Container Security: Preventing a Nuclear Catastrophe

Todd Konkel

Edmund A. Walsh School of Foreign Service, Georgetown University

Leslie Comstock Editor

Disclaimer:

This paper is intended for discussion and should not be cited without author's permission! If you would like to cite it, please email: IPS_Board@irpsmail.ucsd.edu

I. Introduction

In the immediate aftermath of the September 11, 2001 attacks, the U.S. government passed a significant number of measures to improve aviation security – an area with a high level of public visibility. This nation faces a potentially greater threat, however, from a weapon of mass destruction (WMD) making its way into the U.S. in one of the thousands of cargo containers that enter this country every day. In June 2004, the House Subcommittee on Coast Guard and Maritime Transportation issued a memo reflecting this view: "Despite the importance of seaport security, perhaps no other mode of transportation is currently more vulnerable to future attacks than our Nation's Marine Transportation System."[1]

Although a future attack involving a chemical or biological WMD could have tragic consequences, a nuclear weapon, which could cause hundreds of thousands of deaths in an instant, presents the most concerning threat. In *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, Harvard professor Graham Allison shares a brief but revealing excerpt from a private conversation that took place with former Secretary of Homeland Security Tom Ridge in February 2004. When asked what worried him most, Secretary Ridge replied with a single word: "nuclear."[2] Later in his book, Allison states that a nuclear weapon used by terrorists in an attack on the United States "is far more likely to arrive in a cargo container than on the tip of a missile."[3]

The threat of a nuclear attack involving a seaborne container lies at the nexus of two critically important security issues: the availability of nuclear materials and the vulnerability of cargo containers. Although the U.S. government has taken a number of steps in the past few years to secure nuclear materials and improve the security of the

country's ports, the threat of a nuclear weapon entering the United States undetected in a shipping container remains very real. Much additional work, including international standards for container security and expanded international cooperation to prevent the proliferation of nuclear materials, is necessary to prevent a catastrophe that could dwarf the tragedy of 9/11.

II. The Nature of the Threat

An act of nuclear terrorism involving a cargo container could take one of two forms: a nuclear weapon or a radiological dispersal device (commonly referred to as a "dirty bomb"). A nuclear weapon requires the presence of a critical mass of fissile nuclear material – specifically, plutonium or highly enriched uranium (HEU) – in order to achieve a nuclear chain reaction. A nuclear detonation generates extreme levels of heat and radiation, which, in a densely populated area, would result in immediate, large-scale destruction, as occurred in Hiroshima and Nagasaki in 1945. In contrast, a dirty bomb involves conventional explosives designed to spread radioactive material over a wide area. For example, a terrorist might use a fertilizer bomb, such as the one used to destroy the Alfred P. Murrah federal building in Oklahoma City in 1995, in order to disperse radioactive material in a commercial center. Although a dirty bomb could result in long-lasting contamination of the affected area, its potential impact pales in comparison to that of a nuclear detonation. Thus, logistical considerations aside, a terrorist seeking to maximize damage in a nuclear attack would choose a nuclear device over a dirty bomb.

What, then, is the potential impact of an attack on a major U.S. port involving a nuclear weapon or dirty bomb? Without question, the damage would be devastating. Gal Luft and Anne Korin at the Institute for the Analysis of Global Security describe a

scenario where terrorists ram a cargo ship loaded with explosives, or possibly a WMD, into a major port or terminal. "Such an attack," they state, "could bring international trade to a halt, inflicting multi-billion-dollar damage on the world economy."[4] Robert Bonner, currently the Commissioner of Customs and Border Protection, painted a similarly bleak picture in August 2002: "There is virtually no security for what is the primary system to transport global trade. The consequences of a terrorist incident using a container would be profound . . . If terrorists used a sea container to conceal a weapon of mass destruction and detonated it on arrival at a port, the impact on global trade and the global economy could be immediate and devastating – all nations would be affected. No container ships would be permitted to unload at U.S. ports after such an event."[5]

Although these assessments give a general idea of the impact of a nuclear attack, a better perspective can be achieved by quantifying the potential effects. Historical disruptions of port operations provide some indication of the potential magnitude of a large-scale shutdown of U.S. ports. In 2002, a strike by the International Longshore and Warehouse Union caused the closing of twenty-nine West Coast ports for ten days. One study estimated that the shutdown cost the U.S. economy $19.4 billion.[6] If a lengthy shutdown of cargo traffic at all U.S. ports occurred in response to a container-based nuclear attack, the total costs would be staggering.

In October 2002, consulting firm Booz Allen Hamilton conducted a two-day "Port Security War Game" in order to determine the implications for U.S. supply chains of such a terrorist attack. The war game presented participants with a simulated scenario involving the discovery of two dirty bombs in shipping containers in Los Angeles and Minneapolis. In response to the threat, the participants ordered the closing of two ports for three days and, as the crisis continued, all U.S. ports for nine subsequent days. The

total economic impact of the port closings was estimated to be $58 billion, which resulted from a three-month container backlog and ensuing spoilage, sales losses and manufacturing slowdowns.[7]

