11, 2001 attacks, only $24 million were blocked in the following two years—a small fraction of the total funds believed to be available to terrorist organizations. See *UN High-level Panel report*, para 149.

[29] See Report of the UN Monitoring Group, UN Document S/2003/669, July 8, 2003, pp. 10-18; and the Report of the Analytical Support and Sanctions Monitoring Team, UN document S/2004/679, August 25, 2004. See also Alden, Edward and Mark Turner, "UN Says Lack of Cooperation is aiding al-Qaeda," *The Financial Times*, November 14, 2003, p. 1.

Travel bans were similarly hampered by implementation problems. Border controls are weak in many countries; many governments do not have the capacity to effectively police the territories under their jurisdiction. In addition, the travel bans imposed on members of al-Qaeda, the Taliban and associated groups are difficult to implement because of the widespread use of forged travel documents and a lack of information regarding the individuals concerned.[30]

Third, UN Security Council actions lacked coordination. In 2005, the UN Security Council had four main bodies dealing with counter-terrorism and overseeing various sanction regimes:

- The CTC, which had a broad counter-terrorism mandate and was assisted by the CTED;
- The 1267 al-Qaeda/Taliban Committee, which was created in 1999 to monitor implementation by states of sanctions against the Taliban, al-Qaeda, and their associates and was assisted by a Analytical Support and Sanction Monitoring Team;
- The 1540 Committee, which was created in 2004 to monitor measures put into place by UN member states to prevent terrorists from obtaining nuclear, chemical or biological weapons; and
- The 1566 working group, established in 2004 to examine measures against people or groups associated with terrorist activities not covered under the al-Qaeda/Taliban resolutions.[31]

Other UN departments and organizations, such as the Terrorism Prevention Branch of the UN Office on Drugs and Crime, not to mention the over 57 regional and functional international organizations, also had counter-terrorism responsibilities.[32] All of these organizations

[30] Many states have pointed to the deficiencies of the "consolidated list"—that is, the list maintained by the al-Qaeda/Taliban Committee and containing the names of individuals and entities associated with al-Qaeda. Problems have ranged from uncertain spellings of names, to lack of details with regard birth dates, addresses, or other identifying information.

[31] See UNSC Resolution 1566 (2004) of October 8, 2004. Russia had introduced this resolution after the terror attack in Beslan Ossetia, in which hundred of students and teachers had been killed by Chechenyan separatists.

[32] In 2003, the CTC had organized a special meeting with these organizations, but it was not given a central coordinating role.

and Committees asked states for information on counter-terrorism efforts—often in different formats. As a result, many states developed "reporting fatigue."[33] Overlapping mandates and duplication of efforts were inevitable and, without a central coordinating body, international efforts lost their sharp focus. Recognizing this problem, the UN Secretary General announced in March 2005 the creation of an implementation task force.[34]

Fourth, no consensus existed within the United Nations about the problem of non-compliant states. With the adoption of UNSC 1373 (2001), the Security Council ordered states to adopt and implement a wide range of measures, but it had neither formal standards for nor the material capacity to evaluate compliance. In addition, there was no agreement among members of the Security Council on the appropriate responses when faced with non-compliance, or on the question of who was authorized to act.

Fifth, the nature of the terrorist threat has evolved considerably since the 1990s. In 2005, the members of the al-Qaeda/Taliban Monitoring Team identified three distinct but related groups: the established al-Qaeda leadership; the fighters who had attended training camps in Afghanistan and had graduated as experienced terrorists; and the growing number of supporters who had never left their countries of residence, but had embraced core elements of the al-Qaeda message. This third group is growing, is mostly unknown to the international community, and presents a great challenge.[35] The terrorist attacks in Madrid (March 2004) and in London (July 2005) were manifestations of these homegrown terrorist challenges.

International coercive measures, such as financial sanctions and travel bans, are of limited value against this third group. First, it is

[33] For example, by September 30, 2003, 48 states were late in submitting their reports to the CTC. All were mentioned in a report to the UN Security Council (see UN document S/2003/1056 of October 31, 2003) and except for Sweden were developing countries. The UN Sanctions Committee overseeing sanctions on the Taliban and al-Qaeda operatives (also known as the 1267 Committee) also complained about the few numbers of states reporting. See UN Document S/2003/669 of July 8, 2003.

[34] See the statement by Kofi Annan at the international summit on Democracy, Terrorism, and Security in March 2005 in Madrid. Press release SG/SM/9757, March 10, 2005. The task force met for the first time in the fall of 2005.

[35] See the Report of the Monitoring Team, UN document S/2005/572 of September 9, 2005, para 8-16. See also the statement by the Chair of 1267 Committee to the UN Security Council on July 20, 2005 (5229th meeting), Press Release SC/8454.

difficult to compile lists of people who do not have terrorist track records. Second, many of these terrorists do not have to travel, because they already live in their target countries. Third, the attacks carried out by this type of terrorists involve small amounts of money that are hard to track.

In sum, sanctions are not panaceas and formidable challenges remain. That said, the international opprobrium on terrorist activities is firmly established. Sanctions helped to bring about this change. Second, the international sanctions machinery established to deny terrorists access to resources and deny them safe havens is now also accepted and likely to be reinforced. Third, national capacities to monitor borders and financial flows are being strengthened. This will have important collateral benefits that might help UN Security Council efforts to deal with violent conflicts and other threats to international peace and security.

