Table of Contents
Issue 1, Volume 1 (2004)
LALP-04-023

Editor's Comments: Welcome to The Journal of Physical Security

> He that will not apply new remedies must expect new evils; for time is the greatest innovator.
>
> -- Francis Bacon (1561-1626)

> Security can only be achieved through constant change, through discarding old ideas that have outlived their usefulness and adapting others to current facts.
>
> -- William O. Douglas (1898-1980)

> In theory there is no difference between theory and practice. In practice there is.
>
> -- Yogi Berra

Physical security is about protecting valuable, tangible assets from harm. The "assets" can include, inter alia, people, buildings, equipment, materials, chemicals, hazardous waste, documents, products, merchandise, food & drink, drugs, weapons, money, and museum artifacts. The "harm" that we wish to avoid might involve theft, destruction, sabotage, vandalism, terrorism, espionage, counterfeiting, tampering, or unauthorized access.

It is clear that modern physical security has myriad problems. It suffers from a serious lack of identity, efficacy, innovation, rigor, integrity, metrics, standards, peer-review, theories/models/paradigms, and a "scientific" or academic footing. It often fails to be sufficiently holistic, predictive, preventative, and multi-disciplinary. Physical security practitioners are rarely effective in combining the social sciences with the technical sciences. The horrific terrorist attacks of September 11, 2001 only serve to further highlight some of these shortcomings.

This new journal is a modest effort to deal with some of the serious problems with the field of physical security—in particular, the lack of scholarly peer-reviewed journals. There are a number of useful trade journals that cover physical security. There are also numerous peer-review journals that focus on criminology, law enforcement, cryptography, terrorism, national security, computer security, or security management. The field of physical security, however, has long needed a journal that can serve as a central focus, as well as

a vehicle for rigorous discussion and advancement of the field, especially in the areas of research, development, modeling, testing, and analysis.

What are some of the other problems with the field of physical security? Well, for one thing, it is scarcely a "field" at all. Despite the past, present, and future importance of physical security, it is very difficult to get a formal degree in physical security from a major U.S. university. (A degree in criminology or computer security is about as close as one can usually come.) There are remarkably few introductory or advanced textbooks covering major areas of physical security, such as tamper detection, access control, and biometrics. There are some useful introductory survey textbooks about physical security in general, but few that operate at a very sophisticated level. Despite the fact that physical security is becoming increasingly high-tech, there are almost no national or international conferences where research and development results regarding physical security can be presented. Most conferences that cover physical security emphasize lectures by (often self-identified) security experts who tell war stories or espouse simplistic solutions and platitudes. Platitudes are a particularly annoying scourge for physical security—along with other unsavory elements borrowed from modern Management Science. For a variety of reasons (including that it doesn't seem to fit anywhere else), physical security is often viewed as a pseudo-subfield of management.

Physical security is also problematic because it is so difficult. Recognition of this fact is essential because complacency, overconfidence, and arrogance are incompatible with good security. One of the reasons that physical security is such a daunting task is that it is highly multidimensional. Whereas an adversary need only find and exploit one or a small number of vulnerabilities to succeed, physical security managers must identify, understand, and manage all possible vulnerabilities. While adversaries can attack at only one or a small number of points, security managers must often protect large, spatially distributed facilities. They must plan for all possible attacks at unpredictable times from all possible adversaries, many of whom may be completely unknown. Whereas security personnel are generally constrained by legal, ethical, humane, organizational, and public relations considerations, their adversaries (e.g., terrorists) may not be.

Another serious challenge for physical security is the general lack of useful performance measures. The traditional performance measure for security is pathological: success is defined as nothing happening. This kind of performance measure does not permit effective cost/benefit analysis, and

often results in insufficient resources being made available for security. Moreover, it tends to result in irrational cyclical fluctuations in security funding. Security budgets typically decay over time as long as there are no major security incidents. Once a major incident occurs, however, hysteria tends to ensue. Massive resources are suddenly thrown at the problem, much of them ultimately wasted. Draconian and often downright silly measures are introduced, some of which actually decrease overall security, or at least divert attention and resources from more effective measures. (Thus, for example, we saw airport screeners after September 11th confiscating fingernail clippers from airline passengers—presumably to keep would-be terrorists from threatening the pilots with bad manicures.) Once a security crisis passes, the emphasis on physical security typically again erodes away until the next serious incident, at which point another frantic spike in funding and activity occurs.

Effective physical security is also hampered by a lack of standards. The few standards that do exist are of little value. Standards, however, are not automatically a guarantee of effective security. If they are too broad or too narrow, not well thought through, and/or mindlessly applied, they can cause more harm than good. Moreover, there is the potential problem referred to in the old engineering joke: that the great thing about standards is that there are so many to choose from!

Physical security is also commonly plagued by ambiguity. Security programs are frequently quite vague as to exact goals and adversaries. Not helping the problem is the fact that security terminology is often sloppy, misleading, misunderstood, or misused, even by experienced security professionals.

Attitude can be a particularly significant problem for a physical security program. While there are potential benefits to showing great confidence to the outside world (because this may discourage adversaries), a healthy security program does not believe its own public guarantees and assurances. Far too often, however, physical security managers, and the high-level personnel they report to, believe their own press releases. Even worse, many security programs retaliate against insiders or outsiders who question security measures, identify vulnerabilities, offer suggestions, or call for improvements. The idea of genuine “peer review” is a largely alien concept to the field of physical security, either for the practice of security, or for research, development, and testing.

The field also suffers from society’s ambivalent attitudes towards security,

often involving the inevitable conflict between liberty and security. Other challenges include the multidisciplinary and (increasingly) technological nature of physical security, the relatively low status and educational level of many security practitioners, the boredom often associated with routine security functions, and the tendency for the field to attract the wrong type of people. Indeed, the field of physical security seems to have more than its fair share of linear, concrete, and wishful thinkers, as well as control freaks, knuckleheads, egotists, charlatans, washouts, socially maladjusted loners, bureaucrats, and those skilled at self-deception. Ironically, physical security actually requires some of the most sophisticated and diverse of all possible abilities: good observational skills, a subtle understanding of human psychology, respect for civil liberties, awareness of complex legal issues, sound judgment when working in gray areas, the ability to plan effectively but also to think and react quickly on one's own initiative, engineering sophistication, and considerable imagination and creativity in order to foresee threats. To make matters worse, people and funding are nowadays drawn more towards digital security (computers, software, networks, and the Internet) than to physical security—even though physical security is in many ways far more critical to both society and the economy than digital security.

"Compliance mode" can also be a major problem. This involves security managers or other security personnel being so focused on satisfying superiors, auditors, regulators, bureaucrats, and formal security requirements that they lose sight of real-world security threats. Being distracted by paperwork and busywork is a serious problem with physical security which, first and foremost, needs to be about paying attention. Compliance mode is very difficult to avoid in large organizations and bureaucracies, in well-established operations, and for security programs that do not encourage security personnel to be flexible, creative, introspective, clever, and proactive (and that do not have senior officials with these attributes).

Further supporting the suspicion that physical security is not a serious or mature field is the behavior of vendors and manufacturers of physical security products. Far too many make "snake oil" claims that are blatantly inaccurate, misleading, naive, or ludicrous. This is especially the case in the areas of tamper detection, access control, and biometrics. Even the most outrageous claims are rarely challenged.

This Journal will not solve all these problems. We can hope, however, to contribute to the advancement and understanding of the field. Physical

security is not just of great practical importance, it is also an intellectually challenging, multidisciplinary, fascinating subject worthy of thoughtful study.