According to another study, prepared by Abt Associates for the U.S. Department of Transportation's Volpe National Transportation Systems Center, a Hiroshima-sized (10- to 20-kiloton) nuclear detonation at a major seaport would kill fifty thousand to one million people and result in direct costs from property damage and trade disruption of $150 billion to $700 billion.[8] Indirect economic costs are expected to add up to another $1.4 trillion. Thus, the total one-year economic cost to the U.S. of a container-based nuclear attack on a major seaport such as Los Angeles-Long Beach or New York-New Jersey could approach $2 trillion. The report also states that the "global and long-term effects, including the economic impacts of the pervasive national and international response to the nuclear attack . . . are believed to be substantially greater."[9]

In order to place these figures in proper perspective, it is helpful to examine the impact of the September 11, 2001 attacks. One study estimated that the attacks resulted in a total cost to New York City of between $82.8 billion and $94.8 billion.[10] Although certain sectors, such as the airline industry, are still suffering lingering effects, the U.S. economy has managed a reasonably swift recovery. During 2001, the U.S. experienced a meager 0.8 percent growth in real GDP and witnessed two quarters of contraction. In each subsequent year, however, the country's real GDP has grown at an increasing rate, registering growth rates of 1.9, 3.0 and 4.4 percent.[11] Furthermore, a report by the Congressional Research Service concluded that "the direct effects of the attacks were too small and too geographically concentrated to make a significant dent in the nation's economic output."[12] This would not be the case if terrorists were to detonate a nuclear

device or dirty bomb at a major seaport such as Los Angeles or Long Beach, which together accounted for more than 35 percent of all container traffic in the U.S. in 2003.[13]

III. Availability of Nuclear Materials

A fundamental factor contributing to the threat of a container-based terrorist attack is the disturbing availability of nuclear materials, which include unsecured nuclear weapons, fissile nuclear material and other sources of radioactivity. As previously stated, given a choice, a terrorist would opt for a nuclear device over a dirty bomb in order to maximize casualties and damage to physical infrastructure. The first obstacle a potential nuclear terrorist faces is the acquisition of a functional nuclear weapon. There are more than two hundred locations worldwide where a would-be terrorist could acquire a nuclear weapon or the fissile material to make one.[14] The area of greatest concern is Russia, which may still possess as many as twelve thousand low-yield tactical nuclear weapons that are often kept in less secure conditions than the weapons in the nation's strategic arsenal.[15] Fortunately, a nuclear bomb in a terrorist's hands has thus far been only the subject of spy thrillers and Hollywood productions rather than a live CNN newscast.

If the theft of a complete nuclear weapon proved too difficult, terrorists could attempt to steal or purchase the necessary fissile material and construct a bomb on their own. The minimum amount of weapons-grade fissile material required for a nuclear detonation varies with bomb design but can be as little as twelve kilograms of uranium-235 or four kilograms of plutonium-239. Terrorists seeking this path might look to one of the 130 research reactors in more than 40 countries worldwide that use highly enriched uranium (HEU) as fuel.[16] Attempted thefts of materials from such facilities occur with disturbing frequency. In the first three years after the fall of the Soviet Union in 1991,

for example, the German government reported more than seven hundred incidents of attempted nuclear sales, including sixty cases that involved seizure of nuclear materials.[17] Furthermore, the Database on Nuclear Smuggling, Theft and Orphan Radiation Sources (DSTO), compiled by researchers at Stanford University's Center for International Security and Cooperation, has documented twenty-five "highly-credible" incidents involving the trafficking of weapons-grade plutonium or HEU since 1992.[18] Fortunately, in all but one of these cases, the stolen nuclear material was recovered by law enforcement officials. Although open-source literature may offer little evidence of successful thefts involving significant amounts of weapons-usable nuclear material, the potential existence of unreported or as yet undiscovered thefts is sufficient cause for concern.

Whereas obtaining enough fissile material for a working nuclear bomb could prove logistically challenging, there is no shortage of radioactive material that a terrorist could use to construct a dirty bomb. Sources of radioisotopes can be found in a diverse array of medical and industrial technologies. For example, cesium-137 and cobalt-60 are commonly used in nuclear medicine, and americium-241 can be found in certain oil exploration equipment. According to a 2003 study by the Center for Non-Proliferation Studies, between October 1996 and September 2001, an average of three hundred commercial radioactive sources were lost or unaccounted for (or "orphaned") each year. Of these orphaned sources, 56 percent were not recovered.[19] Figures published by the U.S. Environmental Protection Agency in 1998 are even more pessimistic, estimating that there were as many as thirty thousand orphaned radioactive sources in the U.S. at that time.[20]

Given the availability and relative insecurity of nuclear materials, policymakers must address the very real risk that sophisticated terrorists might succeed in obtaining such materials. The story of David Hahn, a nuclear-savvy Michigan teenager, should serve as ample warning. Over the course of three years beginning in 1991, Hahn collected and purified enough radioactive material in his mother's potting shed to put forty thousand nearby residents at risk due to the dangers posed by the release of radioactive dust and radiation.[21] A terrorist organization with sufficient determination and financial resources would no doubt pose a much greater threat.

