
Ecoterror: Rethinking Environmental Security after September 11

Michael J. Penders and William L. Thomas

Among the more chilling stories to emerge after September 11, 2001, is that of Danny Whitener, a Tennessee salvage-car dealer. According to Whitener, a man calling himself "Mo" landed his small plane at Copperhill airport in March 2001 and began asking questions about a nearby chemical plant. As Whitener recounted to federal investigators, the stranger wanted to know "What kind of chemicals are in those massive storage tanks?" Whitener informed the pilot he thought the tanks were empty. The tanks actually contained as much as 250 tons of sulfur dioxide, an amount that if released would be sufficient to harm as many as 60,000 people, according to worst-case estimates developed by the plant. Whitener and at least two other witnesses believe the stranger in Tennessee that day was none other than Mohamed Atta, a key suspect in the strikes that felled the World Trade Center.

The attacks of September 11, coupled with subsequent anthrax incidents, have deeply undermined America's sense of security. The threat of a terrorist group using chemical, biological, and nuclear weapons now seems far less remote than it did before, as does the prospect of an act of sabotage at a major industrial facility. The events of the last few months and President Bush's declaration of a war on terror have fundamentally altered the risk calculus, resulting in a reexamination of our safety against such threats. The newly created Office of Homeland Security will focus attention on this area, as will Congress, as evidenced by legislation such as the Chemical Security Act of 2001, S.1602, introduced in the Senate. State antiterrorism legislation has also been introduced placing new restrictions on hazardous materials transportation. The sense of danger is acute.

Much has been written in recent years on the theme of environmental security. The Millennium Project of the American Council for the United Nations University captured the essence of the idea in the following definition: "Environmental security is the relative safety from environmental dangers caused by

natural or human processes due to ignorance, accident, mismanagement or design and originating within or across national borders." *Environmental Security Study: Emerging International Definitions, Perceptions, and Policy Considerations* (Sept. 1998). In the wake of September 11, efforts to foster environmental security must be enhanced to adequately address risks from biological, chemical, and nuclear materials, and those individuals and groups who would use them as weapons of mass destruction and terror. Addressing these risks in an era of global commerce and freer and faster trade requires better international frameworks for systematic integration of information among law enforcement agencies, customs services, environmental regulatory agencies, trade agencies, and intelligence sources. Nations must improve their capabilities to share and analyze such data across borders, using new information technologies to detect shipments of agents that may be precursors to acts of terrorism or environmental crime.

The events of September 11 have also altered the context of the debate over environmental policy reform, bringing security into the dialogue about sound law, regulation, and business management. New legislation has been introduced on every level of government that would superimpose new security measures on the construct of existing environmental laws. The imperative to implement environmental security measures for industry and infrastructure provides a new lens through which to consider "next generation" environmental legislation, with an emphasis on facilitating the widespread deployment of more strategic and efficient approaches to minimize environmental risks.

Even with advances in environmental management systems over the last several years, few facilities have carefully integrated security monitoring and defenses into such frameworks, or adequately addressed risks of sabotage from outside or inside the organization. Despite advances in technologies for security systems, most companies fail to adequately address threats from chemical or biological agents. The search for safety from a newly apparent array of threats, at home and from abroad, has created new incentives for sustainable and secure environmental management practices. This article explores the dangers posed by terrorist groups seeking to further political, military, or religious objectives through environmental harm, the implications of

Mr. Penders is president and chief executive officer of Environmental Protection International, in Washington, D.C. He may be reached at mpenders@epinetwork.com. Mr. Thomas is a senior attorney in the Washington, D.C., office of Pillsbury Winthrop LLP, and chair of the Section's Committee on International Environmental Law. He may be reached at wthomas@pillsburywinthrop.com.

this threat for policymakers and corporate decision-makers, and efforts that can be undertaken to improve environmental security.

Weapons of Green Destruction

Acts of terror involving biological or chemical agents and other weapons of mass destruction are not new. As with the poisoning of kings in ancient times, such techniques have historically allowed small groups or individuals to attack those in power without confronting their armies directly. Nor is the threat of biological warfare unknown in America. In 1777, British Major Robert Donkin “proposed to shoot against the Americans arrows dipped in the matter of the small pox, and so conquer them by their known terror of that disorder.” Only relatively recently, however, have technological developments made it possible to produce and deliver these agents to cause catastrophic harm. It would be imprudent to think that minds that conceived of using a passenger airplane as a weapon of mass destruction would hesitate to use ecoterror for a similar purpose. Indeed, *The Washington Post* reports soldiers found copies of U.S. chemical trade publications in an Afghanistan hideout formerly occupied by Osama bin Laden.

