



U.S. DEPARTMENT of STATE

KEYWORD SEARCH

[Subject Index](#)+ BOOKMARK    ...[Home](#)[Issues & Press](#)[Travel & Business](#)[Countries](#)[Youth & Education](#)[Careers](#)[About State](#)You are in: [Under Secretary for Arms Control and International Security](#) > [Bureau of International Security and Nonproliferation \(ISN\)](#) > [Releases](#)> [Remarks](#) > [2006](#)

Reducing Chemical Terrorism Risk: The Role of Public-Private Partnerships

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

Remarks at the Fourth Annual Toxic Industrial Chemicals (TICs)/Toxic Industrial Materials (TIMs) Symposium

Richmond, Virginia

July 12, 2006

Introduction

In 1995 the Japanese cult Aum Shinrikyo released sarin in the Tokyo subway leading to twelve deaths and several thousand injured civilians. Aum used just a single front company to purchase 180 tons of phosphorus trichloride, along with other toxic industrial chemicals, in its successful attempt to produce and release sarin. While this attack has largely faded from memory in the aftermath of 9/11, there are several reasons why the risk of chemical terrorism deserves the sustained attention of government officials and industry leaders worldwide. First, Al Qaeda has shown an interest in acquiring and using cyanide and other chemicals in terrorist attacks. Second, the widespread availability of toxic industrial chemicals increases the risk that terrorists may exploit them. Finally, with nuclear and biological terrorism receiving greater attention and resources from policymakers focused on the global challenge of weapons of mass destruction (WMD) terrorism, the risk of chemical terrorism, especially that involving toxic industrial chemicals, may suffer from comparative neglect.

Applying Our National Strategy

In 2002, the President approved the National Strategy to Combat Weapons of Mass Destruction, which outlined a comprehensive approach for combating the world's most dangerous weapons. The strategy set forth three pillars – nonproliferation, counterproliferation, and consequence management – and emphasized the importance of international cooperation, along with intelligence, research and development, and targeted strategies to securing our future. The National Strategy also stated:

One of the most difficult challenges we face is to prevent, deter, and defend against the acquisition and use of WMD by terrorist groups. The current and potential future linkages between terrorist groups and state sponsors of terrorism are particularly dangerous and require priority attention. 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.

Nonproliferation, counterproliferation, and consequence management efforts have all contributed to mitigating the risk of chemical terrorism. For example, the dismantlement of state chemical weapons programs through nonproliferation treaties, arrangements, and programs such as the Chemical Weapons Convention, the Australia Group, the Cooperative Threat Reduction Program, and the Nonproliferation and Disarmament Fund has helped to deny terrorists access to some of the world's most dangerous chemical weapons. Counterproliferation activities, such as the Proliferation Security Initiative, have also played a central role, by improving our ability to stop chemical shipments of concern. Consequence management preparedness activities carried out bilaterally or through multilateral entities such as NATO's Euro-Atlantic Disaster Response Coordination Center have contributed to mitigating chemical terrorism risk.

Despite these efforts, we must bear in mind that the distributed character of the toxic industrial chemical infrastructure presents special challenges that our traditional nonproliferation, counterproliferation, and consequence management efforts have not historically tackled. As we develop international partnerships and partnership capacity to mitigate these risks, a number of strategic principles should guide our efforts. First, we must improve our understanding of terrorist motivations and capabilities regarding the use of chemical weapons. Second, we must develop new approaches to denying terrorists access to toxic industrial chemical facilities, associated chemicals, or other capabilities they need to carry out chemical attacks. Third, we must tailor our deterrence strategies to counter terrorists and those who might facilitate a chemical attack. Fourth, we must detect and disrupt the flow to terrorists of toxic industrial chemicals, funds, and other resources necessary to carry out a chemical attack. Finally, we must take measures to strengthen our crisis operations capabilities should an attack be imminent, and in the event of a chemical release, take measures to manage the consequences, as well as call on next generation forensic and investigative techniques. Taken together, these principles offer a focused and robust strategy for combating chemical terrorism on a global basis.

The Threat in Brief

Toxic industrial chemicals could offer an attractive weapon of mass destruction to terrorists. Some of the earliest chemical weapons, such as chlorine and phosgene, are toxic industrial chemicals whose use led to almost 100,000 deaths during World War I. The large number of toxic industrial chemical facilities around the world could make such chemicals a weapon of choice for terrorists seeking to acquire a simple, cheap, and effective WMD. Open source information readily available on the Internet could guide a terrorist seeking to develop a more sophisticated chemical weapon by using toxic industrial chemicals. Along with Aum Shinrikyo, Al Qaeda has shown an interest in acquiring, developing, and deploying chemical weapons against innocent civilians.

Managing Risk: Threat, Vulnerability, and Consequences

In a widely noted speech to the American Chemistry Council, Secretary of Homeland Security Chertoff highlighted the importance of risk management as the essential framework for effectively combating chemical terrorism. He pointed out that a comprehensive risk management approach demands not only a focus on the threat – the intent and capabilities of our terrorist adversaries, but also on the vulnerability of targets to acts of chemical terrorism, as well as the consequences of attacks against such locations.

The vulnerability and consequences related to a particular target depend to a large degree on the countermeasures that have been taken to protect it, its proximity to urban areas, and the effect of an attack on economic assets of significance. In the United States and abroad, there are a large number of chemical facilities in and around urban areas where sabotage attacks would likely result in mass destruction. Homeland security experts have estimated that attacks on some of the more dangerous facilities could result in thousands of deaths. Although there was no conclusive evidence of sabotage or terrorist involvement, the chemical incident that afflicted Bhopal, India in 1984, provides us some sense for the scale of damage likely in a major terrorist attack on a chemical facility. In that case, 30-40 tons of highly toxic methyl isocyanate gas were released into the atmosphere resulting in 6,000 deaths.