A Successful Sanctions Strategy

The track record of sanctions since the end of the Cold War has shown that sanctions are complex policy instruments. The use of sanctions to deal with violent conflicts had limited success in the early-mid 1990s. The Security Council increasingly used sanctions to combat terrorism since the end of the 1990s. At the same time it started to pay greater attention to sanction implementation. The sanctions machinery it has put into place, particularly after September 2001, may also be useful if sanctions are employed in the future to deal with other threats to international peace and security.

An effective sanctions strategy should contain five elements. First, it must assess the target's strengths and weaknesses. Second, it must define an objective. Third, it must determine which tactics to follow. Fourth, it must evaluate and ensure implementation. Fifth, it must subject sanctions regimes to periodic review.

Assessing the Target

The effectiveness of coercive efforts, including sanctions, depends on the economic and political characteristics of the target. These characteristics will determine whether the target is able to withstand economic pressures and devise counter actions that could neutralize the effects of sanctions. Knowledge about the target is particularly important in the case of targeted sanctions.

Sanction designers should start by examining the general characteristics of the target economy. For example, labor-intensive economies tend to be less vulnerable to sanctions. Imposing sanctions on developing or troubled economies may not be advised, because sanctions aggravate existing problems and can result in humanitarian crises. Knowledge about export and import dependencies and the target's main trading partners is key. Sanction designers should also be able to evaluate the volume of overseas assets and the nature of international banking contacts, including the volume and nature of the financial portfolios of the elites to be targeted. When dealing with non-state actors—rebels or terrorists—it is important to know the source of their financial assets and the extent of their international financial and economic networks. Identification of specific target individuals is key, but may be difficult.

Social and political characteristics of the target must also be assessed. The level of group cohesion—the willingness to withstand outside pressures—tends to be stronger in rural and ethnically and religious homogenous societies. Similarly, authoritarian regimes are generally less vulnerable to sanctions than democratic governments because the former are usually better able to control their political opponents. The effectiveness of travel bans depends on knowledge about the social, cultural and political behavior of the ruling elites, rebels or terrorists one is trying to target. Finally, the existence of a political opposition is often cited as one of the critical conditions for the success of sanctions, since one of the principal aims of sanctions is to bolster political opposition to a regime. However, imposing sanctions when the opposition is weak may be counterproductive. Ruling elites may depict their domestic opponents as traitors, and thus amplify existing jingoistic attitudes. This in turn insulates the political leadership from criticism, and allows it to draw strength from its defiance of outside forces.

When a country is in the midst of a civil war, sanctions will often have asymmetric effects, because different groups will almost always have different vulnerabilities. Identifying the different strengths and weaknesses of these groups, including the different effects sanctions may have on them, is essential to avoid hurting innocents or the "good guys."

Objectives

Sanctions can be used to compel, to deny, or to deter political actors. Compellence is particularly difficult in cases of violent conflict. Indeed, the parties engaged in many of these conflicts have become engaged in violent behavior because of perceived threats to the survival of a group, or because of a belief that violent behavior would produce considerable political gain. In intra-state and inter-state conflicts, the stakes are very high.[36] Compelling terrorists is also difficult because they too believe that vital interests are at stake.[37]

Compellence within a multilateral—UN—context is particularly difficult. It requires the members of the UN Security Council to clearly define and agree on what needs to be reversed, and it requires international actors to maintain this consensus over time.[38] Whether they are able to do so will depend on how their interests are affected. The position of the P-5 is particularly important in this regard.

Denial is easier to achieve. However, for denial to be effective, outside powers need to effectively implement embargoes of the singled out goods and/or services. The longer an embargo is in effect, and the more parties are involved, the more difficult that will become. Long-lasting embargoes also tend to lose their effectiveness because the embargoed party will often develop alternative sources of supply.

Deterrence is relatively easy. Deterrence means discouraging certain behavior through fear of the consequences. It "…involves setting the stage—by announcement…—and waiting."[39] This makes why

[36] Similarly, asking states to forego nuclear weapons or stop the development of a nuclear weapons program is extremely difficult. Again, political leaders will embark on such courses only if they believe that vital interests are at stake. They will consequently invest a considerable amount of political capital and resources in the policy. Reversal of the policy could lead to their removal of office. See Sagan, Scott D., "Why do States Build Nuclear Weapons: Three Models in Search of a Bomb," *International Security*, Vol. 21, No3, (Winter 1996/97), pp. 54-86.

[37] Making states stop support terrorist groups is more a question of deterrence than compellence. States sponsors of terrorist, have generally complied with demands to hand over suspected terrorists because few states are willing to publicly support terrorist activities.

[38] As Schelling reminds us "Compellence,… usually involves *initiating* an action (or an irrevocable commitment to action [ChJO: such as the adoption of a UN Security Council Resolution under Chapter VII]) that can cease, or become harmless, only if the opponent responds." See Schelling, *Arms and Influence*, p. 72.

[39] Schelling, *Arms and Influence*, p. 71.

deterrence is easier to achieve, particularly in a multilateral setting. In a multilateral setting, it is not necessary for all outside powers to be able to make that threat credible—it suffices if there is one leader who can. The onus for breaking the deterrent threat is on the other side. Engaging in such an action will not be an easy step to take since retaliation will follow. Deterrence has been particularly effective in reducing state support for terrorist activities.

