



Preventing Weapons of Mass Destruction (WMD) Terrorism in the Maritime Supply Chain

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

Remarks at Maritime Security Expo

New York, New York

September 20, 2006

Introduction

Five years after 9/11, who among us cannot remember where they were on that day? We harbor no illusions that those who attacked us five years ago cease to threaten us now. We have been assured by the same terrorists who planned the attacks on the World Trade Center and the Pentagon that they will use nuclear and biological weapons against us, should they find a way to acquire them. We also know that the enemy we face adapts to our defenses; while aircraft may have served as the preferred weapon of choice five years ago, tomorrow they may seek to slip a weapon of mass destruction into a container ship headed for one of our ports and then onto the streets of our cities.

Weapons of mass destruction (WMD) -- chemical, biological, radiological, and nuclear -- in the hands of a terrorist pose the single gravest threat to international peace and security today. The United States government is determined to work with its foreign partners, both in government and in the private sector, to strengthen our national and collective defenses against this preeminent threat.

Our Strategic Approach since 9/11

Since 9/11, the United States has taken a strategic and comprehensive approach to combating WMD and terrorism and protecting the maritime domain from these and other twenty-first century threats. Let me briefly summarize the elements of the various strategies that touch on these areas.

In 2002, the President announced the National Strategy to Combat Weapons of Mass Destruction, which established a comprehensive approach for preventing the world's most dangerous weapons from falling into the hands of the world's most dangerous actors. Our National Strategy to Combat Weapons of Mass Destruction establishes the following three pillars:

- Robust Counterproliferation Policies and Capabilities
- Strengthened Nonproliferation Measures
- WMD Consequence Management Preparedness

To integrate these pillars effectively, the strategy also called for strengthened intelligence capabilities, research and development, targeted strategies against proliferants, and enhanced international cooperation. It also emphasized the importance of bringing to bear all three pillars -- counterproliferation, nonproliferation, and consequence management -- against the WMD terrorist threat.

In 2005, the President announced the National Strategy for Maritime Security which outlined a strategic approach to protecting the maritime domain, including from the threats of both WMD and terrorism. This strategy set forth four strategic objectives:

- Prevent Terrorist Attacks and Criminal or Hostile Acts
- Protect Maritime-Related Population Centers and Critical Infrastructure
- Minimize Damage and Expedite Recovery
- Safeguard the Oceans and Their Resources

The National Strategy for Maritime Security specifically identifies the important connection with the National Strategy to Combat Weapons of Mass Destruction and outlines a vision for bringing together federal government maritime security programs and initiatives into a comprehensive approach involving all appropriate federal, state, local, and private sector entities. Equally important, it contains a strategy for cooperating and coordinating our efforts with key allies worldwide. Most recently, the President signed a new National Strategy to Combat Terrorism, which identifies the central importance of combating WMD terrorism by integrating our counterterrorism, counterproliferation, and nonproliferation tools to confront and defeat the nexus of WMD and terrorist actors. This new strategy emphasizes the following six areas as critical elements in a comprehensive approach to combating the WMD terrorist threat:

- 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
- Defining the nature and source of a terrorist-employed WMD device

The National Strategy to Combat Weapons of Mass Destruction, the National Strategy for Maritime Security, and the National Strategy to Combat Terrorism demonstrate the comprehensive approach the President has outlined to ensure that our government harness all elements of national power and that the United States works closely with allies and partners to protect and defend the maritime domain from today's most serious national and international security threats.

Turning Strategy into Capabilities

The United States government has not rested on strategy alone; it has taken numerous proactive steps to implement these new strategies, establishing new initiatives, programs, and partnerships to protect the global maritime supply chain from the threat of WMD terrorism. Let me cite just a few examples of the various initiatives the Department of State is working to advance.

The Department of Homeland Security's Customs and Border Protection (CBP) has taken a leadership role in protecting the global maritime supply chain through the Container Security Initiative (CSI), a program that places U.S. officers overseas to detect and inspect high risk containers in ports abroad. CBP has steadily expanded this program and has also established the Customs Trade Partnership Against Terrorism (C-TPAT), a public-private partnership that strengthens supply chain security practices among private sector actors. The Department of Energy has established the Megaports Initiative to install radiation detection equipment at foreign seaports to enhance host governments' capabilities to detect, deter, and interdict illicit trafficking in nuclear and other radioactive materials. The Megaports Initiative also works in close partnership with CBP to strengthen our ability to detect nuclear and radiological threats in global container traffic. And, more recently, the Department of Homeland Security's Domestic Nuclear Detection Office (DNDO), established in 2005 by National Security Presidential Directive, was charged with developing an effective global nuclear and radiological detection architecture to protect the homeland, an effort that offers an excellent opportunity to strengthen our partnerships with our friends and

allies abroad.