Roger G. Johnston

Detecting Nuclear Material in International Container Shipping: Criteria for Secure Systems

Stanford Study Group[1]
Center for International Security And Cooperation
Stanford University

Abstact

This article grew out of a week-long study in August 2002 to assist ongoing efforts inside and outside the government to remedy some vulnerabilities of the international shipping system on which US and a great deal of world prosperity depend. The study's objective was to identify the most important research initiatives and the major policy issues that need to be addressed in order to improve security of imports using shipping containers, particularly against the importation of nuclear materials and weapons, while maintaining an open trading system. To be effective, a system to detect nuclear weapons or special nuclear material before they reach U.S. ports must be international in scope and reach. It must also be economically acceptable both in terms of total cost and with respect to how these costs are allocated; degrade gracefully when subjected to attack; produce actionable intelligence in a timely manner; treat false alarms realistically; be adaptable to a variety of local physical and political conditions; be auditable, secure yet accessible to the needed foreign and domestic security agencies, and have clear lines of oversight and responsibility. Finally, the system should be flexible enough to allow for regular updates as users and operators gain experience and system performance is reviewed. This study identified a sample technical approach that is feasible technically and operationally and involves components already in the early deployment stage. The approach involves container certification; monitoring at ports of embarkation, debarkation, and continuously during shipment and storage; and continuous data fusion. Specific recommendations regarding system characteristics made by the study include rigorous testing during deployment and in the field, international coordination of standards and protocols, careful analysis of the system for compatibility with pertinent governmental policies and business and labor agreements, and early provision for forward-looking research and development.

I. Introduction

This paper presents the results of a summer study conducted at Stanford University that examined how existing technology and resources can be applied most effectively to prevent the transport, by means of international commercial shipping, of illicit nuclear materials for use in terrorist activities.[2] The focus of this effort was on the detection of nuclear weapons and special nuclear materials (SNM), as well as detecting forms of radioactive material that could be used in other types of terrorist attacks, including radiological dispersal devices ("dirty bombs").[3] Issues associated with the illicit transport and import of chemical and biological weapons agents for use in

[1] Members of the study group were: Sam Chiu, Sid Drell, Bill Dunlop, Steve Flynn, Zack Haldeman, John Harvey, Tom Karzas, Michael Levi, Howard Lowdermilk, Michael May, Rob Nelson, Vic Orphan, Pief Panofsky, Tonya Putnam, Phil Stroud, and Dean Wilkening. Michael May, Tonya Putnam, and Dean Wilkening took responsibility for drafting this article.

[2] During the week of August 18-23, 2002, the Center for International Security And Cooperation (CISAC) of the Institute for International Studies (IIS) at Stanford University hosted a set of four summer studies sponsored by The John D. and Catherine T. MacArthur Foundation. The Container Security Study was one of these studies. It brought together physicists, engineers, and social scientists with experience on issues that included nuclear detection and radiography, port and container security, systems engineering, and international relations.

[3] Special nuclear materials, hereafter referred to as SNM, are the fissile materials essential to make nuclear weapons, plutonium and highly enriched uranium (HEU). Procuring them is generally agreed to constitute the major technical impediment to making nuclear weapons. Aside from a few state-to-state and state-sanctioned and monitored arrangements, there is no licit international trade in SNM or, obviously, nuclear weapons.

terrorist activity, while extremely important and in many ways more difficult to deal with, are not considered here.

The objective of this study was to assist ongoing efforts inside the government and in the private sector to remedy obvious security vulnerabilities in the international maritime shipping system. This system as it exists today has been designed for speed and efficiency—not security. A nuclear terrorist act against a major port would have extremely grave economic, political, and human consequences that would extend far beyond the port or country of attack, and could temporarily paralyze the international trading system.

An effective system for detection of nuclear weapons or SNM before they reach U.S. ports must be international in its scope and reach. Some sharing of information and technology with foreign governments and personnel will be, therefore, unavoidable to ensure needed coordination and cooperation. However, care should be taken to ensure that potential terrorists are not, at the same time, aided in their efforts to introduce illicit nuclear weapons or materials into international trade. With this caution in mind, this report omits detailed discussion of all government functions, equipment or security practices of a sensitive nature.[4]

The system of international maritime shipping handled approximately 230 million twenty-foot equivalent container units (TEU) in 2000, of which 31 million TEU (17 million actual container boxes) came through North American ports.[5] Shipping containers account for 95% of U.S. import-export cargo tonnage. Under normal conditions, the system of international maritime transport depends on the ability to maintain a steady flow of container traffic through the world's major ports. Efforts to achieve a secure system must not threaten the economic viability of the network and, by extension, the system of global trade.

Clearly, preventing the importation of materiel for nuclear terrorism involves activities that go beyond container security. Consequently, container security should be viewed in the context of an overall security architecture for preventing, disrupting, deterring, and protecting against terrorism. A comprehensive analysis of the threats posed by international terrorism requires consideration of both the operational capabilities of the organizations that pose a threat—including attention to recruiting, training, financing, command, control and communications, attack planning, mobility, and weapons acquisition, production, handling, and delivery—as well as our own security weaknesses that can be exploited. Terrorists intent upon smuggling nuclear weapons or materials into the territory of the United States or one of its allies have a number of delivery modes from which to choose. Among them are maritime shipping, airplanes (not just commercial airliners), trucks, trains, buses, private cars, and possibly even cross-border foot traffic. Among the maritime delivery modes are commercial shipping containers, other material taken aboard container vessels (e.g., supplies, equipment, luggage, fuel, etc.), non-containerized freighters, tankers, cruise ships, fishing boats, ferries, and private pleasure boats. Thus, shipping containers are only one means for transporting an assembled nuclear weapon or special nuclear material (SNM) across international borders, albeit an obvious and particularly important one given the economic impact associated with disrupting the international maritime shipping industry.

---

[4] This study was conducted at an unclassified level and drew exclusively upon information available in the public domain. As a rule, the sample technical approach described in this report incorporates commercial equipment and technologies currently available. However, in a few cases the approach recommends equipment that has not yet been developed for use in the commercial sector, but which is within the range of existing technical expertise.

[5] Testimony of Paul F. Richardson, President of Paul F. Richardson Associates, Inc., on behalf of the United States Maritime Alliance, The Pacific Maritime Association, and the National Association of Waterfront Employers before the Subcommittee on Coast Guard and Maritime Transportation, United States House of Representatives, On Funding for Seaport (Intermodal Cargo) Security, Washington, D.C., March 14, 2002; and *Drewry Container Market Quarterly*, Drewry Shipping Consultants, March 2001 as reproduced in http://www.p-and-o.com/results/Presentations/02Overview.pdf.

Unfortunately, the short duration of this study precluded an analysis of the overall security architecture and detailed consideration of these other transport methods.[6] The conclusions and recommendations of this study follow from an informal estimate of how the system of international commercial maritime traffic would figure into a comprehensive risk assessment. However, a comprehensive risk assessment should be conducted both to verify this estimate, and to ensure effective resource allocation of within an overall strategy for US homeland security. The resources in question are not only financial but also include opportunity costs associated with dedicating personnel and diplomatic efforts to enhance the security of maritime shipping, as opposed to other aspects of the international terrorist threat.

For example, a comprehensive risk assessment might conclude that, after allocating resources to fix the most urgent security vulnerabilities, it would be more cost-effective to deal with terrorism by attacking the problem as close to the source as possible. This would imply that a higher priority should be placed on US and foreign intelligence to identify and monitor groups likely to attempt to acquire nuclear weapons and SNM for terrorist purposes, thus allowing states to preempt terrorist operations. Similarly, efforts to reduce and secure existing stockpiles of nuclear weapons and SNM, especially in Russia, and to eliminate illegal trade in dangerous radioactive sources may be a key element in a comprehensive strategy for preventing acts of nuclear terrorism. In this regard, the Nunn-Lugar Cooperative Threat Reduction program would continue to be essential. Domestic and international programs for controlling and securing SNM and radioactive sources, such as those managed by the Nuclear Regulatory Commission (NRC) in the United States, the US Department of Energy, and the International Atomic Energy Agency (IAEA) internationally would also be important.

In addition, a security assessment that attempts to fully account for the costs of enhancing the security of international container traffic in the context of other threats and vulnerabilities should also factor in counter-balancing, non-terrorism-related benefits. For example, criminal activities are common in the realm of international container shipping. Private shippers, insurers, and governments routinely attempt to minimize theft, customs violations, and the flow of illegal narcotics and other contraband. Some of the technologies and equipment recommended here as components in a "systems approach" to detect the transport of illicit nuclear materials have been developed and marketed commercially for these purposes. Shippers and port or terminal operators already are adopting, with or without government support, several elements of a nascent security system.[7] Examples include installations of radiographic imaging and passive radiation detection equipment at Dover and Portsmouth in the United Kingdom, radiographic imaging equipment at ports in Singapore, and installations for scanning cross-border rail and truck traffic on both sides of the U.S. border with Canada and Mexico. Much of this equipment could be integrated into an overall security system to detect illicit international trade in radioactive and special nuclear materials with minimal additional impact on the flow of container traffic.