Sanctions cases have shown that the threat of sanctions is often more effective than their actual imposition.[40] There is also some evidence to suggest that UN sanctions regimes have served as a deterrent to states considering support for terrorists groups.

In sum, sanctions are most effective when they aim to deter political actors—states, in particular—from engaging in behavior that threatens international peace and security. Sanctions are somewhat effective when they aim to deny actors access to resources and services that would make dangerous behavior more difficult. Sanctions are least effective when they are used to compel actors to change or reverse behavior. That said, the threat to impose sanctions has been very effective, when embedded in a comprehensive coercive strategy that included the use of force.

Determining Tactics

Once the target's strengths and weaknesses are properly assessed, sanctions designers must decide which tactics are most likely to be effective: a swift and crushing blow, or a gradual tightening of the screws.

Two schools of thought dominate the debate on sanctions tactics. One school maintains that sanctions are most effective when they are

[40] See, for example the histories of the sanction regimes against; the FRY; Somalia; Libya; Haiti; Sudan; Sierra Leone; and Liberia. Simon Chesterman and Beatrice Pouligny have suggested, "the threat of sanctions may serve to focus the minds of local elites in the context of a bargaining model, with a clear economic choice. Once sanctions are imposed, the clarity of this choice becomes dissipated among the competing economic incentives that emerge." See Chesterman, Simon and Beatrice Pouligny, "Are Sanctions Meant to Work? The Politics of Creating and Implementing Sanctions Through the United Nations," *Global Governance*, Vol. 9 (2003), p. 512. See also David Cortright, and George A. Lopez, *Sanctions and the Search for Security: Challenges for UN Action* (Boulder: Lynne Rienner Publishers, 2002), pp. 13-15; and Chantal de Jonge Oudraat, "UN Sanction Regimes and Violent Conflict."

imposed immediately and comprehensively. Those who subscribe to this line of thinking argue that sanctions should be imposed early in a crisis, since gradual action gives the target time to adjust by, for example, stockpiling supplies, finding alternative trade routes and partners, and moving financial assets.[41]

The other school of thought contends that sanctions are most effective when imposed gradually and incrementally. Proponents argue that swift and crushing blows are the equivalent of wars by attrition, which will almost always cause people to rally behind the regime and solidify the target's position. They argue that sanctions are instruments that should bring parties to the negotiating table.[42]

Both schools of thought are right some of the time. The objectives to be achieved, the political and economic characteristics of a target, and the target's environment, including implementation capacity, are the keys to determining which approach to choose. In determining whether to strike quickly and bluntly or slowly and softly, outside powers should consider the seriousness of the situation at hand. Sanctions should be proportionate to the objective: the more ambitious the goal, the stronger the sanctions regime. When outside powers are faced with trying to reverse gross violations of human rights or genocide, they may want to forego the imposition of sanctions altogether and intervene militarily. In almost all cases, the threat of the use of force should remain on the table. It greatly enhances the deterrent threat of sanctions, as seen in Haiti and the FRY.

[41] See, for example, Elliot, Kimberly Ann, "Factors Affecting the Success of Sanctions," in Cortright, David and George Lopez, eds. *Economic Sanctions: Panacea or Peacebuilding in a Post-Cold War World?* (Boulder: Westview Press, 1995), pp. 51-60; Carnegie Commission on Preventing Deadly Conflict, *Preventing Deadly Conflict: Final Report* (New York: Carnegie Corporation of New York, December 1997), p. 54; U.S. Department of State, Inter-Agency Task Force on Serbian Sanctions, "UN Sanctions Against Belgrade: Lessons Learned for Future Regimes," in *The Report of the Copenhagen Round Table on UN Sanctions: The Case of the Former Yugoslavia, Copenhagen 24-25 June 1996 and Annexes* (Brussels: SAMCOMM, European Commission, 1996), p. 327.

[42] See, for example, Eland, Ivan, "Economic Sanctions as Tools of Foreign Policy," in Cortright, David and George Lopez, eds. *Economic Sanctions: Panacea or Peacebuilding in a Post-Cold War World?* (Boulder: Westview Press, 1995), pp. 29-42; McDermott, James, Ivan Eland, and Bruce Kutnick, *Economic Sanctions Effectiveness as Tools of Foreign Policy* (Washington, DC: U.S. General Accounting Office, February 1992, GAO/NSIAD-92-106).

Evaluating and Ensuring Implementation

Sanctions strategists also must evaluate the target's environment—in particular, the economic and political characteristics of neighbors. Third-party compliance with sanctions regimes is critical. Four problems stand out.

First, interpretation problems interfere with the effectiveness of sanctions. Once a UN sanctions resolution is adopted, most states have to adopt national legislation to implement UN measures. However, the language of UN sanctions resolutions is often the result of compromise formulations with vague and ambiguous wording.[43] The interpretation of sanctions resolutions will thus often vary from state to state. In addition, interpretation problems may lead to acrimonious discussions within UN Sanction Committees. This undermines political unity, and may lead targets to doubt the resolve of outside powers. Building a strong political consensus is key, and may help overcome some of these issues.