Yet Al Qaeda is not the only group that poses a potential threat to U.S. environmental security. Any one of dozens of aggressive movements espousing varieties of nationalism, fascism, or apocalyptic religious or ideological zeal could mount such an attack. It need not even be a group. As Thomas Friedman explains in *The Lexus and the Olive Tree*, during the post Cold War era a single “Super-Empowered Angry Man, or Woman, can use the powers embedded in globalization to attack even a superpower.” Farrar, Straus & Giroux, May 2000, at 322. The ecoterrorist seeks to turn the forces of nature to a hostile purpose either by targeting the environment itself (e.g., by contaminating a public drinking water supply) or by using it as a means to bring about loss of life and property (e.g., by destroying a dam and releasing a large river).

As a recent report for the Pacific Institute notes, the threat of ecoterror can take many shapes. See Elizabeth Chalecki, *A New Vigilance: Identifying and Reducing the Risks of Environmental Terrorism* (Sept. 2001) (available at www.pacinst.org/environmental_terrorism_final.pdf). Hundreds have died in Nigeria, for example, as a result of acts of sabotage and theft directed either at oil production and refinery operations or

pipelines. There were seventy-seven separate bombings in Columbia alone during 1998, including an explosion at the country’s central oil pipeline that killed seventy-one people. The operation’s commander subsequently announced that he would continue to target the nation’s oil infrastructure to prevent foreign “looting” of Columbia’s wealth. The 1995 nerve gas attack on a crowded Tokyo subway station by the Japanese millenarian cult Aum Shinrikyo killed a dozen people, injured scores of others, and illustrated the particular vulnerabilities of cities, with their infrastructure and population density, to chemical and biological attacks. In December 2001, the Washington D.C. Metro System announced it had deployed sensors to detect chemical agents in response to such threats, including a scare in October in which a man doused passengers with what he claimed was a toxic chemical agent. It turned out to be a relatively benign substance, but the time it took to make that determination, coordination problems with the emergency response, and the crippling impact to the system demonstrated to officials

the need to deploy new technologies to detect and analyze threats accurately and quickly.

Threats such as these have long been recognized and had become an increasingly prominent component of national security strategies and diplomatic efforts in the 1990s. Still, prior to September 11, the federal government remained organized primarily around Cold War era challenges. International efforts to provide security from chemical, biological, and nuclear weapons through treaties largely assumed national control of these agents. While the effect of the international agreements on security among nations can be debated, and the ability to monitor the compliance of nations

remains a serious concern, it is clear these agreements have had little impact on smaller groups of organized criminals or terrorists. In fact, rogue nations may support these groups clandestinely rather than produce chemical or biological weapons in ways that can be easily identified with the governments.

Political and industry leaders in the United States must also grapple with the growing aggression of radical environmental and animal rights groups. The Earth Liberation Front, the Animal Liberation Front (ALF), and other zealous organizations are increasingly resorting to intimidation and violence to force environmental change, by targeting loggers, ski resorts, university research centers, and numerous other entities. These organizations, using tactics ranging from protest demonstrations to use of explosives to accomplish their aims, have caused more than \$40 million in prop-

Recent technological developments have made it possible to produce and deliver agents to cause catastrophic harm.

erty damage since 1980. Their efforts, which have grown increasingly violent over the last few years, have not diminished since September 11. In fact, just nine days after the World Trade Center fell, ALF set fire to a maintenance building at a primate research facility in New Mexico. Countering the threat of ecoterror in its various manifestations will require the coordination of policy- and decision-making, as well as information- and intelligence-sharing by an array of actors, including international organizations, nongovernmental organizations, corporations, and governments (including military, civilian, and intelligence elements).

Prevention and Deterrence

Over the last decade, as environmental issues attained greater significance in U.S. security policy design, the capacity of various agencies to implement such policies lagged behind. The late 1990s witnessed a proliferation of initiatives regulating the international traffic of hazardous substances, but rarely were the mechanisms or resources provided to effectively implement policies across different agencies with overlapping jurisdiction.