IV. Vulnerability of Containerized Cargo

Once nuclear materials have been obtained, a terrorist's next challenge is avoiding detection while bringing that material into the United States. As government officials and independent security experts repeatedly point out, the easiest way for a terrorist to accomplish this is by exploiting the vulnerability of the global cargo transportation system. The efficiency of this system relies on the versatility of intermodal containers – standardized containers (usually 40 x 8 x 8 feet in size) that can travel by ship, train or truck without being repackaged or reconfigured. Every day, 30,000 trucks, 6,500 rail cars and 140 ships deliver more than 50,000 such containers to destinations within the United States.[22] Although some of these containers initially make their way into the U.S. via highway and rail, the vast majority of containers enter through one of the country's 361 public ports, which handle over 95 percent of U.S. overseas trade.[23] As the global economy continues to expand, the total volume of goods imported and exported through U.S. ports is expected to more than double over the next twenty years, dramatically increasing the burden on inspectors tasked with securing the nation's ports.[24]

Although shipping containers enter American ports at a rate of roughly twenty thousand per day, fewer than 5 percent are opened for inspection.[25] In the findings outlined in the Maritime Transportation Security Act (MTSA) of 2002, the U.S. Congress acknowledged this problem: "Current inspection levels of containerized cargo are insufficient to counter potential security risks. Technology is currently not adequately deployed to allow for the nonintrusive inspection of containerized cargo . . . Security-related and detection-related equipment, such as small boats, cameras, large-scale x-ray machines, and vessel tracking devices, are lacking at many ports."[26]

This has created a situation where terrorists seeking to smuggle a nuclear weapon into the U.S. via a cargo container face highly favorable odds of escaping detection. According to one study, in fact, the probability that inspectors will detect a shielded nuclear weapon in a shipping container using the current screening system is only about 10 percent.[27] In order to decrease the likelihood of a nuclear weapon entering the U.S. in a container, the odds of detection must be significantly improved. Otherwise, terrorists will eventually attempt to exploit this system, given the relatively low risk that a nuclear weapon or dirty bomb would be detected.

Although the U.S. government made significant investments in national security during the first term of the Bush Administration, there is evidence to suggest that the dollars have not been allocated in proportion to the threat. According to Stephen Flynn, a Senior Fellow in National Security Studies at the Council on Foreign Relations, the CIA has concluded that the most likely way that a WMD would enter the U.S. is by sea.[28] Despite this assessment, as of September 2004, the U.S. government was spending more every three days to finance the war in Iraq than it had provided over the previous three years to improve security at all 361 U.S. seaports.[29]

V. Current Initiatives

Preventing terrorists from smuggling a nuclear weapon into the country in a shipping container will require concurrent efforts both to reduce the availability of nuclear materials and to improve the security of maritime cargo transportation. The U.S. government has launched several programs to tackle each of these issues, but these existing initiatives fall short of what is necessary to achieve adequate security.

First of all, the United States has taken the critically important step of seeking the cooperation of former Soviet states to prevent the proliferation of nuclear materials and to keep such materials out of the hands of terrorists. For example, the Soviet Nuclear Threat Reduction Act of 1991 (also called the Nunn-Lugar Act) launched the Cooperative Threat Reduction (CTR) Program to assist states of the former Soviet Union in controlling and protecting their nuclear weapons, materials and infrastructure. By funding activities such as the removal of strategic nuclear warheads to Russia and the elimination of ICBMs, the CTR Program was instrumental in assisting Kazakhstan, Ukraine and Belarus to become non-nuclear weapons states after the fall of the Soviet Union.[30] Likewise, the Department of Energy's Materials Protection, Control and Accounting Program (MPC&A) works to prevent the proliferation of nuclear materials, technologies and expertise from former Soviet states.[31] Such initiatives merit urgent attention and significant government resources. Currently, however, these efforts are limited to former Soviet states and are dangerously underfunded. Of the nearly $500 billion that the U.S. has budgeted for defense spending in 2005, a mere $1 billion will be allocated to all forms of nuclear-material control.[32] In contrast, the missile defense

program, which on February 13, 2005, experienced its second interceptor missile failure in as many months, is slated to receive more than $50 billion in the next five years.[33]

If a terrorist does succeed in obtaining nuclear materials, additional layers of defense must exist to increase the likelihood that the materials are detected before they can be used in an act of terror. The commonly accepted standard in cargo inspection is that it takes five agents three hours to conduct a thorough physical examination of a single fully loaded intermodal container.[34] Clearly, physical inspection of every cargo container is not a possibility, as it would bring global shipping to a halt. Fortunately, the U.S. government has initiated a number of programs designed to address this facet of the problem in more practical ways.

First, Operation Safe Commerce (OSC) is a $75 million-initiative aimed at strengthening security at the nation's three largest regional ports: Los Angeles-Long Beach, New York-New Jersey, and Seattle-Tacoma.[35] The program brings together private businesses, ports, and representatives from local, state, and federal agencies to analyze current security procedures for cargo entering the U.S. Specifically, OSC seeks to leverage existing technology to monitor the movement and integrity of containers through the supply chain. Although the preliminary results of the Seattle-Tacoma portion of OSC seem promising, additional federal funding will be necessary to expand OSC beyond its initial pilot programs to incorporate the fifty largest U.S. ports.[36]

Another major program is the Container Security Initiative (CSI), which inspects and clears containerized cargo before shipment to the U.S. Announced by U.S. Customs Commissioner Robert Bonner in January 2002, the Container Security Initiative consists of four core elements: 1) using intelligence and automated information to identify and target containers that pose a risk for terrorism; 2) pre-screening those containers that pose

a risk at the port of departure before they arrive at U.S. ports; 3) using detection technology to quickly pre-screen containers that pose a risk; and 4) using smarter, tamper-evident containers.[37] Through CSI, U.S. Customs and Border Protection (CBP) has deployed inspectors at thirty-five major seaports (including the twenty largest) in North America, Europe, Asia and Africa. Although CBP has extended a reciprocal offer to participating nations to station their own customs inspectors at U.S. ports, as of April 2005, only Canada and Japan have accepted.[38]

