



Building Transformational Partnerships to Combat WMD Terrorism

Thomas Lehrman, Director, Office of Weapons of Mass Destruction Terrorism

Remarks at the U.S. Military Academy
Washington, DC
November 7, 2006

Introduction

The events of September 11, 2001 awoke the United States and the world to a new era. On that day, we confronted the threat of terrorists carrying out attacks with ever more destructive weapons. We had left behind the Cold War and had entered a new strategic environment marked by a very different kind of threat. In this new environment, we face our most dangerous enemies in the form of transnational terrorist networks, motivated by violent and extreme ideologies, and which have declared their intent to use weapons of mass destruction against us.

As we face enemies who are willing to inflict mass death on innocent civilians, we also confront the danger of illicit networks selling WMD and related technology to the highest bidder, and through whom terrorists may seek their new weapons of choice. Preventing this nexus of terrorism and the proliferation of WMD is the preeminent challenge to international peace and security in the twenty-first century. Meeting this challenge will require that the United States develop a network of transformational partnerships - within our own government, with international organizations, with partner nations and their constituent governments, and with the private sector.

Disruptive Technologies, Networks, and the Risk of WMD Terrorism

In the history of warfare, technological change has played a central role in shifting the landscape of rivalry and advantage among peoples and nations. For example, it was the use of the stirrup in the seventh century that contributed to the swift Arab conquest of North Africa and to the development of the emerging European feudal social order. Later, the development of the crossbow and then firearms catalyzed new forms of military organization and the economic and social orders that sustained them. In the nineteenth and twentieth centuries, the internal combustion engine led to the development of the tank and enabled the tactics of *blitzkrieg* employed by Hitler to bypass the Maginot line and occupy France and much of Europe. Eventually, the United States raised up its own technological and industrial base to neutralize and then surpass the early advantages of the Axis powers. But the lesson is clear - every epoch has its ascendant technologies which enable new forms of organization, both social and military, and which can shift the balance of power among and between nations and peoples.

We find ourselves today living through an era of profound technological change, which brings with it both opportunities as well as new security challenges. The advances in the fields of semiconductors and fiber optics since the 1950s have enabled the digital electronic networks of today and have accelerated the pace of globalization and led to a period of unprecedented prosperity. As globalization has taken hold, terrorists have sought to extend their reach and multiply their power by using these same technologies to coordinate their operations as well as to incite action by decentralized cells operating closer to their targets of choice. The networked character of these terrorist organizations presents a growing risk that they will link up with other illicit networks trafficking in WMD and related materials. At the same time, advances in the biological sciences, as well as the diffusion of WMD-related information through the Internet, have lowered the "barriers to entry" for terrorist organizations seeking to develop their own weapons of mass destruction. As President Bush stated clearly in his speech at the National Defense University in 2004:

"These terrible weapons are becoming easier to acquire, build, hide, and transport. Armed with a single vial of a biological agent or a single nuclear weapon, small groups of fanatics, or failing states, could gain the power to threaten great nations, threaten the world peace."

Our National Strategy

Combating this gathering danger of the nexus of WMD and terrorism requires a forward-looking strategic vision, and President Bush has supplied that vision. In 2002, the President signed the National Strategy for Combating Weapons of Mass Destruction, which urged that "the full range of counterproliferation, nonproliferation, and consequence management measures must be brought to bear against the WMD terrorist threat, just as they are against states of greatest proliferation concern."

This past summer the President announced a new National Strategy for Combating Terrorism and identified the central importance of bringing together our traditional counterterrorism, counterproliferation, and nonproliferation tools into an integrated and comprehensive strategy for combating WMD terrorism. This new strategy emphasizes the following six objectives:

- Determining terrorists' intentions, capabilities, and plans to develop or acquire WMD;
- Denying terrorists access to the materials, expertise, and other enabling capabilities required to develop WMD;
- Deterring terrorists from employing WMD;
- Detecting and disrupting terrorists attempted movement of WMD-related materials, weapons, and personnel;
- Preventing and responding to a WMD-related terrorist attack; and
- Defining the nature and source of a terrorist-employed WMD device.

The strategy also emphasizes the need to achieve an effective implementation of all six objectives simultaneously to minimize the risk of a WMD terrorist attack. We often refer to this systematic approach to combating WMD terrorism as a layered defense-in-depth.

Risk Management: A Framework for Optimizing Scarce Government Resources

But, since government resources are finite, an effective combating WMD terrorism strategy should also outline a methodology for allocating resources most efficiently among the many programs and initiatives that compete for the attention of both the executive and legislative branches. An integrated risk management methodology provides an intellectually rigorous framework for enabling policymakers, as well as academics here at West Point, to identify the right mix of capabilities to optimize reduction in WMD terrorism risk.