Many of the initiatives urged ratification of various conventions and called for “increased cooperation in fighting trans-boundary environmental crime.” This latter point reflected a growing recognition that the treaties themselves had little or no impact on actual environmental security, unless the related multilateral environmental agreement (MEA) was adequately implemented in law, and the capacity to enforce across national borders was established. As the United Kingdom’s Secretary of State for the Environment John Gummer put it: “These Conventions are worthless words on paper, unless their provisions are enforced in practice.”

The efforts undertaken to address the black market that emerged in Ozone Depleting Substances (ODS) in the 1990s are relevant here. The Montreal Protocol banned the most harmful ODS in developed countries in the early 1990s, but permitted the use of existing stockpiles and allowed developing nations an additional five to ten years to phase out these same chemicals. After the phase out of chloroflourocarbons (CFCs) as ODS under the 1990 Clean Air Act Amendments, an enormous black market emerged for smuggling prohibited CFCs into the U.S. from countries still permitted to manufacture and use them. Once in the U.S. illegally, these CFCs were virtually indistinguishable from existing stockpiles that were permitted until depleted. In 1995, one could purchase a container of refrigerant in Mexico for \$2, and sell it in Texas for \$20.

In fact, illegal trafficking in ODS was second only to narcotic trafficking during periods in the 1990s. After the U.S. Customs Service (Customs), EPA, IRS, the Department of Justice, and other agencies began working together to identify illegal shipments, thousands of tons of CFCs were seized in U.S. ports, originating from Russia, China, and India. U.S. chemical companies assisted by providing information, machines, and pressure gauges which could be used to identify prohibited forms of ODS. This cooperation stemmed in part from the fact that industry had spent hundreds of millions of dollars in developing the alternatives to CFCs—and its market was being crippled by illegal imports.

The multi-agency initiative involved bringing together Customs agents with their automated customs and trade data; EPA agents and data from EPA’s Office of Air and Radiation regarding the notification and controls of lawful shipments of ODS under the Montreal Protocol; IRS agents and their tax information on such shipments and receiving facilities; the FBI; and prosecutors from various U.S. Attorneys’ offices and DOJ’s Environmental Crime Section. Ultimately, the initiative involved foreign governments and international organizations such as the

World Bank, with its data on the allowable production of ODS by facilities around the world. Dozens of prosecutions, hundreds of years’ imprisonment, and hundreds of millions in fines resulted from this coordinated effort that became known as the National CFC Initiative.

By the late 1990s, the successful prosecution of CFC smugglers in the U.S. was recognized internationally as a model for how law enforcement agencies, regulators, international organizations, and corporations could work together to enforce national laws that implemented international environmental agreements. The Na-

tional CFC Initiative identified the type of compliance information, trade data, and various law enforcement information that must be collected in a systematic way to detect illegal shipments of chemical, explosives, and other goods in international commerce that may be precursors to acts of terrorism, or international environmental crime that threaten national security. The success of the National CFC Initiative in the U.S., however, was the exception, not the rule. Few countries have developed the capacity to detect violations of these laws at all. Even in the U.S., how many CFCs got through for every illegal shipment detected is unknown.

Better mechanisms are needed for sharing data within and among nations as a prerequisite for meaningful enforcement of laws governing international commerce in regulated substances. There has been some progress and useful models developed in recent

*Illegal CFCs were
indistinguishable from
existing stockpiles
that were permitted
until depleted.*

years. In 1999, the so-called G8 Nations (the United States, Canada, France, Germany, Italy, Japan, United Kingdom, and Russia) initiated a law enforcement project on international environmental crime estimated at that time to exceed \$5 billion a year in illegal trafficking in chemicals, hazardous wastes, and other regulated substances. The G8 Nations' Lyon Group Project on International Environmental Crime was launched to improve information exchange, data analysis, and cooperation among law enforcement agencies, international organizations such as Interpol, the World Customs Organization, and the Secretariats of the multilateral environmental agreements, as well as environmental and trade regulators. G8 Nations' Project participants collaborated in the use of new technologies, as well as information and intelligence exchange to detect international environmental crime. Specifically, they agreed to adopt tools such as the Internet-based communication system established between the ports of Rotterdam and Hong Kong that transmits pictures of suspect containers with their ID numbers to the receiving port. Perhaps most relevant was the agreement to pursue analysis of compliance data and other information across nations, and the various regulatory and law enforcement agencies in those nations, to detect shipments that violate environmental or other laws administered by regulatory agencies. EPA's Center for Strategic Environmental Enforcement designed an international environmental crime and intelligence system to provide the U.S. and participating nations' law enforcement agencies access to compliance data and law enforcement information over secure Internet connections regarding a specific shipment or exporter, importer, receiving facility, or other entity or individual involved in a suspect shipment. Compiling such information on a broader scale, and enabling its comparison to Customs, trade, and commercial data before a shipment clears Customs, is one key to enhancing national security by preventing illegal import of hazardous substances, and identifying organized criminal and terrorist groups associated with some of these shipments.