Building a Defense-in-Depth

A systematic approach to chemical terrorism risk mitigation builds on the premise that no single capability or defense can provide a fail-safe approach against terrorists seeking to acquire and use chemical weapons. Instead of focusing on the single "silver bullet", we must develop a "layered" defense-in-depth with our international public and private sector partners to optimize our collective and individual risk reduction efforts.

A defense-in-depth applies across multiple domain areas. For example, we must employ defense-in-depth concepts in the geospatial domain involving air, land, and maritime elements. We must also employ defense-in-depth concepts against ungoverned virtual spaces that terrorists might exploit to acquire resources and plan for attacks. Today, there is a special urgency to detect and block the financing and communications regarding attack plans that may be occurring in cyberspace. Finally, a defense-in-depth approach should address capabilities across the time domain, from the moment a specific terrorist threat is recognized until the post-attack consequence management and criminal justice phase. An effective defense-in-depth will result in that mix of capabilities and defenses across all domains that can achieve maximum risk reduction.

Public-Private Partnerships

The substantial majority of chemical infrastructure worldwide is owned by the private sector. As such, the private sector can and should play a central role in enabling a defense-in-depth and mitigating the risk of chemical terrorism worldwide. 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.

The chemical industry has already shown initiative to enhance the security of its infrastructure. For example, the American Chemistry Council and the Synthetic Organic Chemical Manufacturer's Association have developed codes of conduct to guide the behavior of their members. The American Chemistry Council (ACC) designed the Responsible Care Security Code that 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. ACC reported that as of May 2004, all of its 2,000 facilities have completed security vulnerability assessments at their sites using the Sandia National Laboratories vulnerability assessment methodology, the Center for Chemical Process Safety methodology, or an equivalent methodology approved by the center. Recognizing the thoroughness of this code, the United States Coast Guard has declared that implementation of this code is an acceptable alternative security program that can be utilized in order to fulfill the facility security requirements prescribed by the Maritime Transportation Security Act.

Private sector-led risk mitigation efforts are not only underway in the United States but also abroad. In Europe, the International Chemical Environment- European Emergency Response Network, a voluntary initiative that specifically pertains to the transport of chemicals, provides emergency response and consequence management assistance. In the event of a chemical terrorism incident, industry participants will share information and, if necessary, provide equipment to the appropriate emergency authorities.

A Role for the Insurance Industry

Public-private partnerships to mitigate chemical terrorism risk should not begin and end with the chemical industry. 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 chemical 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, leads to incentives to avoid high risk behavior.

In addition to enhanced private sector risk assessment tools and capabilities, innovation through the application of concepts such as mandatory coverage availability, damage caps, compulsory insurance for inherently risky activities, and terrorism risk insurance bonds could help to create the right market-based framework for private sector chemical terrorism risk management. These efforts, along with those taken to strengthen national legal and regulatory frameworks by international organizations such as the International Maritime Organization or the International Civil Aviation Organization can help to strengthen risk management, as we seek to reduce the risks of transporting toxic industrial chemicals throughout the global supply chain.

Mitigating Indirect Risk

Public-private partnerships can also play a central role in mitigating indirect risks of chemical terrorism. Indirect risks can be classified as those risks that affect a location or an enterprise whose infrastructure may be exploited during the planning or carrying out of a chemical terrorist attack. For example, a logistics provider that unwittingly provides chemical transport services may face liability for transporting chemicals to actors whose backgrounds they should have more thoroughly researched. Financial intermediaries that provide funds to front companies moving or transporting chemical weapons to terrorist organizations will face substantial reputational risk, if not liability risk.

A central challenge facing private sector risk managers and security professionals lies in modeling such indirect risks, particularly as they pertain to liability. These risks present modeling challenges since courts are still in the process of defining the contours of enterprise liability related to the facilitation of acts of terrorism. Most notably, the Arab Bank is currently defending itself in United States (U.S.) District Court from charges that it facilitated terrorist activities in the Middle East by managing financial accounts whose beneficiaries included the widows of suicide bombers.

Building a partnership between law enforcement and the private sector abroad also requires priority attention. In recent years, the U. S. has strengthened its suspicious activity reporting guidelines at the federal level for a range of industries, including financial services and nuclear utilities. Private sector initiative can support such national government efforts. For example, Internet service providers (ISPs) can help to detect plans developed in cyberspace that involve sabotage attacks against chemical facilities and pass such information on to law enforcement for appropriate action.

Catalyzing a Virtuous Circle

The terrorist attacks of the last five years have shown the adaptability of today's terrorists and those that provide them aid. Our international approach to WMD terrorism risk management must be equally adaptable. The task facing policymakers, regulators, and lawmakers alike is to shape the powerful economic and technological forces driving globalization to ensure that private sector entities that maintain leading WMD terrorism risk management practices gain a competitive advantage over those that do not, and those entities that continuously improve their risk management practices over time widen their advantage over their competitors. Where legal and regulatory frameworks have failed to catalyze this virtuous circle, we must adapt our frameworks, our tools, and our public-private partnerships to the emerging threats and risks at hand.

Released on July 28, 2006



[Updates](#) | [Frequent Questions](#) | [Contact Us](#) | [Email this Page](#) | [Subject Index](#) | [Search](#)

The Office of Electronic Information, Bureau of Public Affairs, manages this site as a portal for information from the U.S. State Department. External links to other Internet sites should not be construed as an endorsement of the views or privacy policies contained therein.

[About state.gov](#) | [Privacy Notice](#) | [FOIA](#) | [Copyright Information](#) | [Other U.S. Government Information](#)