However, measures adopted voluntarily by commercial operators are, in general, not adequate to the task of ensuring reliable detection of smuggled nuclear weapons and special nuclear materials (SNM). First, a different selection and configuration of sensors would be required to detect nuclear weapons and SNM, as opposed to more common forms of commercial contraband such as drugs. Second, and more important from a systems perspective, the permissible failure rate for

[6] The suggested system for detection of nuclear materials in shipping containers could be adapted with some effort to international commercial truck, rail, airplane, and other maritime transport modes. Clearly, each of these modes has features that differ in potentially important ways from maritime shipping, but the group did not have time to investigate those differences in any detail.

[7] To date these investments have been made mainly for the purpose of interdicting drugs, reducing pilferage and other criminal activities.

commercial inspection systems falls short of a tolerable threshold for security—some losses due to crime are accepted as part of "the cost of doing business." By contrast, the consequences of even a single breach of security involving a nuclear weapon could be catastrophic. Therefore, a more sophisticated strategy is required to fulfill the objective of preventing incidents of nuclear terrorism on U.S. territory.

Nevertheless, every effort should be made to integrate any security system against nuclear smuggling with efforts to provide commercial security. A government-sponsored counter-nuclear effort could benefit from commercial investments in security, while commercial security interests could benefit from the surveillance added by government-sponsored efforts.

A significant proportion of the total volume of international shipping passes through very large "super-ports." Roughly 25% of all container handling worldwide is performed at the five busiest container ports—Hong Kong, Singapore, Pusan, Kaoshiung, and Rotterdam.[8] Steps to detect illicit nuclear materials at these and other "choke points" in the international system of maritime shipping should be a focus of early efforts. Similarly, a large fraction of the shipping destined for the United States enters through a relatively small number of ports. Much of the transportation, terminal operation, insurance and re-insurance business is similarly concentrated. This level of concentration does not eliminate the need to secure the many smaller installations that could provide vulnerable entry points, but it makes it possible to begin testing equipment and system approaches in a few major locations with a realistic expectation that practices adopted at those sites may, with suitable inducements and economies of scale, spread to cover the rest of the industry.

No single technology can detect illicit nuclear weapons and materials with 100 percent reliability. Consequently, a security-oriented approach to container inspection should be structured as a "layered defense," incorporating a number of independent detection opportunities along the supply chain. System design, and continued system monitoring is as important as appropriate equipment and practices, given that all static systems and technologies are vulnerable to eventual evasion by a sophisticated enemy. Attention to minimizing overall system vulnerabilities—including those arising from human operators—is important. Care should be taken in overall system design and maintenance not to introduce new vulnerabilities as existing weak points are addressed. To achieve those ends, the system should be continuously tested by means of "red-team" exercises that probe for vulnerabilities because, unlike other forms of contraband and theft, there will be relatively few if any real-world experiences with nuclear weapon smuggling to draw upon, although the number of smuggling incidents involving radioactive sources is somewhat larger.

One program for installing and testing new equipment and new ideas, Operation Safe Commerce, has received congressional approval and funding, and is in the early stages of implementation at three major U.S. ports.[9] Operation Safe Commerce is a voluntary partnership between private companies, commercial carriers, terminal operators, and local U.S. agencies to develop and test procedures, equipment, and information systems to improve the security of the maritime shipping system.[10] The program permits government and commercial entities to install experimental systems and equipment, and to conduct trials of new technologies, information

[8] None of the five largest ports are located in the United States. However, if the port facilities at Long Beach and Los Angeles are considered together, then they are third in the ranking.

[9] The ports of Los Angeles-Long Beach, Seattle-Tacoma, and New York-New Jersey have been designated as testing sites, together with companion ports outside the United States—Hong Kong and Singapore for the west coast ports, and the port of Rotterdam for New York-New Jersey.

[10] Three different types of players will be eligible to run test-bed experiments at these designated ports: (1) groups that win contracts from the $28 million dollars in federally appropriated funds; (2) commercial entities that have developed technologies for port security and which hope to earn endorsements for their products; and (3) scientists and technicians from government laboratories who want to test newly developed equipment and technologies.

systems, and procedures, with minimum disruption to port activities.[11] The Stanford Container Security study group strongly recommends ensured funding for Operation Safe Commerce and similar projects that incorporate a systems approach to maritime and port security, and which also contain specific provisions for collecting needed data, and developing and testing new technologies for improving maritime and port security.[12] The recommendations made in this report are intended to be compatible with this and other test-bed projects.

More generally, three major categories of challenges are associated with improving the security of international commercial shipping networks and port facilities:

1. Technical challenges: Equipment and system design, and research management;
2. Economic challenges: Anticipating the costs of required technical and human investments, and determining which entities will bear those costs; and
3. Institutional challenges: Overcoming domestic and international impediments to securing cooperation from various market participants, interest groups, and nation-states.

Of these, economic problems appear to be paramount. However, concerns surrounding sovereignty over ports and inspection facilities, labor agreements, and other underlying political constraints will be far from simple to overcome. Commercial equipment is currently available that can remotely scan closed containers to determine, with a reasonable degree of confidence, whether they contain many types of nuclear or radiological materials. However, it has yet to be determined whether more discriminating methods of interrogation, which tend to be more expensive and time consuming, will be adopted at large ports, not to mention many smaller port facilities. To be readily embraced by system participants, the costs of achieving a secure system will have to be small relative to shipping costs (a few percent of the cost of the goods shipped), unless significant government subsidies are made available to alleviate the financial burden. Deciding how to spread these costs fairly, and in such a way as to maximize incentives for compliance among legitimate market participants, will be a critical component in reducing opportunities for maritime transport to be used either as a conduit for or a target of nuclear terrorism.

Fortunately, improvements in container security will produce economic and social benefits that will accrue to partner governments and market participants. As already noted, integrating existing and prospective systems for commercial security and security against nuclear terrorism can substantially reduce the overall cost of the system. Moreover, benefits from reducing theft, contraband (e.g. drugs, trafficking in humans, small arms, etc.) and other forms of illegal activity suggests that the cost of improving security for container traffic need not be charged primarily to defense against nuclear terrorism since other public goods will benefit.

A number of more specific problems were also identified within the three general categories mentioned above. They include challenges associated with:

[11] Constructing a Secure Trade Corridor: A Proposed Multilateral Public/Private Partnership, by Dr. Stephen E. Flynn, Senior Fellow, Council on Foreign Relations, p. 4.

[12] One such program is the Container Security Initiative run by the US Department of Commerce (see http://www.customs.gov/news/ctpat/index.htm).

- Development of internationally acceptable standards for certification of "trusted" shippers, together with methods for monitoring the continued integrity of those arrangements;
- Specification of an optimal combination of types of external scanners and detectors at ports of embarkation;
- Devising cost-effective technologies for assuring container integrity after inspection, including technology to communicate to monitors when a breach occurs;
- Designing technologies and systems to assess the presence of dangerous nuclear material under realistic conditions;
- Overcoming difficulties associated with inspecting the contents of tightly packed containers, and bulk goods;
- Identification of suitable locales and procedures for handling suspect containers entering or approaching a U.S. border;
- Developing a system for reliable communication, control, and data fusion in the monitoring of container traffic, including coordination with the intelligence community;
- Advancing effective international agreements for safeguarding the international trading system from the consequences of illicit trafficking in nuclear weapons and SNM.

This report attempts to provide at least preliminary solutions to these issues—particularly as they relate to maritime shipping of dangerous nuclear materials, with priority given to nuclear weapons and special nuclear materials.

III. Objective and Scope of Report

Objectives

- Develop an example of a technical "systems approach" to detecting nuclear weapons, special nuclear weapons material (SNM), and other radioactive material, in internationally shipped containers, that is feasible within the economic and political constraints of the international trading system;
- Lay out key criteria, features and cautions for a layered system reaching as far "upstream" in the chain of custody as needed to guarantee the security of the container contents; and
- Identify legislative and executive branch initiatives that will be helpful for the short term and within a longer time horizon, while also highlighting steps likely to prove counterproductive.