Another U.S. initiative, the Customs-Trade Partnership Against Terrorism (C-TPAT), seeks the voluntary participation of companies that agree to work with CBP to protect their supply chains from the concealment of WMDs.[39] One C-TPAT objective is the development and implementation of more secure shipping containers. C-TPAT members who participate in the oceangoing smart box pilot testing of container security devices must adhere to specified sealing standards and procedures. The results of this pilot program will contribute to CBP's efforts to establish minimum regulatory requirements for high-security seals on all in-bound ocean containers.[40] One weakness of C-TPAT, however, is the nearly complete absence of Customs Service officials to monitor compliance levels among C-TPAT participants overseas.[41]

VI. Closing the Gap: Securing Nuclear Materials

The U.S. government is making progress toward reducing the availability of nuclear materials and improving the security of maritime cargo transportation, but much more remains to be done. Though leading terrorism experts may hold different views on how to approach the challenge, most agree that the foremost priority should be an all-out

effort to secure nuclear weapons and fissile materials worldwide, with a particular focus on Russia.[42]

In 2001, Harvard professor Graham Allison, in a spending proposal prepared for the Baker-Cutler task force, estimated that a $30 billion investment over eight to ten years would secure and reduce Russia's nuclear stockpiles, nuclear complex, and control its nuclear expertise.[43] More recently, however, in his role as an advisor to John Kerry's presidential campaign, Allison said that, if made a priority, securing Russia's nuclear materials could be achieved in only four years at a cost of between $30 billion and $50 billion.[44] Although the Bush Administration requested $1.06 billion in FY 2005 for cooperative programs to reduce WMD threats, only about $700 million of that total is focused on reducing the threat of unsecured nuclear weapons, material and expertise.[45] As a comparison, as of February 2005, Congress had appropriated more than $207 billion to fund the war in Iraq.[46] This sum would have been sufficient to fund all of the recommendations of the Baker-Culter panel many times over.

Although working with Russia to secure its nuclear weapons and materials should be a first priority, it falls short of a complete solution. The U.S. government should launch additional initiatives to broaden the base of cooperation throughout the international community. For example, working in concert with the International Atomic Energy Agency (IAEA), the U.S. should exercise global leadership by encouraging the establishment and enforcement of mandatory international standards for secure storage, transportation and tracking of nuclear weapons and materials.

The foundation for such standards currently exists in the form of the Convention on the Physical Protection of Nuclear Material (CPPNM). The CPPNM, which was organized by the IAEA and opened for signature in 1980, obliges participants to ensure

the protection of "peaceful" nuclear material during international transport.[47] The Convention is limited in scope, however, as its current form does not apply to nuclear material for military purposes or to the domestic transport of peaceful nuclear material. In addition, the application of the Convention reflects the participants' beliefs, at the time of negotiation, that the physical protection of nuclear materials within the domestic sphere is a national responsibility and should not be subject to binding international standards. Fortunately, CPPNM signatories have exhibited renewed interest in amending and strengthening the Convention.[48] When the CPPNM convenes its next Diplomatic Conference in July 2005, the United States should lead its fellow signatories in completion of an already initiated amendment process to expand the scope of the Convention. If the CPPNM is amended as proposed, the Convention will also apply to the physical protection of nuclear material in domestic use, storage and transport, as well as to the protection of nuclear materials and facilities against sabotage.

One obstacle to the implementation of the proposed changes is the ability of the IAEA to enforce the standards of the Convention. The CPPNM does not currently provide for inspections; rather, the IAEA has initiated the International Nuclear Security Advisory Service (INSServ) to help nations evaluate their nuclear security regimes. Under the current Convention, a nation must request a visit by IAEA experts, who identify any deficiencies in the country's nuclear security. In order to be effective, participants in the CPPNM should agree to mandatory periodic audits by IAEA inspectors to evaluate the level of compliance with international standards for nuclear security. Naturally, participants must also agree to a reasonable set of measures if a member state is found in violation of CPPNM standards. Such measures might involve large fines, which could be used by the IAEA to further its nuclear security efforts.

VII. The Second Piece: Securing Containerized Cargo

In addition to making significant increases in appropriations to secure nuclear weapons and material around the globe, the U.S. must simultaneously strengthen efforts to enhance the security of containerized cargo. These efforts must include initiatives to ensure the integrity of shipping containers in transit and well as the development and deployment of technologies to detect radioactive material within containers.