Knowledge-Sharing Is Power

Better communication between federal, state, and local authorities will be critical to reducing the threat of ecoterror. That much is clear from the testimony of Baltimore Mayor Martin O'Malley, who recently explained to Congress how an unwary Maryland trooper

let an international terrorist slip through his fingers: "The CIA had him on a watch list, the FBI didn't, and no information was shared with state or local law enforcement." The motorist would a few days later hijack the jetliner that crashed into the Pentagon. We possess the technology to enable local law enforcement to identify drivers that have outstanding tickets, warrants, and matters pending in other jurisdictions. We have yet, however, to adequately coordinate information flow at the federal level, and internationally among relevant agencies, so that the law enforcement agency best positioned to counter the threat can do so.

The challenges of coordinating different law enforcement agencies and integrating information among them have long been recognized but difficult to surmount absent a task force approach in a high-priority case or initiative or without a galvanizing event such as September 11. For example, in May 2000, the President's Interagency Commission on Crime and Security in U.S. Seaports (PICCS) urged greater coordination of

*We have yet to
adequately coordinate
information flow at the
federal level, and
internationally among
relevant agencies.*

all federal, state, and local law enforcement agencies with significant regulatory and enforcement missions. PICCS' first recommendation was to strengthen interagency, intergovernmental, and public/private-sector efforts to address the threats of seaport crime (including terrorism), and to enhance control of imports and exports. The 361 public seaports in the U.S. are among the most vulnerable components of the international and intermodal trade system. With billions of tons of cargo coming through ports every year, and the smuggling of contraband and illegal aliens that may be connected to terrorism, PICCS' finding that the state of security in U.S. seaports generally ranges from poor to fair is not comforting.

Ports are vulnerable targets because of the exponential growth of trade over the last twenty years, the nature of modern container shipments, and the failure of inspection and control resources and technologies to keep pace. Economic globalization has compressed reaction time for law enforcement and has blurred national borders. Most import crimes go undetected at ports because less than 2 percent of cargo imported into the U.S. is inspected. This includes illegal transport of precursor chemicals, hazardous materials, drugs, munitions, and potential weapons of mass destruction. Less than 1 percent of export cargo is inspected. With different law enforcement and regulatory agencies, each with their disparate data collection and dissemination systems designed for their administrative functions, there is too little integration across functions to

allow for a central assessment of illegal imports that may pose a threat.

Although reports like the Seaport Crime and Security study have identified these issues in recent years, little has been done to implement recommendations in a serious and comprehensive way across and within various levels of government. Indeed, agencies already spread thin to address their core functions are often reluctant to devote their resources to an interagency process, particularly where other agencies have overlapping jurisdiction and when an investment in new information technologies may be required. However, technology widely used in the private sector and for military purposes is available to compile relevant information across agencies and nations to better determine threats as they cross national borders. It is imperative that agencies and international organizations that have designed and are administering regulatory processes, or are developing new ones, structure them to take full advantage of these tools, especially electronic reporting, and design their administrative processes to be compatible with other agencies' information systems, particularly customs automated data systems.

Some agencies, such as EPA, have not fully implemented electronic reporting and recordkeeping, which is the most effective way to facilitate comparison with customs data and other agencies' law enforcement information to detect illegal imports. Efforts to implement bar-coded electronic manifests, and to render compliance data in secure and harmonized electronic form will improve the ability of law enforcement to detect and track illegal shipments and other violations of international agreements. If trucking and shipping lines can track their cargo using global information systems, and grocery stores can track their inventory using bar codes and electronic systems, governments should also be capable of using the same technology to detect and track shipments that pose threats to national security.

The National CFC Initiative, the G8 Nations' Lyon Group Project on Environmental Crime, and other international task forces provide models for how agencies can synthesize critical information and use new technologies to do so. To be effective on a broader scale, however, building blocks must be put in place to facilitate the communication required between federal agencies and among nations that trade as well. New international agreements designed to provide international environmental security from the most harmful chemicals and other risks must keep pace with both methods of automated trade, and those who seek to gain illicit profits or to commit acts of terror.