The objectives of the Container Security study were to:

Audience

The intended audience for this report includes policy makers, staff and researchers in the executive and legislative branches involved in designing and implementing the U.S. approach to preventing catastrophic terrorism against, or by means of, the system of international maritime shipping. More narrowly, the observations and recommendations contained in this report are directed toward groups carrying out Operation Safe Commerce, the U.S. Customs' Container Security Initiative, and other dedicated testing and evaluation programs.

Focus and Context of Study

Measures to improve the security of shipping containers and the international system of maritime transport make sense only as part of a more comprehensive strategy for protecting the

United States against nuclear and radiological terrorism. Such a strategy should include (but need not be limited to) the following four elements:

1. To prevent unauthorized acquisition of nuclear weapons, SNM, and radiological materials;
2. To deter at a system-wide level attempts to use these types of weapons if prevention fails;
3. To develop the means to detect and interdict illicit nuclear and radiological materials, i.e., defend the United States, if deterrence fails; and
4. To prepare for, and be able to respond effectively to the use of nuclear and radiological weapons against US targets.

The study group focused its efforts on detection and interdiction of dangerous nuclear materials in the system of maritime container shipping, with particular emphasis on nuclear weapons and SNM.

The emphasis on nuclear weapons and SNM was motivated by two considerations. First, a terrorist attack using a smuggled nuclear weapon, or an improvised nuclear device using illicitly acquired SNM, presents a far more dire, although less likely, threat than a non-nuclear terrorist attack using more common radioactive materials. Second, some types of SNM pose particularly challenging detection problems due to their comparatively low levels of radioactivity. With this caveat, the content of this report is in substantial measure applicable to broader efforts to detect many types of illicitly shipped dangerous radioactive materials.

The focus on maritime shipping was prompted by the observation that groups seeking to acquire a nuclear weapon or illicit SNM are more likely to conduct those activities overseas than inside the United States, where nuclear weapons and SNM are tightly controlled. Without appropriate safeguards, commercial shipping containers are an obvious mode for covert delivery of dangerous contraband, including heavy, bulky objects, such as fully assembled nuclear devices, or heavily shielded radioactive sources. Sufficient effort should be placed on improving container security to make this delivery mode relatively unattractive to any terrorist group that has managed to procure an assembled nuclear device, or SNM. A layered system offering opportunities to detect such a weapon *before* it enters a U.S. port would increase the security not just of the United States, but also of the international maritime commerce system, against the global disruption that detonation of a nuclear weapon in any major port would cause. In addition, a system for detecting smuggled nuclear weapons and SNM may also succeed in intercepting illicit radioactive materials contained in an RDD. Finally, such a system should be integrated into an overall architecture for protecting the United States form any form of nuclear and radiological terrorism, regardless of delivery mode.

Threat Scenarios and Overall Priorities

The following three threat scenarios underlie the analysis undertaken in this study:

1. Importation of an assembled nuclear weapon that could be detonated in a U.S. port, or at some inland point of transit;
2. Importation of SNM for assembly into a nuclear weapon within the United States.
3. Explosion of a radiological dispersal device (RDD) in a commercial port in order shut down port operations and jam international maritime traffic. [13]

[13] The group did not consider scenarios involving the importation of high explosives alone (a common ingredient for assembled nuclear weapons and RDDs), which involves very different control measures.

The study group concluded that preventing importation of an assembled nuclear weapon should receive the highest priority. Although this scenario is the least likely of the three *a priori*, the catastrophic nature of the consequences that would follow if carried out successfully warrant significant preventive efforts. Preventing the importation of SNM is a slightly lower priority because, even though it could lead to an outcome comparable to the importation of an assembled nuclear device, illegally transported special nuclear materials cannot be used immediately in an attack. The requirement for assembly within the United States offers further opportunities for law enforcement agencies inside the United States to detect and prevent a planned attack.[14]

The third threat scenario, illicit importation of an assembled RDD or radiological materials for use in a radiological dispersal devise (RDD), would have less catastrophic consequences if successfully carried out than either of the two scenarios just described. At the same time, detection of illicit radiological materials poses a different type of challenge to any screening system. In contrast to the close governmental and IAEA monitoring of all *legitimate* international transport of nuclear weapons and SNM, there is a significant legitimate international commercial trade in radioactive sources, and in products containing radioactive materials and components.[15] Therefore, the development of security systems capable of distinguishing quickly and efficiently legitimate from illicit radioactive cargo—possibly even within a single shipping container—constitutes a key technical design challenge. Meeting this challenge will be essential to avoiding unnecessary delays for legitimate shipments and for minimizing costly false alarm rates.

IV. Desirable System Characteristics

In this section, we suggest some universal criteria for evaluating the effectiveness of a security system designed to prevent nuclear terrorist attacks. Implications for system testing and deployment are likewise discussed where appropriate. We also note the desirability, when framing legislation and regulations, of distinguishing between short-term measures that may be needed to meet immediate problems, and more long-term steps toward an effective, robust, and affordable system that only experience can provide. We return to the latter topic later.

Cost Effectiveness

Estimates of the overall cost for the design and implementation of a security architecture for detecting illicit trafficking of nuclear materials must take into account both 'direct' and 'indirect' costs. Direct costs include equipment, real estate and operating costs over a specified system lifetime ("life-cycle cost"). Indirect costs include those associated with likely shipping delays caused by the security measures, or costs generated by widespread reorganization of contracting and insurance arrangements under a new set of rules.[16]

Direct and indirect system costs will be offset by expected savings in the form of more accurate shipping manifests, reduced theft, spoilage, and other sources of loss, to yield the "net system cost." As noted above, to be feasible from an economic perspective, the net system cost should not exceed a small fraction of the overall shipping costs, or, alternatively, a very small fraction of the value of the goods shipped. The final step in this process entails comparing the net system cost to the total expected social benefits of the system. The most important metric is the benefit from preventing, or reducing the likelihood of, a catastrophic terrorist event, although

[14] Unfortunately, a quantitative risk assessment of these threat scenarios was not possible due to data limitations.

[15] It follows that the guiding assumption in designing a system to prevent a nuclear terrorist attack on U.S. territory—that nuclear weapons and SNM are more easily acquired abroad—is less robust with regard to these types of radioactive materials.

[16] Note that each component of the system design is likely to entail a range of choices that require trade offs.

reduced contraband (e.g., drugs, small arms, and trafficking in humans) is clearly another social benefit.

The relative cost-effectiveness of different security systems must also be considered. Because some systems will be more effective than others in detecting specific forms of contraband, the outcome of this analysis depends in part upon the goals and requirements of the system in question. This is an issue of policy choice—not a technical issue. At the technical level, any proposed security architecture should be tested on a prototype basis during development to collect information on actual equipment costs and reliability, operating costs (i.e., personnel costs and shipping delays), and the false alarm rates experienced at each stage of inspection under normal operating conditions. Only then will it be possible to make informed comparisons between different systems and configurations.

Realistic Cost Allocation

The international trading system is comprised of manufacturers, port authorities, terminal operators, transportation companies (both local and international), security companies, together with local and national governments and participating agencies (e.g., customs and immigration), and consumers. The cost of any security system will be allocated among these various actors. If the net security system cost is small (a few percent of shipping costs, or a few tenths of a percent of the value of the goods shipped), it may, in many cases, be possible to pass those costs on to the consumer without noticeable effect. However, as the net costs of security increase relative to shipping costs this option may become exhausted, and the political and economic dilemmas of deciding where in the system those costs will be absorbed will become more difficult to resolve. For example, commercial shipping companies already operate within a very narrow margin of profitability, which means that they are unlikely to be able to absorb the costs of the proposed security system. How cost allocation issues are decided can have an effect on the effectiveness of system operations. For example, the greater the financial burden placed upon commercial operators, the greater their incentives to attempt to circumvent any system for detecting nuclear or radiological materials in order to obtain a competitive advantage. Again, time and limitations of expertise among members of the study group precluded a detailed evaluation of these issues.