Second, the uneven distribution of sanctions costs is a problem. The costs of sanctions are almost always distributed unequally across states. Sanctions often have unintended negative effects on third states, and some states are harder hit than others. Moreover, targeted states may engage in countermeasures and make the cost of compliance too high for third parties.[44] Without assistance from the international community, these states may not be sufficiently motivated to implement and enforce the sanctions regime in question.[45]

Third, capacity problems must be addressed. Few states have the expertise or resources needed to establish or maintain efficient monitoring and enforcement mechanisms. Sanctions regimes that do not investigate violations and consequently deal with violators are regimes that ultimately lose their credibility. Since the late 1990s state capacities to monitor and regulate financial services and physical borders has

[43] Many authors have argued that the UN Security Council should adopt standardized texts for its sanctions resolutions. This would also facilitate efforts to develop national legislation for sanction regimes. See Cortright and Lopez, *The Sanctions Decade*, p. 234.

[44] Indeed, the enforcement of a sanction regime may entail the use of force. Naval blockades are the most common sanction enforcement mechanism.

[45] Article 50 of the UN Charter gives states the right to consult with the Security Council if they suffer unduly from sanctions imposed on other countries.

improved, but more needs to be done. Improving state capacity would also help to stabilize regions as a whole—an important collateral benefit. Finally, building up state capacity has potential strong deterrent effects.

Fourth, outside actors need to deal with non-compliant third parties. A regime that does not deal with violations will quickly lose its effectiveness. The use of investigative panels and naming and shaming has produced good results.[46] Similarly, the threat and use of secondary sanctions against non-compliant states seems effective.[47]

Implementation—third-party compliance—is essential for the effectiveness of sanctions efforts. They require the building of an international political consensus, the provision of financial resources to address burden-sharing problems, capacity building, and the establishment of monitoring and enforcement mechanisms. Contrary to popular belief, economic sanctions are not cost-free.

Periodic Review

All sanction regimes should be subject to periodic review. Time limits in sanctions resolutions force states to periodically question whether sanctions should be maintained.[48] Those imposing sanctions should also formulate the conditions under which sanctions should be lifted. Sanctions may be lifted either because the behavior that led to

[46] In the case of the sanctions imposed on the UNITA rebels in Angola, this led to good results. According to one observer, those sanctions were among the best observed and most effective in Africa. See Vines, “Monitoring UN Sanctions in Africa,” pp. 253. Vines also notes that compliance was so good because of the political will in the Security Council and an aggressive advocate—the Angolan government. Ibid.

[47] In 2001, the Security Council imposed secondary sanctions on Liberia and on key individuals in Liberia responsible for undermining the peace process in Sierra Leone. This was the first time that the Council imposed secondary sanctions.

[48] Since 2000, all UN sanctions regimes have included time limits. That said, the issue of time limits remains very controversial and was triggered by the debate over the Iraq sanctions. In the late 1990s France and Russia had been advocating a change in the sanctions regime on Iraq. However, the U.S. and the UK opposed this and were able to block such a decision by the Council. The UK and the U.S. are in principle opposed to time limits, even though they have voted in favor of Council resolutions that have imposed such limits. They have argued that time limits take the bite out of sanctions. France and Russia, on the contrary, have argued that periodic renewal of a sanctions regime shows resolve by UN Security Council members. These issues have been discussed at length in the UN Informal Working Group on General Issues of Sanctions. See the statement of the Chairman of the Group, S/2003/1197, January 22, 2004.

their imposition has changed, or because sanctions have failed to bring the desired results.[49] If the imposition of sanctions has no political effect, two alternatives should be considered. First, outside powers can promise to lift some elements of a sanctions regime if the target starts to engage in "good" behavior. That said a "carrot-and-stick" approach requires accurate and timely assessments of the target's aspirations and intentions. Outside powers should be careful that the target doesn't use this opportunity to strengthen its forces so it can resume its deviant behavior later on. The second alternative is to increase pressure on the target by threatening the use of military force. The threat may have to be made early if the target is not vulnerable economically or politically. The threat to use force often makes sanctions more effective by giving credibility to the coercive effort.

Conclusion

The UN Security Council has used economic sanctions on many occasions since the end of the Cold War to maintain and restore international peace and security. The use of sanctions changed dramatically over this period. In the early 1990s sanctions were comprehensive in scope, had ambitious objectives, and focused on violent conflicts. Their track record was poor. In the mid and late 1990s, the Security Council increasingly turned to targeted sanctions. It also scaled down the strategic objectives it sought to achieve and became increasingly focused on terrorism. Together, these developments improved the sanctions track record.

Economic sanctions are complex policy instruments. Although formidable challenges remain, the international community has steadily improved its understanding of economic sanctions—and hence their effectiveness.

[49] The importance of exit or termination strategies has been recognized within the UN community. However, in practice such strategies have not been adopted. See, for example, *United Nations Sanctions as a Toll of Peaceful Settlement of Disputes: Non-paper submitted by Australia and the Netherlands*, A/50/322, August 3, 1995.