The first vital need is to protect container integrity throughout the entire global supply chain. Currently, no standard exists for a tamper-proof intermodal shipping container. Under existing port security regimes, terrorists might be able to break into and hide nuclear materials in a container from a "trusted shipper," thus increasing their chances of escaping the scrutiny of inspectors. One possible solution is a multipurpose security device that would be required on every shipping container. Such a device would conform to internationally mandated standards and would enhance the security of a container in several ways. First, the device would have intrusion detection capability to protect the integrity of the container against unauthorized access. In addition, the device would contain basic radiation detection equipment to identify the presence of nuclear materials. Finally, the security device would also serve as a GPS-based tracking device to monitor the location of the container. The device would be assayed via radio frequency (RF) at various points during its journey, including loading, embarkation and disembarkation, to enable inspection officials to access the collected data and determine if a container posed a potential threat. According to one study, such devices could be produced at a cost of between $100 and $200 each, or roughly 2 percent of the cost of a single shipping container.[49]

Any solution to improve the security of containerized cargo must take into account the commercial nature of the shipping industry. Although a $200 device may initially seem costly in an industry that already faces relatively low margins, the cost of a security device will be spread over multiple shipments over an extended period of time. One way to mitigate the economic impact of new security measures is to ensure that none of the stakeholders in the maritime shipping industry are forced to bear an unfair share of the costs. Shippers are unlikely to adopt any solution that will inhibit their ability to compete in the marketplace. One way to achieve this is by instituting mandatory international standards for container security, so that no shipper can obtain a competitive advantage by opting out of security enhancements. Current initiatives, such as the Customs-Trade Partnership Against Terrorism, are largely voluntary in nature, and firms that choose not to participate may possess a cost advantage over their competitors that do participate. Mandatory standards address the challenge of enlisting the cooperation of profit-oriented businesses that are reluctant to do anything, even for the sake of security, that will place them at a disadvantage.

VIII. The Last Layer: Detection Technologies

A critical complement to container security standards is the deployment of technologies to detect nuclear materials within a shipping container. There are two main types of systems for detecting nuclear and radiological materials: passive and active. Current systems, such as the ground-mounted Radiation Portal Monitors planned for use by U.S. Customs and Border Protection at Calexico on the California-Mexico border, are primarily passive and rely on trace signs to detect the presence of radioactive isotopes. Unfortunately, many passive detectors, such as the handheld radiation detectors used by

customs agents in many countries, suffer from an inability to detect HEU with even a very small amount of shielding.[50] Active systems, which use gamma rays or x-rays to probe the contents of a truck or container, are generally more expensive than passive systems but are better suited for inspecting specific objects.[51] Although public concern about health and safety risks might preclude the use of active detection systems on occupied vehicles, there should be little risk using active systems to examine unoccupied shipping containers, provided that steps are taken to protect the inspectors from radiation exposure.

Scientists at Los Alamos National Laboratory have developed one of the most promising new technologies with applications for detecting nuclear materials in shipping containers. This new active technique, called muon radiography, can detect uranium and plutonium, even when shielded with heavy materials such as lead and tungsten. Detectors employing muon radiography are far more sensitive than those using x-rays, and they present none of the radiation hazards of active systems utilizing x-ray or gamma-ray detectors. The Los Alamos team is currently working on a full-sized prototype, with completion expected for summer 2005. The new devices, which will be large enough to scan a standard intermodal container or a 50-foot trailer truck, would cost about $1 million each.[52] The researchers estimate that a system to scan every cargo container coming into the U.S. by ship or truck, in a timely manner that would not impede container traffic, would cost about $1 billion.[53]

Continued research and development of new detection technologies will be necessary to ensure the security of the nation's ports. The Bush Administration's budget request for FY 2006 provides hope that the need for such efforts has been recognized. For example, the budget request for the Department of Homeland Security includes $227

million for the creation of a Domestic Nuclear Detection Office (DNDO), which will be charged with developing, acquiring and supporting systems to detect and report nuclear and radiological materials intended for criminal use.[54] Likewise, in 2004, the Homeland Security Advanced Research Projects Agency (HSARPA) issued a Broad Agency Announcement (BAA 04-02) soliciting proposals for the development of an array of radiological and nuclear detection systems.[55] Such federal government appropriations will encourage private sector investment in the development of these critically important detection technologies.

IX. Conclusions

In one of his final interviews before leaving office, former Attorney General John Ashcroft stated that the greatest danger facing the United States in the war on terrorism is the possibility that al Qaeda or a sympathetic terrorist group could obtain a nuclear bomb.[56] Security experts from the CIA, the Department of Homeland Security, Customs and Border Protection, the Coast Guard, and a multitude of think tanks have repeatedly identified the maritime cargo transportation system as the most likely means by which terrorists might bring a nuclear weapon into the United States. Despite these warnings, current measures to defend against a container-borne nuclear attack remain terribly inadequate.

In the wake of the September 11, 2001 attacks, the U.S. government moved swiftly to improve the security of aviation transportation. In light of the potentially devastating costs of a nuclear attack, this nation cannot afford to take a similarly reactive approach to container security. Programs such as the Cooperative Threat Reduction Program and the Container Security Initiative must be given adequate funding and must

be augmented by mandatory international standards for container integrity and the deployment of cost-effective radiological detection systems. Although the U.S. government has taken a number of steps toward preventing a nuclear catastrophe, there are still miles to go before we can all sleep comfortably knowing that our nation's ports are secure against a nuclear attack.

References

Abt, Clark C. *The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability*, Executive Summary. Abt Associates Inc., April 30, 2003.

Allison, Graham. *Nuclear Terrorism: The Ultimate Preventable Catastrophe.* New York: Times Books, 2004.

American Association of Port Authorities, Port Industry Statistics, "North American Port Container Traffic - 2003," http://www.aapa-ports.org/industryinfo/statistics.htm.