Unless law enforcement agencies at international borders have systematic access to regulatory information about shipments before they clear Customs, nations cannot realistically expect to achieve widespread compliance with international agreements designed to control the trade in hazardous substances, including those that may be used as weapons of mass destruction. Yet many international agreements, such as the Basel Convention on the Control of Transboundary Movement of Hazardous Wastes and their Disposal, still rely on the environmental agency from the exporting nation faxing notification and consent forms to the environmental agency of the importing nation, with no direct connection to customs agencies and their largely automated data systems for tracking trade. Moreover, the regulatory classification systems for hazardous wastes, chemicals, and pesticides bear little resemblance to the tariff codes and other nomenclature used by customs services to track goods in international commerce. These are among the obstacles that have made certain international agreements notoriously difficult to enforce.

New environmental agreements, and revisions to existing ones, must facilitate the exchange of compatible data between regulatory agencies and customs services, through electronic reporting harmonized with the automated data processes governing international trade and customs' clearance processes. Negotiators of recent agreements have considered the problems of detecting illegal traffic, but whether nations implement measures enabling them to detect violations of international trade agreements remains to be seen. For example, at the October 2000 meeting of the Intergovernmental Forum

on Chemical Safety, the forum accepted several proposals aimed at the prevention of illegal international traffic in toxic and dangerous products, including proposals urging mechanisms for the integration of compliance information with customs data, and law enforcement intelligence. Unless nations implement administrative notification and consent regimes using electronic reporting with Internet connection to customs trade data and inspection and control functions, an opportunity will be lost to use the best available technologies to provide a greater measure of international environmental security.

Trade agreements and customs agreements that implement technical exchange of information between nations provide other avenues for the data integration required to better assure compliance with international environmental agreements. While trade agree-

*Some agencies
have not fully
implemented electronic
reporting and
recordkeeping.*

ments have become increasingly sophisticated in their use of technologies, and customs electronic data systems have facilitated faster trade with expedited clearance processes, trade agreements do not adequately interface with statutes that implement most environmental agreements. With increased international trade and relatively fewer opportunities for meaningful inspection, it is increasingly critical that the framework for data exchange imbedded in trade agreements, such as the Free Trade Agreement of the Americas, facilitate a link with the environmental compliance data necessary to determine whether a shipment is legal, or may pose a threat.

Countermeasures and Ecodefense

Better integration and management of data from different sources is not only a key to improving national security, but also applies to safeguarding industrial facilities and infrastructure. As Frederick Webber, president of the American Chemistry Council (ACC), stated in testimony before the U.S. Senate on the proposed Chemical Security Act of 2001, "Knowledge is security. The cornerstone of effective security is intelligence about potential threats that allows the threat to be intercepted and allows the target of the threat to be properly prepared. In fact, knowledge is our best defense." He added: "After September 11, everyone began to revisit potential threat scenarios. Our estimations of the probability of a worst-case scenario have changed, and we are moving rapidly to prepare for these new potential threats." *Testimony Before Senate Environment and Public Works Committee, Subcommittee on Superfund, Toxics, Risk, and Waste Management* (Nov. 14, 2001). Noting that the chemicals industry "is moving aggressively to establish better information sharing mechanisms with federal, state, and local officials," he called for more action by the Office of Homeland Security in this area.

Potential sabotage of chemical facilities or petroleum refineries raises a host of frightening scenarios. According to EPA, numerous plants located in the U.S. each maintain amounts of toxic chemicals that, if released, could endanger more than 1 million people. The submissions required under the Clean Air Act's Risk Management Program describe a host of evils that could occur in the event of an explosion or significant toxic chemical release. Recognizing these risks and the need for stricter discipline in the wake of September 11, the ACC, the American Petroleum Institute, the Fer-

tilizer Institute, and other industry groups have urged member companies to undertake a range of actions to increase security. Even they concede, however, that more can and should be done to enhance security further. One key to this effort will be the Department of Justice's assessment of the vulnerability of chemical plants and transported chemicals, now more than a year overdue. This assessment should be adequately funded, comprehensively executed, and released as soon as possible so that policymakers and corporations can benefit from its insights and recommendations.