Table 1 UN Security Council Sanctions Imposed under Chapter VII of the UN Charter (1945-2005)

Country/Groups	Date Imposed	Date Lifted	Arms*	TS†	CES‡	Enabling UNSC Resolution
Southern Rhodesia	Dec 1966	Dec 1979			Y	232 (1966) 460 (1979)
South Africa	Nov 1977	May 1994	Y			418 (1977) 919 (1994)
Iraq	Aug 1990	May 2003			Y	661 (1990)[50]
	May 2003		Y			1483 (2003)[51]
Republics of the Former Yugoslavia	Sept 1991	June 1996	Y			713 (1991)[52] 1021 (1995)
Federal Republic of Yugoslavia	May 1992	Nov 1995			Y	757 (1992)[53] 1022 (1995)[54]
	Mar 1998	Sept 2001	Y			1160 (1998) 1367 (2001)[55]
Bosnian Serbs	Sept 1994	Oct 1996			Y	942 (1994) 1074 (1996)
Somalia	Jan 1992		Y			733 (1992) 1425 (2002)[56]
Libya	Mar 1992	Apr 1999 (suspension) Sept 2003 (lifted)	Y	Y		748 (1992)[57] S/PRST/1999/10 1506 (2003)
Liberia	Nov 1992	Mar 2001	Y			788 (1992)
	Mar 2001		Y	Y		1343 (2001)[58]
Haiti	June 1993	Aug 1993	Y	Y		841 (1993) 861 (1993)
	Oct 1993		Y	Y		873 (1993)
	May 1994	Oct 1994			Y	917 (1994)[59] 944 (1994)
UNITA (Angola)	Sept 1993	Dec 2002	Y	Y		864 (1993)[60]
Rwanda	May 1994	Aug 1995	Y			918 (1994)[61] 1011 (1995)[62]
Sudan	May 1996	Sept 2001		Y		1054 (1996)[63] 1372 (2001)
	July 2004		Y			1556 (2004)
	Mar 2005		Y	Y		1591 (2005)[64]
Sierra Leone	Oct 1997		Y	Y		1132 (1997)[65]
Taliban (Afghanistan)	Nov 1999		Y	Y		1267 (1999)[66]
Eritrea/Ethiopia	May 2000	May 2001 (expiration)	Y			1298 (2000)
Terrorists/States/Non-state actors UNSC 1373	Sept 2001		Y	Y		1373 (2001)[67]
Democratic Republic of the Congo	July 2003		Y			1493 (2003)[68]
Terrorists/Nonstate actors	Apr 2004		Y			1540 (2004)[69]
Côte d'Ivoire	Dec 2004		Y	Y		1572 (2004)[70] 1584 (2005)

Notes: ***Arms Embargo, †Targeted Sanctions, ‡Comprehensive Economic Sanctions.** See additional table notes on following pages.

Source: United Nations, Office of the Spokesman for the Secretary-General, Use of Sanctions under Chapter VII of the UN Charter, March 31, 2000, http://www.un.org/News/ossg/sanction.htm.

[50] For subsequent resolutions on Iraq, see Office of the Spokesman for the Secretary-General (OSSG), Use of Sanctions under Chapter VII of the UN Charter, http://www.un.org/News/ossg/sanction.htm.

[51] UNSC Resolution 1483 (2003) of May 22, 2003, ended all sanctions established by UNSC Resolution 661 (1990) of August 6, 1990, with the exception of sale or supply of arms and related materiel, other than those required by the occupying power to serve the purposes of Security Council resolutions.

[52] See also UNSC Resolution 727 (1992) of January 8, 1992, which reaffirmed that the arms embargo applied to all republics of the former Yugoslavia.

[53] See also UNSC Resolution 787 (1992) of November 16, 1992, and UNSC Resolution 820 (1993) of April 17, 1993, which strengthened the sanctions regime. UNSC Resolution 943 (1994) of September 23, 1994, suspended certain sanctions on the Federal Republic of Yugoslavia.

[54] Sanctions were suspended in November 1995. They were lifted on October 1, 1996. See UNSC Resolution 1074 of October 1, 1996.

[55] This resolution, passed by a unanimous vote, lifted the remaining sanctions on the Federal Republic of Yugoslavia and ended the work of its sanctions committee.

[56] UNSC Resolution 1425 (2002) of July 22, 2002, established a panel of experts to study the violations of the arms embargo imposed in 1992. See also UNSC Resolution 1474 (2003) of April 8, 2003, and UNSC Resolution 1558 (2004) of August 17, 2004, which extended the panel's mandate.

[57] Targeted sanctions included a reduction of Libyan diplomatic personnel serving abroad. See also UNSC Resolution 883 (1993) of November 11, 1993, which tightened sanctions on Libya, including freezing funds and financial resources in other countries and banning provision of equipment for oil refining and transportation. On September 12, 2003, UNSC Resolution 1506 (2003) formally lifted all sanctions against Libya and terminated the mandate of the sanctions committee.

[58] Additional measures in this resolution included a ban on the direct or indirect import of all rough diamonds from Liberia and travel restrictions on senior members of the government and their spouses as well as any other individuals who provide financial and military support of armed rebel groups in countries neighboring Liberia.

[59] UNSC Resolution 917 transformed the sanctions regime into a comprehensive regime.

[60] See also UNSC Resolution 1127 (1997) of August 28, 1997, and UNSC Resolution 1130 (1997) of September 29, 1997, which strengthened the sanctions regime.