Anderson, Curt, Associated Press, "Ashcroft: Nuke Threat the Largest Danger," *CNN.com*, January 28, 2005, http://www.cnn.com/.

Baker, Howard and Lloyd Cutler, co-chairs, *A Report Card on the Department of Energy's Nonproliferation Programs with Russia*, Secretary of Energy Advisory Board, January 10, 2001.

Beckner, Christian, Mark Shaheen, and Vesna Cuk. "The FY 2006 Homeland Security Budget Request: Key Implications for the Private Sector." Civitas Group LLC, February 2005.

Bunn, Matthew, *Controlling Nuclear Warheads and Materials*, Securing Nuclear Warheads and Materials, "Materials Protection, Control & Accounting," http://www.nti.org/e_research/cnwm/securing/mpca.asp,.

Bunn, Matthew and Anthony Wier. *Securing the Bomb: An Agenda for Action.* Project on Managing the Atom, Harvard University, May 2004.

Cohen, Stephen S. "Economic Impact of a West Coast Dock Shutdown," January 2002.

"Convention on the Physical Protection of Nuclear Material (CPPNM)," Inventory of International Nonproliferation Organizations and Regimes, Center for Nonproliferation Studies, updated April 22, 2005, http://cns.miis.edu/pubs/inven/pdfs/cppnm.pdf.

"Detection Systems for Radiological and Nuclear Countermeasure," Broad Agency Announcement 04-02, Proposer Information Pamphlet, Department of Homeland Security, Homeland Security Advanced Research Projects Agency, January 30, 2004.

The Economist, "Muon-Assured Defence," February 26, 2005.

Fallows, James. "Success without Victory." *Atlantic Monthly*, January/February 2005.

Federation of American Scientists, "Cooperative Threat Reduction Status," http://www.fas.org/nuke/control/ctr/status.htm.

Ferguson Charles D., Tahseen Kazi, and Judith Perera. *Commercial Radioactive Sources: Surveying the Security Risks.* The Center for Non-Proliferation Studies, Occasional Paper No. 11. Monterey, CA: Monterey Institute of International Studies, January 2003.

Flynn, Stephen E. "The Fragile State of Container Security." Written Testimony before the Senate Governmental Affairs Committee, March 20, 2003, http://www.cfr.org/pub5730/stephen_e_flynn/the_fragile_state_of_container_security.php.

Flynn, Stephen E. "The Neglected Home Front." *Foreign Affairs*, September/October 2004.

Gerencser, Mark, Jim Weinberg and Don Vincent. "Port Security War Game: Implications for U.S. Supply Chains." Booz Allen Hamilton, Inc., 2003.

Healy, Patrick. "Kerry Says He'd Secure Nuclear Materials," *Boston Globe*, June 2, 2004, http://www.boston.com/news/nation/articles/2004/06/02/kerry_says_hed_secure_nuclear_materials/.

Holdren, John and Matthew Bunn. "Technical Background: A Tutorial on Nuclear Weapons and Nuclear Explosive Materials – Part Five." Nuclear Threat Initiative Research Library: Controlling Nuclear Warheads and Materials, January 2004, http://www.nti.org/e_research/cnwm/overview/technical5.asp.

House Subcommittee of Coast Guard and Maritime Transportation, Hearing on Implementation of the Maritime Transportation Security Act, June 9, 2004, http://www.house.gov/transportation/cgmt/06-09-04/06-09-04memo.html.

International Atomic Energy Agency, International Conventions and Agreements, Convention of the Physical Protection of Nuclear Material, http://www.iaea.org/Publications/Documents/Conventions/cppn.html.

Los Alamos National Laboratory, "Los Alamos Muon Detector Could Thwart Nuclear Smugglers," February 19, 2005, http://www.lanl.gov/orgs/p/pdfs/muon_rls.pdf.

Luft, Gal and Anne Korin. "Terrorism Goes to Sea." *Foreign Affairs*, November/December 2004.

Makinen, Gail et al. *The Economic Effects of 9/11: A Retrospective Assessment*. Congressional Research Service, CRS Report RL31617, September 27, 2002.

Maritime Transportation Security Act of 2002, Public Law 107-295, *U.S. Statutes at Large* 116 (2002).

May, Michael, Tonya Putnam and Dean Wilkening. "Detecting Nuclear Material in International Container Shipping: Criteria for Secure Systems." Center for International Security and Cooperation, Stanford University, January 2003.

Naraine, Neil and John M. Karhnak. "The New Orphaned Radioactive Sources Program in the United States." International Conference on the Safety of Radiation Sources and the Security of Radioactive Materials, September 1998, http://www.epa.gov/radiation/docs/cleanmetals/dijon_pa.pdf.

National Priorities Project, "Cost of War Rises for American Tax Payers," February 2005, http://www.nationalpriorities.org/issues/military/iraq/highcost/us.pdf.

Port of Seattle, "Senator Patty Murray Announces Completion of Test Phase of Operation Safe Commerce, Discusses Project Findings," September 4, 2004, http://www.portseatttle.org/news/press/09_02_2004_73.shtml.

Potter, William C., Charles D. Ferguson, and Leonard S. Spector. "The Four Faces of Nuclear Terror and the Need for a Prioritized Response." *Foreign Affairs*, May/June 2004.