Market forces can be expected to provide some parts of the needed response. For example, most of the passive and active scanning equipment in the system proposed in the next section is being produced commercially, albeit in many cases using technologies developed in partnership with government laboratories. Various firms have begun marketing technologies for intermittent or near-real-time tracking of the location and condition of individual containers**.** Bonded, private firms are likely to appear both in the United States and abroad to provide verification of container contents for "certified shipper" programs. In other areas, such as the construction and operation of an integrated international data network, it is unlikely (and indeed possibly undesirable) that private commercial operators would fulfill this requirement.

At the broadest level, ensuring that the system of international container traffic is secure against use by terrorists should be viewed as a public good and, therefore, appropriate for government action and support– particularly for countries that stand to lose a great deal from the disruption of the international trading system. Indeed, there are strong incentives for governments to cooperate with, if not subsidize, enhanced security measures, assuming they share a similar view of the threat. Even if they don't place nuclear terrorism as high on the list of threats as the US government, the public good of reduced contraband may provide a strong incentive to participate. Cooperative arrangements incorporating standards that are acceptable internationally will have to be established to identify shippers and ports that fail to adhere to specified security measures, and to establish procedures for managing such situations as they arise.

Robustness

Any proposed security architecture should be designed to degrade gracefully if performance at any level is compromised. Systems must be scrutinized for potential common-mode failures, *i.e.*, failures at one level that affect system performance at multiple levels simultaneously, thereby degrading system performance unexpectedly and often drastically. For example, large databases are subject to illicit intrusion. They should have smaller, local backups. The same is true of detection and communication equipment. Since every system component can be expected to fail at some time, efficient levels of redundancy, together with monitoring by human operators, are important to a robust system design. To ensure that security systems maintain a high level of robustness under many types of conditions, they should be subjected to mock attacks (i.e., "red teaming"), both simulated and actual field exercises.

To the greatest possible degree, the system should be designed to capitalize on existing alignments of incentives that favor compliance, and to identify those areas that will require greater degrees of monitoring and a more heavy-handed approach. In some cases, market discipline itself may provide adequate incentive—perhaps with some government subsidization—for industry actors to adopt and adhere to preferred security practices. In other contexts, the alignment of incentives may be achieved with targeted inducements—for example, faster processing of containers that meet "certified shipper" criteria. In still other areas, the threat of official sanctions—such as the loss of privileges to ship to U.S. ports—may be required to elicit desired responses.

Finally, any security system should be designed with enough flexibility to permit incorporation of new equipment and procedures during and after initial design and implementation. This feature is essential, since neither the threats posed by terrorist groups, nor the technology available to deal with those threats will remain static. At the same time, it is important to ensure that new vulnerabilities are not introduced in the course of attempting to eliminate existing vulnerabilities. Therefore, modifications to the system architecture should be undertaken with a view to their likely effect on the entire system.

Production of "Actionable Intelligence"

Another criterion of effective system design is that alarms in the system must be "actionable"—they must occur at points where the triggering containers can be identified, diverted from the regular flow, and handled appropriately. For example, hard intelligence information that a nuclear or radiological weapon has been loaded onto a ship headed for the United States in the current maritime security system is not at present "actionable" because there is no way to identify and track down the specific ship or container, or to know when or where it is scheduled to arrive. For instance, the container in question could be transferred to another ship at an intermediate port without the knowledge of US authorities. A US President facing this situation would have to invoke burdensome ad hoc inspections at all US ports of debarkation for an indefinite period of time to guarantee that the weapon does not arrive, thus substantially disrupting global trade.

By contrast, portal monitoring and improved tracking procedures under a future security system could detect the presence of the weapon before it is loaded onto a ship, thus allowing the appropriate authorities to take effective action. This includes, for example, tracking suspect ships and containers after they depart the port of embarkation for interdiction before they enter US territorial waters. In short, intelligence improvements in the international system of maritime transport should be geared toward producing alarms that are triggered at points in the system that will permit action that is both effective, and minimally disruptive to the system as a whole.

Realistic Assessment and Treatment of False Alarms

Under the proposed systems-approach to container security, when radioactivity is detected at any stage in the scanning and sensing process, further investigation is triggered to determine if illicit

nuclear or radiological material is present. False alarms (also called 'false positives' or 'Type II errors') are events that occur when personnel at one level of the security system erroneously believe that illicit nuclear material has been detected based on sensor responses or other information. The problem of false positives in the detection of radioactivity among commercial shipped goods is complicated by the widespread presence of background radiation, which in some cases mimics radiation from SNM, as well as the legitimate trade in materials with traceable radioactive signatures.

The number of false positives generated by a security system is an important factor in overall system cost. In general, adding layers to the inspection process can reduce the false alarm rate—particularly layers that attempt to detect nuclear material via different physical signatures. However, increasing system complexity also increases costs. As a suspect container advances to higher levels of scrutiny, more sophisticated imaging and sensing equipment is required, as well as more time to collect data, and additional expertise to interpret it reliably.

Determination of an acceptable overall system false alarm rate for detection of a nuclear weapon in a shipping container is both an economic question and a policy judgment.[17] However, the number should almost certainly be small—perhaps on the order of one or at most a few such events per year (at least in the beginning) somewhere within the international shipping system. Because the economic and political consequences associated with the highest level of response are quite serious, incentives will be very strong to ensure that false alarms are kept to an absolute minimum. False alarms at lower levels in the system can be tolerated more frequently, up to a point.

Another concern is the effect that false alarm rates and thresholds may have on the human components of the system. If the false alarm rate is determined to be too high at some stage of the process, operators may be tempted to modify or circumvent procedures or sensors that are perceived to be unreliable, thereby undermining the integrity of the entire system. Therefore, before a security system is deployed, it is critical to collect data to determine actual false alarm rates at various levels of the system under normal operating conditions. In addition, care should be taken to ensure that when alarms do occur using recommended procedures, that operator compliance with system procedures is not discouraged.

Compatibility With Existing Systems

To be effective, a container security system must be able to function in multiple contexts. It must be adaptable to variety of local conditions, including variance in the organization and physical layout of port operations, education and training levels of personnel, cultural habits, financial arrangements, and contracts governing shipping and delivery. In few if any contexts will it be feasible to construct a comprehensive security system from the ground up. Rather, components of the system will have to be implemented incrementally, particularly in major ports, to permit continuity of operations.

Adoption and implementation of many of the recommended technologies, such as X ray and gamma imagers, may be achieved relatively quickly, given their dual use in detecting contraband and reducing economic losses. However, many port facilities have extreme space constraints for increasing the number of scanning facilities and diversion areas, and this may limit how quickly adaptations can be achieved. Other aspects of the proposed system, such as certified shipping programs, and various types of data collection, can be initiated on a small scale, with the objective of eventually linking and standardizing the overall system using international "best practices."

[17] The lower immediate risks from contraband SNM imply that even high-level false positives pose a less serious problem than with assembled nuclear devices.

Political Feasibility

The sample layered security system presented in this document is designed to push the risk of a nuclear terrorist attack as far as possible from U.S. shores.[18] To achieve this goal, the system will have to serve the security needs not only of the United States, but those of all major participating countries—who will also wish to minimize their own risk becoming targets of nuclear terrorism. The particular form that the required international coordination and cooperation should take—be it an international convention, a series of bilateral agreements, or a formal international organization modeled on the IAEA—was not discussed in detail by the study group.

Any proposed security system must be acceptable domestically within major participating countries. Where local architectures and practices are a source of concern for security, international standards need to be clearly spelled out, and resources and expertise made available to help correct the problem. In the United States, among the debates that should be anticipated are those from unions regarding new labor practices at ports, resource allocation issues, and turf fighting between various federal agencies with responsibility for international commerce and counter-terrorism. Another traditionally sticky issue will involve determining rules and practices regarding the sharing of technology and potentially sensitive intelligence with foreign personnel.

Clear Lines of Oversight and Responsibility

As with any complex international security system, establishing clear lines of oversight and responsibility will require considerable coordination, time and effort. Above all, to prevent the lines of oversight and responsibility from becoming confused by bureaucratic compromises will require continued attention from the governments involved. The US government will have a major oversight role, in view of the US position as the world's largest importer, exporter, and possibly most likely terrorist target. Given that the US Department of Homeland Security has just been created, it is impossible to go into meaningful detail on this issue. However, it is very important that it be raised.