[61] See also UNSC Resolution 997 (1995) of June 9, 1995, which affirmed that the prohibition on the sale and supply of arms for use in Rwanda also applied to persons in the states neighboring Rwanda.

[62] The sale and supply of arms to nongovernmental forces for use in Rwanda remained prohibited.

[63] See also UNSC Resolution 1070 (1996) of August 16, 1996, which foreshadowed an air embargo on Sudan. This embargo never went into effect because of the expected humanitarian consequences.

[64] In January 2006 the Panel of Experts on Sudan submitted to the Security Council a confidential list of names the panel believed should be designated for sanctions. See S/2006/65, January 2006.

[65] UNSC Resolution 1306 (2000) of July 5, 2000, prohibited the direct or indirect import of all rough diamonds from Sierra Leone. UNSC Resolution 1385 (2001) of December 19, 2001, extended the ban for a period of eleven months, to be further extended by UNSC Resolution 1446 (2002) of December 4, 2002, for an additional period of six months.

[66] See also UNSC Resolution 1333 (2000) of December 19, 2000, which established an arms embargo, targeted financial sanctions (Bin Laden and associates), and a flight ban; UNSC Resolution 1390 (2002) of January 16, 2002, and UNSC Resolution 1455 (2003) of January 17, 2003, maintained sanctions measures in UNSC Resolution 1267 (1999).

[67] Resolution 1373 also established a Counter-Terrorism Committee (CTC) to monitor implementation of the resolution. In March 2004 the Security Council established a Counter-Terrorism Executive Directorate (CTED) to assist the CTC.

[68] UNSC Resolution 1493 (2003) of July 28, 2003, imposed a ban on all arms, related materiel, and assistance, advice, or training related to military activities. See also UNSC Resolution 1553 (2004) of March 12, 2004, establishing a sanctions committee and UNSC Resolution 1596 (2005) of April 18, 2005, which added a travel ban and an assets freeze to those violating the embargo.

[69] UNSC Resolution 1540 decided that all states shall act to prevent the proliferation of WMD, particularly to nonstate actors.

[70] See also UNSC Resolution 1584 (2005). In February 2006, three individuals were put on the sanctions list.

About the Authors

Heiko Borchert directs a business and political consultancy in Switzerland and is member of the advisory board of IPA Network International Public Affairs. He has worked with different military and national security organizations in Switzerland, Austria, and Germany on issues like scenario-based security policy planning, security sector evaluation, homeland security, defense science and technology, and energy security.

Esther Brimmer is Deputy Director and Director of Research at the Center for Transatlantic Relations (CTR) at the Paul H. Nitze School of Advanced International Studies at The Johns Hopkins University. She has served as a Member of the Office of Policy Planning at the U.S. Department of State, a Senior Associate at the Carnegie Commission on Preventing Deadly Conflict and as a Special Assistant to the Under Secretary of State for Political Affairs. She has written numerous articles and book chapters on international security issues. She is the author of a Chaillot paper entitled: *Seeing Blue? American Visions of the European Union* (2007). Her edited volumes for CTR include: *Transforming Homeland Security: U.S. and European Approaches* (2006).

M. Elaine Bunn leads an INSS project assessing future strategic capabilities and concepts. Before joining INSS, she held a number of policy management and analysis positions in the Office of the Secretary of Defense beginning in 1980. She served as Principal Director, Nuclear Forces and Missile Defense Policy, in the Office of the Assistant Secretary of Defense for Strategy and Threat Reduction from 1993-98. Her other assignments in OSD include Staff Analyst, Deputy Director, and Acting Director in the Office of Strategic Defense Policy, Staff Analyst, Strategic Arms Control Policy, and Staff Analyst, Theater Nuclear Forces Policy. Ms. Bunn was with the RAND Corporation 1998-2000 on a DoD exchange assignment. From February through June 2001, she co-chaired a nuclear panel for the Secretary of Defense, framing issues for the 2001 Nuclear Posture Review.

Richard Burmood, Senior Doctrine and Policy Analyst (L3 Communications), JTF-CS Plans and Policy Directorate, is the primary writer and lead contributor of the paper co-written with Barry Cardwell and Bruce Davis.

Barry Cardwell, Deputy Division Chief, Strategy and Policy Division, USNORTHCOM, provided significant background material and technical information on the U.S. Department of Defense Homeland Defense and Civil Support Joint Operating Concept and the National Homeland Security Plan concept.

Chantal de Jonge Oudraat is Associate Vice President, Jennings Randolph Fellowship Program at the United States Institute of Peace. At the time of writing, she was Senior Fellow and Research Program Coordinator at the Center for Transatlantic Relations. She was also an Adjunct Professor at the Edmund A. Walsh School of Foreign Service, Georgetown University and Vice-President of Women in International Security (WIIS). Previously she served as co-director of the Managing Global Issues project at the Carnegie Endowment for International Peace in Washington, D.C. (1998-2002), Research Affiliate at the Belfer Centre for Science and International Affairs, Harvard University (1994-1998), and Senior Research Associate at the United Nations Institute for Disarmament Research (UNIDIR) in Geneva (1981-1994). Her research focuses on the United Nations, arms control and disarmament, peacekeeping, use of force, economic sanctions and U.S.-European relations. She is the co-editor of *Managing Global Issues: Lessons Learned* (2001) and the author of many book chapters and articles.