To understand this concept of risk management, it is helpful to have a clear understanding of what we mean by WMD terrorism risk. From the perspective of a country, city, or any other area, one can view risk as a composite function that brings together three distinct concepts: threat, vulnerability, and consequences. In this framework, "threat" refers to the probability of a particular attack type on a particular target, "vulnerability" to the probability that a particular attack type will result in damage, and "consequences" to the expected scale of damages from a particular attack type. Overall risk against a particular target is thus the product of those three factors, for each of the attack types of sufficient probability to evaluate.

The challenge facing our government lies in optimizing the reduction of risk with each marginal dollar allocated to combating WMD terrorism. Not only should we compare existing programs, but we should seek to examine the opportunity costs of existing programs across all agencies of government, an effort which the National Counterterrorism Center with its mandate by law to conduct strategic operational planning is well-positioned to conduct. A comprehensive approach to risk management

will also evaluate the opportunities for private sector risk mitigation, and the possibility of shifting government risk mitigation responsibilities to the private sector through appropriate laws and regulations.

Transformational Diplomacy and the Centrality of Partnerships

While the risk of WMD terrorism involves many uncertainties, what we do know for sure is that no nation possesses the resources to combat the global challenge of WMD terrorism alone. Reducing WMD terrorism risk to the fullest extent possible demands a broad range of international partnerships, partnerships that are capable of closing gaps in national laws and regulations - as well as in enforcement capabilities - that terrorists and other illicit actors exploit to carry on their lethal activities.

In a January 2006 address at Georgetown University, Secretary Rice articulated the nature of the threats we face today and the role that technology is playing in this new environment: "Technology is collapsing the distance that once clearly separated right here from over there. And the greatest threats now emerge more within states than between them..." After identifying the challenge, the Secretary supplied a vision of transformational diplomacy for overcoming these challenges:

"...I would define the objective of transformational diplomacy this way: to work with our many partners around the world, to build and sustain democratic, well-governed states that will respond to the needs of their people and conduct themselves responsibly in the international system. Let me be clear, transformational diplomacy is rooted in partnership; not in paternalism. In doing things with people, not for them; we seek to use America's diplomatic power to help foreign citizens better their own lives and to build their own nations and to transform their own futures."

Developing Common Interests and the Importance of Indirect Risk

As Secretary Rice made clear, only a flexible network of partnerships that adapts to the changing nature of threat will provide us with the security we seek. A flexible and global network will deter potential attackers, enable us to detect plots and provide early warning to our partners, provide a platform for cooperative emergency response to defeat imminent attacks, and enable an effective and timely response following an attack.

But how do we catalyze and sustain this network of partnerships? High principle can help to launch these partnerships, but sustaining them over time will require that we identify common interests. We will discover that some countries judge themselves at risk of a WMD terrorist attack on their own soil, while others do not share that sense of the threat. In the latter case, we will have to raise the awareness of the indirect risks these partners face from a WMD terrorist attack occurring outside of their territory. Such indirect risks could include the economic, reputational, and security consequences that these partners will suffer if they allow WMD traffickers and terrorists to exploit their ports and airports, their financial systems, and other physical, virtual, and legal safe havens subject to their jurisdiction.

We have already begun to develop this transformational network of partnerships to combat WMD terrorism. In Rabat, Morocco, on October 30-31, Australia, Canada, China, France, Germany, Italy, Japan, Kazakhstan, Morocco, Turkey, and the United Kingdom joined the United States and Russia as partner nations in the Global Initiative to Combat Nuclear Terrorism, a comprehensive approach to combating the most serious international security threat we face today. All thirteen nations committed themselves to a Statement of Principles to expand and accelerate the development of partnership capacity to combat nuclear terrorism on a determined and systematic basis. The International Atomic Energy Agency joined the group as an observer. In the coming months, this network will expand to include other partner nations sharing our commitment and will help to coordinate activities, such as training exercises and technical workshops, to strengthen our individual and collective capabilities against this threat.

A Transformational Partnership Concept: Multinational Interagency Operations

While the State Department can begin the process of building the partnerships we need, diplomacy alone cannot develop the capabilities we need. Realizing those capabilities will depend on the sustained efforts of our interagency partners at the Departments of Defense, Homeland Security, Justice, Energy, Treasury, Commerce, Health and Human Services, among other agencies. Strengthening our capabilities will require the development of new systems, operational concepts that enable those systems to be put to good use, and training and exercising relationships that enable confident, rapid, and effective action with our foreign partners.

As the diversity of our foreign partnerships multiply, our command and control relationships will also change. Traditional concepts of unitary command and control will continue to be appropriate in single theaters of operation where authority and jurisdiction to operate and act unilaterally is clear. However, countering terrorists seeking to acquire or use WMD will often involve close cooperation and coordination with authorities that have principle jurisdiction or concurrent jurisdiction to take action against a particular threat. In such situations, the U.S. government's role will be to build up the capacity of our foreign partners to take on their own responsibilities and to provide appropriate operational and technical support to help stave off imminent attacks and mitigate their consequences. Some of these innovative multinational interagency operational concepts are currently under development by United States Joint Forces Command.