Remarks of U.S. Customs Commissioner Robert C. Bonner, Speech Before the Center for Strategic and International Studies, Washington, D.C., August 26, 2002, http://www.csis.org/features/bonner.pdf.

Silverstein, Ken. "The Radioactive Boy Scout." *Harper's Magazine*, November 1998.

Thompson, Jr., William C., Comptroller, City of New York. "One Year Later: The Fiscal Impact of 9/11 on New York City." September 4, 2002.

U.S. Bureau of Economic Analysis, "Gross Domestic Product: Fourth Quarter 2004 (Final)," March 30, 2005, http://www.bea.doc.gov/bea/newsrelarchive/2005/gdp404f.pdf.

U.S. Customs and Border Protection, "CSI Fact Sheet," April 2005, http://www.cbp.gov/linkhandler/cgov/border_security/international_activities/csi/csi_fact_sheet.ctt/csi_fact_sheet.doc.

U.S. Customs and Border Protection, "Securing the Global Supply Chain: Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan," http://cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf.

U.S. Department of Homeland Security, Office for Domestic Preparedness, *Operation Safe Commerce Phase III: Program Application and Guidelines*, http://www.ojp.usdoj.gov/odp/docs/FY05_OSC_revised.pdf.

Wein, Lawrence M. et al. "Preventing the Importation of Illicit Nuclear Materials in Shipping Containers." Unpublished Technical Paper, Stanford University, October 2003.

Woolf, Amy. *Nuclear Weapons in Russia: Safety, Security, and Control Issues*. Congressional Research Service, CRS Issue Brief IB98038, August 15, 2003.

Zaitseva, Lyudmila and Friedrich Steinhausler. "Illicit Trafficking of Weapons-Usable Nuclear Material: Facts and Uncertainties." *Physics & Society*, January 2004, http://www.aps.org/units/fps/newsletters/2004/january/jan04.pdf.

1. House Subcommittee of Coast Guard and Maritime Transportation, Hearing on Implementation of the Maritime Transportation Security Act, June 9, 2004, http://www.house.gov/transportation/cgmt/06-09-04/06-09-04memo.html.
2. Graham Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York: Times Books, 2004), p. 6.
3. Ibid., p. 107.
4. Gal Luft and Anne Korin, “Terrorism Goes to Sea,” *Foreign Affairs*, November/December 2004, p. 64.
5. Remarks of U.S. Customs Commissioner Robert C. Bonner, Speech Before the Center for Strategic and International Studies, Washington, D.C., August 26, 2002, http://www.csis.org/features/bonner.pdf.
6. Stephen S. Cohen, “Economic Impact of a West Coast Dock Shutdown,” January 2002, p. 12.
7. Mark Gerencser, Jim Weinberg and Don Vincent, “Port Security War Game: Implications for U.S. Supply Chains,” Booz Allen Hamilton, Inc., 2003.
8. Clark C. Abt, *The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability*, Executive Summary, Abt Associates Inc., April 30, 2003, p. 4.
9. Ibid., p. 3.
10. William C. Thompson, Jr., Comptroller, City of New York, “One Year Later: The Fiscal Impact of 9/11 on New York City,” September 4, 2002, p. 1.
11. U.S. Bureau of Economic Analysis, “Gross Domestic Product: Fourth Quarter 2004 (Final),” March 30, 2005, http://www.bea.doc.gov/bea/newsrelarchive/2005/gdp404f.pdf.
12. Gail Makinen et al., *The Economic Effects of 9/11: A Retrospective Assessment*, Congressional Research Service, CRS Report RL31617, September 27, 2002, p. 9.
13. American Association of Port Authorities, Port Industry Statistics, “North American Port Container Traffic - 2003,” http://www.aapa-ports.org/industryinfo/statistics.htm.
14. Allison, *Nuclear Terrorism*, p. 67.
15. Amy Woolf, *Nuclear Weapons in Russia: Safety, Security, and Control Issues*, Congressional Research Service, CRS Issue Brief IB98038, August 15, 2003, p. 1.
16. Matthew Bunn and Anthony Wier, *Securing the Bomb: An Agenda for Action*, Project on Managing the Atom, Harvard University, May 2004, p. viii.
17. Allison, *Nuclear Terrorism*, p. 71.
18. Lyudmila Zaitseva and Friedrich Steinhausler, “Illicit Trafficking of Weapons-Usable Nuclear Material: Facts and Uncertainties,” *Physics & Society*, January 2004, http://www.aps.org/units/fps/newsletters/2004/january/jan04.pdf, pp. 5-8.
19. Charles D. Ferguson, Tahseen Kazi, and Judith Perera, *Commercial Radioactive Sources: Surveying the Security Risks*, The Center for Non-Proliferation Studies, Occasional Paper No. 11 (Monterey, CA: Monterey Institute of International Studies, January 2003), p. 17.
20. Neil Naraine and John M. Karhnak, “The New Orphaned Radioactive Sources Program in the United States,” International Conference on the Safety of Radiation Sources and the Security of Radioactive Materials, September 1998, http://www.epa.gov/radiation/docs/cleanmetals/dijon_pa.pdf, p. 2.
21. Ken Silverstein, “The Radioactive Boy Scout,” *Harper’s Magazine*, November 1998.
22. Allison, *Nuclear Terrorism*, p. 107.
23. *Maritime Transportation Security Act of 2002*, Public Law 107-295, *U.S. Statutes at Large* 116 (2002): 2066.
24. Ibid.
25. Allison, *Nuclear Terrorism*, p. 11.
26. *Maritime Transportation Security Act of 2002*, 2066-2067.
27. Lawrence M. Wein et al., “Preventing the Importation of Illicit Nuclear Materials in Shipping Containers,” Unpublished Technical Paper, Stanford University (October 2003), p. 24.
28. Stephen E. Flynn, “The Neglected Home Front,” *Foreign Affairs*, September/October 2004, p. 22.
29. Ibid.
30. Federation of American Scientists, “Cooperative Threat Reduction Status,” http://www.fas.org/nuke/control/ctr/status.htm.
31. Matthew Bunn, *Controlling Nuclear Warheads and Materials*, Securing Nuclear Warheads and Materials, “Materials Protection, Control & Accounting,” http://www.nti.org/e_research/cnwm/securing/mpca.asp.