Bruce Davis, Major General, U.S. Army, is the Commander of Joint Task Force Civil Support, Fort Monroe, Virginia. His service includes Deputy Commanding General of the 32nd Army Air and Missile Defense Command at Fort Bliss, TX; and later Deputy Director of Headquarters Department of the Army G33, Operations, Readiness and Mobilization and the Army Operation Center at the Pentagon. He served as the Principal Director, Deputy Assistant Secretary of Defense—Reserve Affairs for Readiness, Training and Mobilization prior to assuming command of JTF-CS in 2004.

Sean Duggan is a Special Assistant to the National Security Team at the Center for American Progress. His research areas include military affairs, terrorism, foreign policy, and Middle East affairs. He co-authored the report "Caught Off Guard: The Link Between Our National Security and Our National Guard" (May 2007).

Karina Forster directs IPA International Public Affairs Network, a Berlin-based consultancy focusing among other things on defense and security, energy, and trade. Prior to joining IPA, she worked for U.S. consultancies, the European Parliament, the European Commission and the German Bundestag.

Daniel Hamilton is the Richard von Weizsäcker Professor and Director of the Center for Transatlantic Relations at the Paul H. Nitze School of Advanced International Studies (SAIS), Johns Hopkins University; and Executive Director of the American Consortium on EU Studies (ACES), a cooperative venture among five major universities in the nation's capital. He leads the international policy work of the Johns Hopkins-based U.S. National Center of Excellence on Homeland Security, awarded by the U.S. Department of Homeland Security. Hamilton has held a variety of senior positions in the U.S. Department of State, including Deputy Assistant Secretary for European Affairs, responsible for NATO, OSCE and transatlantic security issues, Balkan stabilization, and Northern European issues; and Senior Policy Advisor to the U.S. Ambassador and U.S. Embassy in Germany. He has authored and edited many articles and books, most recently *The Transatlantic Economy 2008* (with Joseph P. Quinlan).

Lawrence Korb is a Senior Fellow at the Center for American Progress and a Senior Advisor to the Center for Defense Information. Prior to joining the Center, he was a Senior Fellow and Director of National Security Studies at the Council on Foreign Relations. From July 1998 to October 2002, he was Council Vice President, Director of Studies, and holder of the Maurice Greenberg Chair. Prior to joining the Council, Mr. Korb served as Director of the Center for Public Policy Education and Senior Fellow in the Foreign Policy Studies Program at the Brookings Institution, Dean of the Graduate School of Public and International Affairs at the University of Pittsburgh, and Vice President of Corporate Operations at the Raytheon Company. Korb served on active duty for four years as a Naval Flight Officer, and retired from the Naval Reserve with the rank of Captain.

James Lebovic is Associate Professor of Political Science and International Affairs at The George Washington University. The author of *Deterring International Terrorism and Rogue States: U.S. National Security Policy after 9/11* (Routledge, 2007), he has written widely on nuclear deterrence, defense spending and policy, weapons acquisition, and international conflict.

Colonel Charles D. Lutes, USAF, was Senior Military Fellow in the INSS Research Directorate, and a member of the Future Strategic Concepts group at the time of writing. He currently serves at the National Security Council as Director for Counterproliferation Strategy. Col. Lutes' prior assignment was as chief of the Weapons of Mass Destruction (WMD) division under the J-5 Deputy Director for the War on Terror. He also served in J-5 as chief of the Strategic Plans Branch. Col. Lutes' expertise is in such areas as WMD proliferation, counter-terrorism, military planning, military strategy and strategic concept development.

Jennifer Machado is currently working as an independent contractor. She served as an Intelligence Analyst for the California Office of Homeland Security at the California State Terrorism Threat Assessment Center. Prior to that, she was a Fellow with the National Center for the Study of Terrorism and Responses to Terrorism (START), part of the Homeland Security Center of Excellence for Behavioral and Social Research on Terrorism and Counter-Terrorism.

Tamara Makarenko works in the private sector as a partner of an applied intelligence consultancy and retains academic affiliations with the Silk Road Studies Programme at Uppsala University and the Diplomatic Academy of London. She is an internationally recognized authority on the interaction between organized crime and terrorism. Her expertise was primarily gained from conducting field research in emerging economies, conflict and post-conflict environments. She has direct experience investigating related issues including: the structure of criminal and terrorist networks with a focus on financial sources, smuggling networks (i.e. arms and narcotics), arms trafficking and weapons proliferation, dual use technologies, and related political corruption.

Robert Quartel serves as Chairman, Chief Executive Officer, and Founder of FreightDesk Technologies. Mr. Quartel is a former U.S. Federal Maritime Commissioner, and is an internationally recognized expert in maritime and national transportation policy. From 1992-1994, he served as President of the U.S. Shipbuilding Consortium and later served as President of the Jones Act Reform Coalition. In October

2001 Mr. Quartel developed a concept for profiling international container cargoes ("Pushing the Border Out") before they moved onto ships for transport to the United States.