Auditability

Another important feature of system design is the question of who will audit overall system performance, and the performance of its component functions. Clearly, auditing requirements will differ considerably from container loading at certified shippers, to operation and maintenance of sensing equipment in foreign and domestic ports or on board cargo ships, to the integration and interpretation of collected data. In some cases, such as the handling of data, these functions are likely to be highly centralized. Other elements of the system, such as on-site monitoring and verification of container contents, have an unavoidably de-centralized character.

Auditing protocols and procedures will require tailoring to local conditions in individual countries to ensure compliance with internationally agreed standards. For example, certified shippers may be required to have security personnel to inspect goods before loading, two-man rules for sensitive inspections, standard equipment for monitoring radioactive emissions, standards for tags and seals, or controlled access areas for goods prior to loading. Standard training for security personnel and subsequent monitoring of a company's performance must also be agreed upon. The latter could be done through a central data repository that collects information about international shipping activities, but it would also require periodic onsite inspections to ensure these data are accurate.

Standards for detection equipment performance and maintenance must be set internationally to avoid incompatible detection capabilities at different ports. The calibration and proper functioning of this equipment must be periodically checked onsite by authorized personnel, possibly

[18] This is a common goal for most strategies aimed at securing international commerce. See Stephen Flynn, op. cit.

from an international team. The output of sensing equipment at port facilities and shipboard may also be remotely monitored using a central data repository. Red team exercises and surprise inspections that test the functioning of the security system at a facility are also possible, although these can be quite intrusive and, therefore, will be possible only with the cooperation of local governments and private companies.

V. Sample Technical Approach

In this section, we present an example of a technical "systems approach" to securing maritime container imports against SNM and other radioactive materials. Organizationally, the approach is separated into operations to be performed during the stages of transport illustrated in Figures 1 and 2. These operations can be usefully grouped into four site-specific stages or 'clusters', and one continuous system-wide function:

- Certification of the packing of individual containers;
- Security procedures at the port of embarkation;
- Continued monitoring after a containers have been loaded onto a ship and during transit;
- Security procedures at the port of debarkation;
- Continuous collection and fusion of data regarding the movement of individual shipments of goods in a computer system designed to fail gracefully under physical or cyber attack on some of its components.

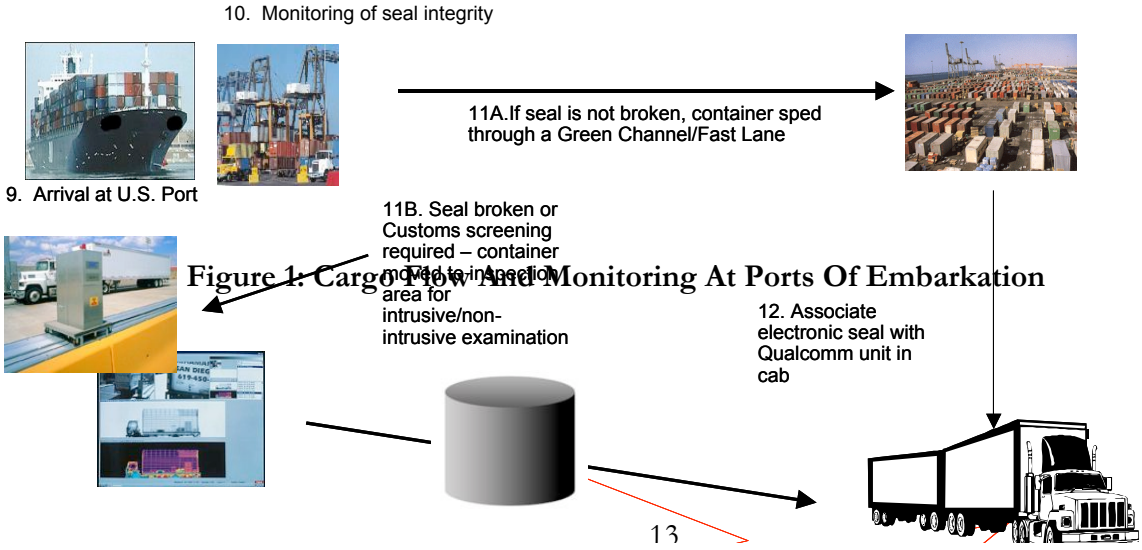

Figure 1: Cargo Flow And Monitoring At Ports Of Embarkation

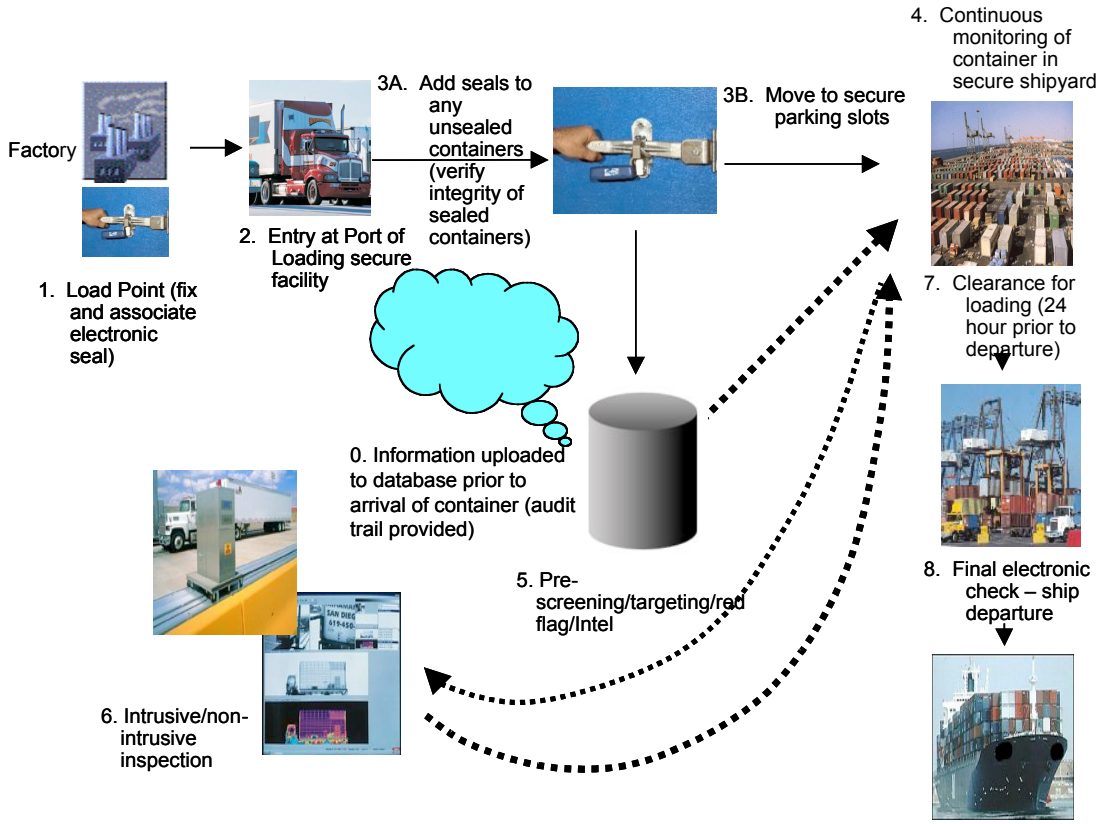

Figure 2: Cargo Flow And Monitoring At Ports Of Debarkation

We have been as specific as possible regarding the technologies to be utilized at each stage of the system. However, this report should in no way be construed as an endorsement of any particular manufacturer of commercial equipment. The purpose of this sample system is to show how a system can, with adequate and continuing monitoring, testing, and adjustment, be designed to meet the requirements outlined in the previous section. Time and experience will undoubtedly produce better systems.

Container Certification

The first stage of this process involves controls on the packing, sealing and storage of intermodal shipping containers until they are transported to the maritime port of embarkation (MPOE). Occasions for security lapses abound in the early stages of container transport, particularly in storage areas, where both time and opportunity to enter the containers can be plentiful. Where possible, security measures should be undertaken *before* individual containers reach choke points in the system where delay is costly or unacceptable.

As a rule, containers are filled either at the point of manufacture, or on the premises of freight consolidators. The standard practice is to close the container using a simple, inexpensive lock (unless the contents have some special value). Once locked, containers are seldom re-opened or inspected by officials. Instead, reliance is placed on information in the cargo manifest. The contents of individual containers are weight-limited, which means that there is often empty volume in the container where additional, non-declared cargo could be placed.