Developing the interagency partnerships capable of cooperating seamlessly with foreign partners may force us to change even further how we train and organize our personnel for service in the federal government. Might we not consider, as Chairman of the Joints Chiefs of Staff General Pace asked in 2004, whether we need a new law like Goldwater-Nichols to strengthen interagency and international collaboration? If 9/11 taught us one thing, it was that information sharing and collaboration among and between federal agencies is essential to disrupt today's agile and adaptable terrorist networks. However, information sharing works best when strong incentives for sharing exist, and developing those incentives may in turn demand governance reforms that so far departments and agencies have been unwilling or incapable of making themselves.

Partnership Capacity Building at the Provincial and Local Level

In stamping out WMD terrorist safe havens abroad, provincial and local governments must also play a critical role. Often the missing element for mission success is not additional financial resources, but rather the techniques and procedures to ensure effective operational cooperation between national governments and governments at the state, provincial, and local level. Here at home, we witnessed with Hurricane Katrina what can happen when a common understanding about the operational and support relationships between federal, state, and local authorities is lacking. A failure to develop common procedures and protocols for catastrophic WMD terrorist attacks will result in far more destructive consequences should an attack take place. Our capacity building efforts with foreign partners therefore must extend beyond the national level and highlight the importance of establishing effective mutual support networks between national, provincial and local authorities.

Shaping a New Relationship with the Private Sector

In an era where many of the principal threats are associated with non-state actors, governments worldwide are struggling to discern how they should relate to the private sector, including industry. Private sector organizations are eager to find practical ways to cooperate to minimize the risk of WMD terrorism, but they often lack an understanding of government priorities. Let me suggest three areas where we can strengthen cooperation between governments and the international private sector to mitigate the global risk of WMD terrorism.

1) *Catalyze the insurance industry as a risk mitigation partner*

Amidst growing budget constraints, the U.S. and other partner nations must find new ways to leverage existing economic resources to mitigate the risk of WMD terrorism. Since 9/11 policymakers and legislators alike have become more aware of the role that the global insurance industry, as well as the legal and regulatory architecture that shapes insurance markets, can play in mitigating WMD terrorism risk. The U.S. passed the Terrorism Risk Insurance Act to help support the development of an effective private market for mitigating and insuring against terrorism risk. While the development of insurance for WMD-related terrorist incidents is still in its nascent phases, it has become increasingly clear that actuarial science combined with computer-based simulations and modeling techniques can clarify the full range of risks that the chemical industry and their suppliers and partners face. Specialized risk assessment firms, along with the research arms of insurance brokerage firms, are enhancing the ability of insurance underwriters to price and transfer risk, which in turn, creates incentives for the private sector to avoid and actively mitigate high risk behavior.

2) Strengthen information sharing with the private sector

Most WMD terrorist attack scenarios will touch some element of the private sector before they intersect with the infrastructure or personnel of the national government. For example, the flow of financial resources to terrorist organizations moves through private financial institutions. The flow of WMD related materials will often flow through a privately operated port or airport. The movement of WMD-related terrorist plans may flow through cyber infrastructure controlled by private telecommunications companies and ISPs. We have already taken steps to strengthen information sharing with the private sector through regulatory regimes that encourage suspicious activity reporting. There are additional opportunities to strengthen partnerships to detect the movement of WMD materials and related resources flowing through the infrastructure of the private sector. Establishing algorithms for threat analysis that can be shared with the private sector as a best practice is one area where government and industry can strengthen our work together.

3) Develop voluntary best practices for the private sector

While in most countries regulatory action has traditionally played, and will likely continue to play, the lead role in influencing private sector behavior, voluntary public-private partnerships that shape the risk environment through market-based incentives can complement a regulatory approach. To take one example here in the United States, the chemical industry has already shown initiative to enhance the security of its infrastructure. For example, the American Chemistry Council (ACC) and the Synthetic Organic Chemical Manufacturer's Association have developed codes of conduct to guide the behavior of their members. The Responsible Care Security Code designed by the ACC outlines 13 practices that company security management systems must include. These practices require companies to assess vulnerability of their facilities, develop and implement plans to mitigate such vulnerabilities, and obtain third-party verification that the necessary security measures have been implemented. Such voluntary best practices offer private sector organizations an opportunity to take concrete steps to strengthen their reputations as reliable partners with government in combating catastrophic terrorism.

Conclusion

The President has made clear that terrorists seeking to acquire and use WMD are our most serious national security threat. To counter an elusive and adaptive adversary, we must transform ourselves and our partnerships to deter, detect, and defeat this growing threat to our country and to the peace and security of the international community.

And will the men and women of the long gray line respond to this challenge? I have no doubt, for here at West Point, we find men and women of character, of discipline for whom the words "duty, honor, and country" still carry with them a sacred trust. And as long as this Corps shall last, we will surely meet the test.

Released on November 30, 2006

 [BACK TO TOP](#)

Published by the U.S. Department of State Website at <http://www.state.gov> maintained by the Bureau of Public Affairs.