Sir David Omand GCB was the first holder in 2002 of the post of UK Security and Intelligence Coordinator, exercising overall direction on behalf of the Prime Minister of the national counter-terrorism strategy and building national resilience ("homeland security") and with responsibility for the health of the UK's intelligence community including holding the budget for the UK's three secret Intelligence Agencies. He also acted as the Government's chief crisis manager for civil contingencies. Before that he was Permanent Secretary of the Home Office, having previously been Director of the Government Communications Headquarters (GCHQ), the UK's Sigint agency. He spent much of his earlier career in the Ministry of Defense, including as Deputy Secretary for Policy, as Under Secretary in charge of the defense program, and as Principal Private Secretary to the Secretary of State. He served for three years in Brussels on loan to the Diplomatic Service as Defense Counselor to NATO. He was particularly concerned in MOD with the reshaping of the long term equipment program, for the British military contribution in restoring peace in the former Yugoslavia and for the recasting of British nuclear deterrence policy at the end of the Cold War. He served for seven years on the UK's Joint Intelligence Committee. He retired in April 2005. He is a visiting Professor at the War Studies Department of King's College, London.

Amy Sands is the Provost and Academic Vice President of the Monterey Institute of International Studies. Prior to becoming Provost, she held two other positions at the Monterey Institute—Dean of the Graduate School of International Policy Studies, and Deputy Director of the Center for Nonproliferation Studies. Her responsibilities involved strategic oversight and daily management of the Center's projects and activities. From August 1994 to June 1996, she was Assistant Director of the Intelligence, Verification, and Information Management Bureau at the U.S. Arms Control and Disarmament Agency (ACDA). Before joining ACDA, she led the Proliferation Assessments Section of Z Division (Intelligence) at the Lawrence Livermore National Laboratory and was Country Risk Manager of New England Merchants Bank.

Jonathan Stevenson, professor of Strategic Studies in the Strategic Research Department of the Center for Naval Warfare Studies at the Naval War College, joined the War College's civilian faculty in 2005. From 1999-2005, he was Senior Fellow for Counter-terrorism and Editor of *Strategic Survey* at the International Institute for Strategic Studies (IISS) in London, and in 2004-05 was also Director of Studies of the IISS-US in Washington. He practiced law for six years with the New York City law firm of LeBoeuf, Lamb, Greene & MacRae. His books include *"We Wrecked the Place": Contemplating an End to the Northern Irish Troubles* (The Free Press/Simon & Schuster, 1996) and *Losing Mogadishu: Testing U.S. Policy in Somalia* (Naval Institute Press, 1995). Stevenson has also published two monographs: *Counter-terrorism: Containment and Beyond*, Adelphi Paper 367, 2004; and *Preventing Conflict: The Role of the Bretton Woods Institutions*, Adelphi Paper 336, 2000.

About PACER

The Center of Excellence for the Study of Preparedness and Catastrophic Event Response (PACER)

The role of universities and research organizations as part of this country's strategic approach to Homeland Security is to harness the nation's scientific knowledge and technological expertise to help protect America and our way of life from terrorism. Moreover, this same knowledge and expertise can be applied to helping this country prepare for and respond to other high consequence events, whether natural or manmade, by promoting novel thinking, generating innovation, and teaching and training the next generation of leaders in science, government, and education. Recognizing this particularly important role in our nation's defense, in December 2005, the U.S. Department of Homeland Security awarded Johns Hopkins University's www.hopkins-cepar.org (CEPAR) a multiple year grant to establish the National Center of Excellence for the Study of Preparedness and Catastrophic Event Response (PACER) to lead a consortium studying how the nation can best prepare for and respond to potential large-scale incidents and disasters.

Homeland Security Center of Excellence consortium, led by CEPAR and under the direction of Principal Investigators Dr. Gabor Kelen and Dr. Lynn Goldman, comprises leading universities, premier corporations with extensive research and development infrastructure, and key government and national organizations from around the country. This consortium also includes the significant involvement of and contributions by minority serving institutions and organizations. Collectively, PACER engages in multidisciplinary, trans-institutional research to study deterrence, prevention, preparedness and response, including issues such as risk assessment, decision-making, infrastructure integrity, surge capacity and sensor networks, and to create knowledge directed toward increased national preparedness for weapons of mass destruction (WMD), and other catastrophic high consequence events.

The mission of PACER **is improve the Nation's preparedness and the ability to respond in the event of a high consequence natural or manmade disaster to alleviate the event's effects by developing and disseminating best scientific practices**. To best achieve this mission, PACER is conducting seventeen different projects focused on five key areas of research: preparedness theory and practice; response networks; analysis, modeling, and simulation; science, technology, and engineering; and education. The education research area, in particular, has been tasked with developing an infrastructure to train disaster experts, from today's scientists to tomorrow's leaders in academia, health care, and public service. Furthermore, PACER has established eight principals around which research projects focus: understanding high impact Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) events; conducting inquiries that serve the goals of the Department of Homeland Security (DHS) and the National Response Plan (NRP); providing relevance to first responders at all levels; engaging all levels of government, public and private sectors for a fully integrated approach; leveraging the diverse resources of our partners to augment efforts; developing educational programs and concepts for broad dissemination to train future leaders, experts, and scholars; engaging appropriate efforts to achieve sustainability; and maintaining flexibility, given the potential changing threats and the need to be prepared for all hazards.

Harnessing the scientific capabilities of some of this nation's finest research institutions, and collaborating with federal, state, and local government partners, PACER will not only further our knowledge and understanding of high consequence events, but will further our country's ability to effectively deter as well as prepare for and respond to such events.