U.S. efforts to strengthen maritime supply chain security have extended beyond port security and radiation detection. In 2003, the President launched the Proliferation Security Initiative, or (PSI), to strengthen our capabilities to interdict shipments by land, air, and sea of WMD, related materials, and their delivery systems. The PSI now includes more than 75 nations and PSI participants have helped stop more than 30 high risk shipments, including centrifuge parts bound for Libya's nuclear program. That interdiction in cooperation with the U.K., Germany, and Italy helped lead Libya to make its historic decision to abandon its chemical and nuclear weapons programs and helped unravel and dismantle the A.Q. Khan network. The State Department has worked closely with a variety of federal agencies to advance the PSI. The Department of Defense has played an active leadership role in hosting and coordinating PSI Operational Experts Group exercises and developing new concepts of operation for interdicting WMD, including in the maritime domain.

Financial enforcement has also played a critical role in protecting the maritime supply chain from WMD and terrorist threats. The Department of State is working closely with the Treasury Department to deter, detect, and disrupt the financial flows that underpin trade in WMD and which can aid and abet terrorist and organized crime activities in the maritime supply chain. In support of these strategies, the United States has worked with a wide range of international partners, both government and private sector, to block the assets of entities engaged in illicit activities and highlight the risks they pose to the integrity of our international financial system upon which our global supply chain relies.

Reducing WMD Terrorism Risk through a Layered Defense-in-Depth

Defending the United States and our international partners from a covert nuclear or biological attack by terrorists presents many operational and technical challenges. Since we cannot afford to fail in this mission, we must embrace a strategic approach capable of reducing this risk to its absolute minimum. We also know that no matter how effective, no single capability can provide a fail-safe protection from a WMD terrorist attack.

To reduce our collective risk from WMD terrorism, we must develop with our partners a layered defense-in-depth. A layered defense, or defense-in-depth, is a strategic concept employed in a diverse range of security-related fields, from missile defense to cybersecurity. Its central premise, especially applicable to combating WMD terrorism, is that no single layer, or capability, can provide us with sufficient protection against a determined and adaptable terrorist adversary. However, a terrorist or a terrorist facilitator who has to overcome multiple defenses in the course of his attack plan is more likely to be detected or deterred, or to fail during the attempt.

An effective layered defense should focus not merely on preventing terrorists from linking up with those facilitators that would provide them with WMD and related enabling capabilities; it should also take active defensive measures to detect and disrupt existing linkages between terrorists and those that might facilitate a WMD attack. Working with our international partners will be essential to deploy and sustain a layered defense-in-depth against WMD terrorism, since terrorist plots and conspiracies have often involved multiple jurisdictions, with the terrorist attackers, weapons designers, transport agents, financiers, and other facilitators all operating in different countries.

The Global Initiative to Combat Nuclear Terrorism: Securing the Maritime Supply Chain from Nuclear and Radiological Threats

To confront the growing risk of nuclear terrorism, President Bush and President Putin announced together on July 15 of this year the Global Initiative to Combat Nuclear Terrorism, a new effort whose purpose is to bring together a growing network of like-minded partner nations to accelerate the development of partnership capacity to combat this threat in a determined and systematic fashion. The Global Initiative to Combat Nuclear Terrorism takes a strategic and comprehensive approach to combating all aspects of the nuclear terrorism challenge, from strengthening physical protection of nuclear material, to detecting and disrupting its movement by or to terrorists, to consequence management in the aftermath of a dirty-bomb or nuclear attack.

The first meeting of initial partner nations participating in this new initiative will take place this October, and both Presidents Bush and Putin have called for outreach to industry and the public to secure full implementation of the initiative's objectives. As the Global Initiative develops, we look forward to working more closely with many of you here today to strengthen our national and global capabilities to combat the most serious security threat we face today: a nuclear weapon in the hands of a terrorist.