A system designed to prevent importation of dangerous nuclear material must begin by separating, to the maximum extent possible, "suspect" and "non-suspect" cargo and containers. Potentially relevant considerations include, the type of material involved, its point(s) of origin, and whether a trusted auditor has overseen the packing of the container. Wherever possible, the establishment of "certified shipper" programs is recommended as a first layer of security. Auditing by bonded, private companies whose business success depends on reliability is suggested, but government officials must be able to perform checks and audits of their own.[19] In most cases, this type of certification will be less expensive than wide use of more technologically sophisticated methods of verifying contents after the container is sealed.[20] The following are elements of our sample technical approach at certified shipper sites:

1. Manufacturers and consolidators adhering to security standards are established as certified shippers.
2. The shippers load containers using secure procedures and "certify" container contents.
3. Certified shippers must be audited regularly to ensure that accepted procedures are followed; existing pre-shipment inspection companies have the infrastructure to implement the audit process in the near term.

Once a container is inspected and certified, it is important to verify that its contents have not been altered or tampered with. The study group recommends development of a small, multi-purpose security device to be affixed to each individual shipping container. This electronic seal-tag, geo-locator, radiometric sensor, and communication device would:

- Add intrusion and radiation detection capability to existing devices;
- Monitor the position and security of the container throughout transfer;
- Be subject to theft, damage, and maintenance requirements; and
- Probably piggyback on increasingly adopted commercial tracking systems.

The proposed device would combine the functions of an electronic seal-tag that incorporates a small intrusion detector, a geo-locator, nuclear sensors, and a communication device. One must realize that "perfect" seals do not exist. All seals can be broken in time and protocols for seal inspection foiled. Therefore, any system for seal monitoring must include visual inspection in addition to automatic monitoring of seal integrity to minimize the chance that a container breach will go unnoticed. The geo-locator envisioned is not a complete GPS system, but would enable a central controller to determine the container location. The nuclear sensor would be passive, and would augment sensors operative at ports, and during shipboard transit.

The device should be designed and placed within the container so as to minimize opportunities for, and maximize detection of, theft and sabotage, including diversion and tampering during transport to the port of embarkation, as well as during any temporary storage period. It should never leave the container except for maintenance by approved personnel. In our judgment, the technology required is well within the state of the art, at a cost of between $100 and $200 per device. To give this figure some perspective, the cost of a single shipping container is approximately

[19] The procedures to be followed by certified shippers need to be negotiated and approved by all parties, and will differ in detail according to contexts and materials. For instance, an automobile shipper is likely to take steps to certify his shipment that differ from a shipper of clothing or refrigerated goods.

[20] Relative costs will depend on relative labor as well as relative equipment costs. Inspection of closed containers may be automated and thus require more expensive equipment but lower labor costs than inspection of contents during filling containers.

$8,000. Aside from the nuclear sensor, which is relatively cheap, all other elements of the device will have independent commercial value.[21]

Ports of Embarkation

Under current practices, individual shipping containers, with the possible exception of those packed with highly perishable cargo, often spend time waiting either at the point of origin, at way stations in the exporting country, or at the port of embarkation. Depending upon the port and the operators, waiting containers may or may not be kept in a monitored, guarded area. Under the proposed system, waiting time will be used to conduct a battery of differentiated screenings to detect undeclared nuclear and radiological materials. The three-tiered detection system suggested for ports of embarkation would include:

1. Gamma and neutron portal monitoring for all containers (designed to detect weapons-grade plutonium, weapons-grade uranium, and RDD materials);
2. Gamma radiography (e.g., VACIS) or X ray radiography for all non-certified containers, all certified containers that alarm portal nuclear monitors, and a certain percentage (yet to be specified) of certified containers that do not alarm portal monitors as a random check;
3. Isotope identifiers (handheld gamma spectroscopy) for passive inspection of high-density "suspect" regions in VACIS image; and
4. Active interrogation (e.g., PELAN-14 MeV neutron activation and thermal imaging) designed to identify shielded highly-enriched uranium for the small percentage of containers showing high-density anomalies.

At ports of embarkation, all containers destined for transport to the United States, or to other cooperating countries that join the system, will be subjected to passive gamma and neutron radiation monitoring before being loaded onto a ship (Stage 1). Such systems are already in place at some ports, as Figure 3 illustrates for the ports of Portsmouth and Dover in the United Kingdom.

Figure 3: Passive Gamma And Neutron Radiation Monitoring

All containers from which radioactivity has been detected will be subjected to a second inspection (Stage 2) involving active radiographic imaging with X rays or gamma rays.[22] An example

[21] As with all system elements, the recommended procedures and equipment characteristics, e.g., the false positive and false negative rates, must be ascertained during the test-bed programs.

of such an imaging system (the "VACIS" system built by SAIC) is shown in Figure 4. The left side of the boom arching over the containers in the figure houses a low-level gamma source while the right side contains two rows of sodium iodine detectors for imaging. An example of the radiographic image created by such imaging systems is shown in Figure 5, where the upper image illustrates a car being carried inside a truck and the lower image illustrates the same configuration with several dark objects clearly visible representing C-4 simulants.

Figure 4: Radiographic Imaging Devices

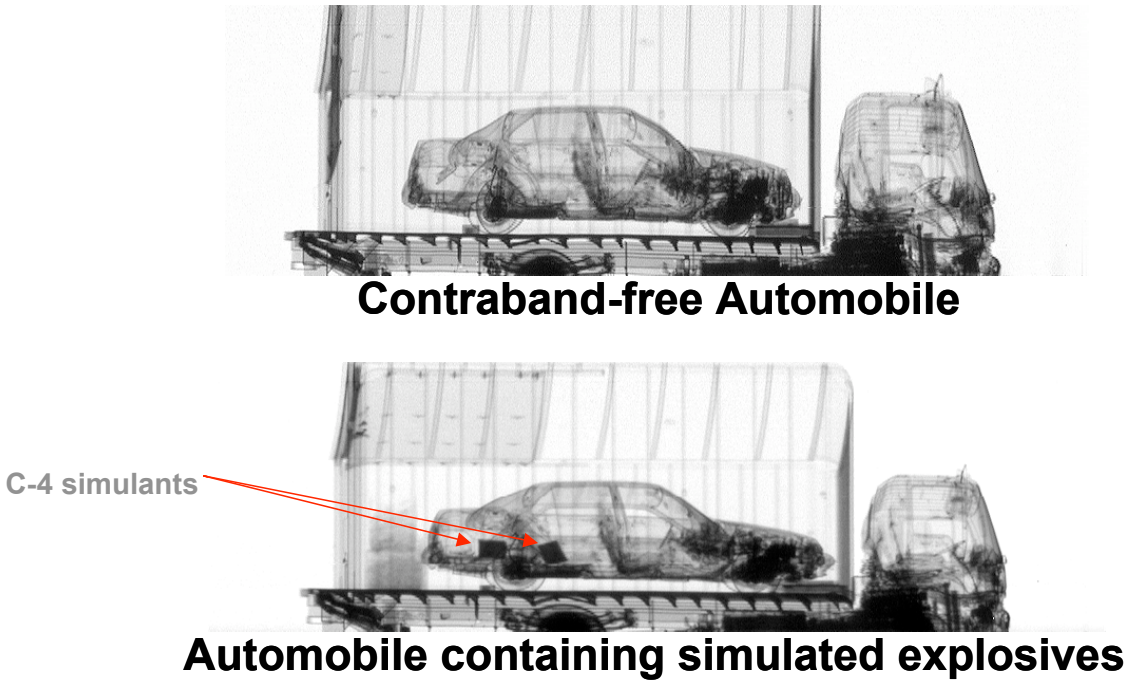

Figure 5: Example Of Radiographic Images

[22] Heavy shielding can be detected using gamma- or X ray radiography—an active measure that irradiates the contents of a closed container with a minimal dose (around 5 μrad—a minute fraction of the daily background dose of radiation received by humans).