Since September 11, many facilities have reviewed both their security and environmental management practices to ensure a higher level of safety against acts of ecoterror. In October 2001, for example, the ACC published guidelines calling for centralization of receiving operations, increased surveillance and number of security guards, enhanced access controls, movement of rail tank cars within the fence-line, and restrictions on the use of employee vehicles. In addition to such measures, companies should reassess their crisis management, response, and evacuation plans, and review their overall environmental management approach.

Many companies are becoming adept at using strategic environmental management tools to minimize risks and liabilities. Less widely recognized, however, is the fact that the elements of environmental management systems (EMS) designed to assure compliance with law, minimize or eliminate the use of the most hazardous substances and wastes, reduce emissions and releases, and improve process efficiencies can also be important from a security perspective. In recent years, as part of their EMS and information management systems, some facilities have deployed innovative technologies, electronic commerce techniques, remote sensing, and integrated monitoring for compliance and security concerns using secure

Many companies are becoming adept at using strategic environmental management tools to minimize risks and liabilities.

Internet-based systems. In addition to achieving new levels of environmental security, such facilities have realized cost and natural resource savings.

For example, NASA's White Sands Test Facility developed a facilitywide monitoring and reporting system under Project XL pursuant to an agreement with the State of New Mexico and EPA which allows the facility to report electronically, saving thousands of dollars every cycle. At the same time, electronic reporting and central monitoring within the facility has made internal information readily available to managers and regulators. The White Sands facility is moving toward website and Internet posting of its environmental compliance

monitoring reports, including using three-dimensional, digital mapping of the facility, its sources, and releases. Ready access to this information provides a greater level of security by facilitating quicker notice of compliance and or other problems that may pose a risk to the facility or community at large.

Security concerns that access to certain facility information over the Internet may provide a roadmap to terrorists had been raised well before September 11 and resulted in restrictions on such information. Additional restrictions and security measures for information that may be useful for terrorists have been proposed. While the disclosure of information may create difficult trade-offs between the public's right to know and its need for safety against terrorist threats, that debate is largely beyond the scope of this article and should not obscure the fact that secure and integrated information systems are the most effective tools for facility managers and government responders to detect threats, minimize impacts, and deter attacks. Defenses and encryption technologies for electronic information systems, such as those used by the military for weapon systems, are now widely available for use in the private sector. These defenses are important in preventing unauthorized access to sensitive information and computer hacker attacks that may pose direct threats to a facility and the surrounding community.

To minimize risks from attacks and the management of explosives and toxic chemicals, some military bases have adopted sophisticated Environmental Management Information Systems (EMIS), incorporating multi-layered defenses and encryption technologies. In addition to tracking environmental compliance, these systems monitor for minute amounts of biological and chemical agents upstream of the facility, screen for changes in meteorological conditions, and detect off-site releases using remote and wireless devices, accessible from the secure web-based control center. In one instance last year, a fa-

cility saved 400,000 gallons of water a day due to the efficiencies realized by moving to such a system. Another facility, by moving to electronic commerce and "just in time" delivery of particularly toxic chemicals, was able to eliminate an on-site chemical storage warehouse, and avoid RCRA Subpart B permitting.

Some of the same techniques that leading companies have come to deploy for sound environmental management purposes may be brought to bear at other facilities to achieve greater security and efficiency as part of an environmental management and security system (EMSS). Facilities seeking to minimize risks from acts of terrorism and other threats should evaluate their traditional security operations and their environmental management practices. A security audit, terrorism threat assessment, and environmental management gap analysis may reveal vulnerabilities that can be addressed through a range of countermeasures. Advances in communications technologies and remote sensing over the last decade offer new ways to monitor and integrate information relevant to detecting a greater array of risks than ever before. These tools allow environmental managers to identify threats, respond quickly, and minimize harm.

U.S. antiterror and environmental laws and international environmental treaties cannot guaranty protection against ecoterrorism. Even if precautions such as those proposed under the Chemical Security Act (S. 1602) or the Agricultural Terrorism Prevention and Response Act (H.R. 3198) are taken, authorities cannot monitor the full array of potential threats to U.S. security from environmental terrorists. Governmental security efforts must be supplemented by deterrence and defensive strategies. Many of the most effective countermeasures will be deployed at the local or facility level. Improving surveillance and information exchange systems and integrating security with EMS will enhance detection, increase safety and, it is hoped, reduce any damages should such a threat materialize. 