Public-Private Partnerships: An Emerging Global Best Practice

In a post-Cold War era, as Secretary Rice has articulated, the gravest threats we face increasingly result not only from nation-states, but also from the activities of non-state actors, either terrorist, criminal, or groups otherwise engaged in destabilizing, transnational illicit activity. Our terrorist adversaries seek not only to kill innocent civilians, but they have also targeted our economic infrastructure with the goal of reducing our capacity and will to continue the fight. Since over 90% of global trade in goods is transported in containers through the maritime supply chain, ports and related infrastructure are an inviting target. We also know illicit non-state WMD traffickers, such as A.Q. Khan, have used the maritime supply chain to transport WMD materials and delivery systems, and the PSI is an important initiative that our government has taken to confront this threat.

Continuously strengthening our capabilities to confront and defeat terrorists and non-state actors operating in the seams of the global maritime supply chain and outside the rule of law will demand new and adaptive public-private partnerships. The partnerships must be capable of detecting illicit and terrorist activity at an earlier stage of development and enable governments to accelerate the appropriate enforcement response. As the work of many agencies has already shown, many public-private partnerships are already in place and have worked well. We must strengthen and extend these partnerships in new directions to deter, detect, and take confident and effective action against terrorists and non-state actors involved in the WMD trade. The private firms that own, operate, and insure ports and the shipping and logistics providers that work with them recognize that promoting best security practices across the global supply chain not only protects our national security, it protects their individual corporate reputations, enhances their bottom lines, and promotes our collective economic security. Public-private partnerships have in a short period of time become a new "best practice," benefiting both government and industry, and we invite private sector entities to consider new ways in which such partnerships can protect the maritime supply chain, and more broadly the global supply chain, from emerging 21st century threats.

Deploying Emerging Technologies to Reduce WMD Terrorism Risk

Reducing WMD terrorism risk in the maritime supply chain depends on more than just partnerships, strategic clarity, and bigger security budgets. It requires the research and development of new technologies, the application of those new technologies into tested systems, and the incorporation of those systems into innovative concepts of operation which interoperate seamlessly with the security capabilities of our trading partners abroad. So let me commend the many contractors, engineers, and suppliers here today who are working hard to translate security innovations in fields such as enterprise risk management, WMD detection systems, biometric identity verification tools, GPS location technology, RFID technologies, and wireless networking into holistic systems that governments and port operators can use on a daily basis to increase our situational awareness, reduce security risk, and keep our citizens safe from even the most adaptive adversaries we might face.

Let me also take a moment to emphasize the importance of researching, developing, and deploying technologies and systems that can facilitate the real-time sharing of information among and between international partners. If 9/11 taught us only one lesson, it was that connecting the dots among and between those involved in a terrorist plot requires agencies across our federal, state, and local governments to share information more rapidly and to enable confident action before terrorists can achieve their goals. As the recent terrorist attempt in the U.K. showed, averting the next attack against the United States or against one of our allies may well depend on our ability to share information in real-time not only within our own government, but also with our foreign partners, either in government or in the private sector. Securing the maritime supply chain in the 21st century will also depend to a large degree on our ability to identify threats and share that information rapidly with those domestic and foreign partners in a position to respond most effectively.

Meeting the Security Challenges of Globalization

We marvel today at the communications and transportation innovations of the last ten years, as well as the international legal and regulatory frameworks that have enabled what we commonly refer to as "globalization." We recognize that the maritime supply chain forms just one element of an increasingly seamless intermodal and

global supply chain. This global supply chain reaches well beyond the maritime domain and interconnects with land, air, cyber, and financial domains, weaving its way, often unnoticed, through our international, national, state, provincial, and local jurisdictions.

As this increasingly global and interdependent supply chain has come into form, governments have often played catch-up to ensure that terrorists, WMD traffickers, and others engaged in transnational illicit activity are denied access to this precious global resource on which our national and economic security increasingly depends. As we reflect on this challenge, let us remember that this resource will not secure itself; it will require energy and innovation to develop the transformational partnerships between governments and with the private sector to ensure that market-based incentives are aligned, best practices are rewarded, and protective measures are in place to deny bad actors access to both a target and a safe haven they have shown a clear intent to exploit. This conference, in this great city, is surely the place to build on and sustain this all-important work.

Released on September 27, 2006



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