32. James Fallows, "Success without Victory," *Atlantic Monthly*, January/February 2005, p. 90.
33. "Muon-Assured Defence," *The Economist*, February 26, 2005, p. 80.
34. Stephen E. Flynn, "The Fragile State of Container Security," Written Testimony before the Senate Governmental Affairs Committee, March 20, 2003, http://www.cfr.org/pub5730/stephen_e_flynn/the_fragile_state_of_container_security.php.
35. U.S. Department of Homeland Security, Office for Domestic Preparedness, *Operation Safe Commerce Phase III: Program Application and Guidelines*, http://www.ojp.usdoj.gov/odp/docs/FY05_OSC_revised.pdf, pp. 4-6.
36. Port of Seattle, "Senator Patty Murray Announces Completion of Test Phase of Operation Safe Commerce, Discusses Project Findings," September 4, 2004, http://www.portseatttle.org/news/press/09_02_2004_73.shtml.
37. U.S. Customs and Border Protection, "CSI Fact Sheet," April 2005, http://www.cbp.gov/linkhandler/cgov/border_security/international_activities/csi/csi_fact_sheet.ctt/csi_fact_sheet.doc, p. 6.
38. Ibid., pp. 1-2.
39. U.S. Customs and Border Protection, "Securing the Global Supply Chain: Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan," http://cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf, p. 3.
40. Ibid., pp. 30-31.
41. Flynn, "The Fragile State of Container Security."
42. William C. Potter, Charles D. Ferguson, and Leonard S. Spector, "The Four Faces of Nuclear Terror and the Need for a Prioritized Response," *Foreign Affairs*, May/June 2004, pp. 130-132.
43. Howard Baker and Lloyd Cutler, co-chairs, *A Report Card on the Department of Energy's Nonproliferation Programs with Russia*, Secretary of Energy Advisory Board, January 10, 2001, p. A-1.
44. Patrick Healy, "Kerry Says He'd Secure Nuclear Materials," *Boston Globe*, June 2, 2004, http://www.boston.com/news/nation/articles/2004/06/02/kerry_says_hed_secure_nuclear_materials/.
45. Bunn and Wier, *Securing the Bomb*, pp. 84-85.
46. National Priorities Project, "Cost of War Rises for American Tax Payers," February 2005, http://www.nationalpriorities.org/issues/military/iraq/highcost/us.pdf.
47. International Atomic Energy Agency, International Conventions and Agreements, Convention of the Physical Protection of Nuclear Material, http://www.iaea.org/Publications/Documents/Conventions/cppn.html.
48. "Convention on the Physical Protection of Nuclear Material (CPPNM)," Inventory of International Nonproliferation Organizations and Regimes, Center for Nonproliferation Studies, updated April 22, 2005, http://cns.miis.edu/pubs/inven/pdfs/cppnm.pdf.
49. Michael May, Tonya Putnam and Dean Wilkening, "Detecting Nuclear Material in International Container Shipping: Criteria for Secure Systems," Center for International Security and Cooperation, Stanford University, January 2003, pp. 15-16.
50. John Holdren and Matthew Bunn, "Technical Background: A Tutorial on Nuclear Weapons and Nuclear Explosive Materials – Part Five," Nuclear Threat Initiative Research Library: Controlling Nuclear Warheads and Materials, January 2004, http://www.nti.org/e_research/cnwm/overview/technical5.asp.
51. Ibid.
52. Los Alamos National Laboratory, "Los Alamos Muon Detector Could Thwart Nuclear Smugglers," February 19, 2005, http://www.lanl.gov/orgs/p/pdfs/muon_rls.pdf.
53. "Muon-Assured Defence," *The Economist*, February 26, 2005, p. 80.
54. Christian Beckner, Mark Shaheen, and Vesna Cuk, "The FY 2006 Homeland Security Budget Request: Key Implications for the Private Sector," Civitas Group LLC, February 2005, p. 10.
55. "Detection Systems for Radiological and Nuclear Countermeasure," Broad Agency Announcement 04-02, Proposer Information Pamphlet, Department of Homeland Security, Homeland Security Advanced Research Projects Agency, January 30, 2004, pp. 5-6.
56. Curt Anderson, Associated Press, "Ashcroft: Nuke Threat the Largest Danger," *CNN.com*, January 28, 2005, http://www.cnn.com/.