The small percentage of containers that continue to be suspicious following stage 2 inspection will advance to a third stage in which more time-consuming and intrusive inspection of the container is conducted. For example, the container could be examined with a pulsed neutron source (see Figure 6) to look for the delayed gamma rays or neutrons associated with fissile materials, or the container could be opened, and the contents scanned for the presence of fissile material with a hand-held gamma ray spectrometer (see Figure 7). Or, a thermal imaging device could be used to detect the heat signature associated with an assembled nuclear device.[23] If, after a container passes through the entire system, security personnel still believe contraband nuclear material is present, higher authorities would be contacted. If a weapon is suspected, special Nuclear Emergency Search Teams (NEST) will be called in to locate, verify and disarm the weapon. During this process, the affected port will in all likelihood cease to operate, and precautionary evacuations of the surrounding areas may be appropriate.

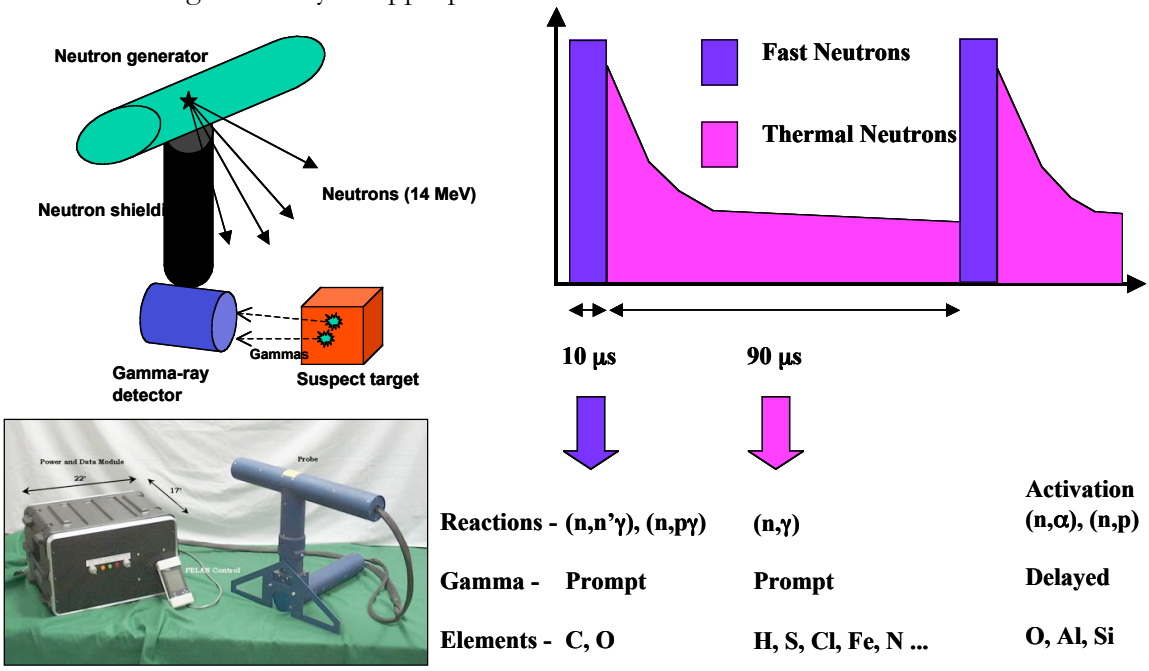

Figure 6: Pulsed Neutron Source To Detect Fissile Material

The proposed layering of technologies is intended to provide a comprehensive screening of container traffic with minimal delays imposed upon the vast bulk of containers passing through the system. Once radioactivity is detected, the system faces the problem of determining quickly and accurately whether its source is legitimate (and only legitimate) cargo. For example, ceramic materials and certain organic compounds emit detectable levels of radioactivity, and lead or other heavy metals will mimic the appearance of shielding on a gamma-ray or X ray scan. Unfortunately, it is not commercially practicable at present to subject the entire volume of international container traffic to the full battery of scanning and imaging technologies at the port of embarkation. Increasing the technical sophistication of scanning equipment brings higher equipment costs, and greater time

[23] There was some difference of opinion among members of the group with respect to the wisdom of allowing port officials to open suspect shipping containers in order to conduct gamma spectrometry and thermal imaging. The possibility of booby-traps or automatic detonation devices suggested, to some members, that only specially trained Nuclear Emergency Search Teams should ever open a container that is suspected of holding a nuclear device.

delays for measurements and interpretation.[24] Certifying shippers helps reduce the inspection load at all but the relatively rapid and cheap stage 1 inspection level. In addition, reliable information collected on individual containers as they advance through the system is important for targeting suspect containers apart from the results of the stage 1 passive radioactive measurements.[25] The layered inspection approach suggested here applies the more time consuming and costly inspections in stages 2 and 3 only to suspect containers tagged in the preceding stage.

- **Detects nuclear and radiological weapons**
- **Provides automatic detection and identification of over 30 radionuclides**
- **Eliminates need for periodic calibration**
- **Lightweight--less than 2 pounds**
- **Uses efficient gamma-ray detector (CsI with photodiode) which minimizes acquisition time**
- **Operates in survey and analysis (expert and non-expert) modes**

Figure 7: Handheld Gamma Radiation Spectrometer

How foolproof the proposed combination will be can only be determined by actual testing with "red teams" attempting to introduce various dangerous nuclear materials, simulated weapons, or their equivalents. The emphasis at this stage should be the detection of assembled nuclear weapons. Once a weapon is loaded onto a ship destined for a U.S. port, it could be detonated before inspection at the port of entry. Again, rates for both Type I errors (false negatives) and Type II errors (false positives) are important to testing system performance. Various combinations of equipment and staffing need to be tested for reliability and efficiency, and these results quantified by test-bed programs.

Transit

Once loaded, containers typically remain on the ship during transit to the United States, although some off-loading and reloading may occur at intermediate ports of call. In addition, some shuffling may occur to make room for other containers destined for earlier off-loading. From the point at which a container is loaded onto the ship, and throughout transit to the United States, operational priorities shift to conducting additional spot-checks using external sensors to detect radioactivity from container contents, monitoring location, detecting intrusion, further sensing nuclear radiation, and communicating information to a data fusion and control center.

The time needed for a container ship to cross an ocean should be viewed as an opportunity to include another stage of detection procedures. However, it was noted that the stacking of containers in tight blocks on board transport ships during loading might limit the ability of ship-mounted detectors to identify and pinpoint suspicious cargo. The group did not evaluate the dimensions of this difficulty quantitatively.

---

[24] Modern radiography, via fixed installations costing a few million dollars each, permits an accurate measurement of density differences, but at the cost of some minutes delay for interpretation. Of course, one installation could be teamed with several interpreters, but this would cause labor costs to rise.

[25] Tighter inspection and tracking procedures are already in place for high value and some time-sensitive shipments.

The multipurpose tamper-detection and radiometric monitoring device described above, and recommended for installation in each container will continue to fulfill the same functions aboard ship as during land transport. The long integration time during transit will improve the ability of the nuclear sensor component of the device to detect low-level radiation signatures. It is possible, for example, that small quantities of SNM that may have escaped detection at the port of embarkation could be detected during ocean transit. Appendix A details the relevant technical considerations. We have not made a quantitative estimate of the cost associated with the required sensors, nor have we analyzed the effect of the environment (shocks during loading and unloading, temperature fluctuations, etc.) on sensor performance.

Ports of Debarkation

At the U.S. port of debarkation, the proposed procedures for handling off-loaded containers will differ somewhat from those at port of embarkation. Although many of the same technologies are suggested, they will need to be applied in different configurations, and with somewhat different parameters and objectives. At the port of entry a more detailed inspection of suspect shipments is possible, since delays at this stage will not have the potential to affect thousands of non-suspect containers, as may be the case at the port of embarkation. Accordingly, more emphasis may be given to the detection of SNM (a tougher target than assembled nuclear weapons) at the port of debarkation.

In addition, information regarding the tracking and handling of individual containers will be available at the port of debarkation. This allows for more precise pinpointing of suspect cargo, including questionable shipments of radiological materials. The system will bring together data from the port of embarkation, the shipper (certified or not), the seal/tracking/radiation sensor device described above, the shipping manifest, and other intelligence sources. As with the POEs, our sample technical approach would require that all containers pass through nuclear portal monitors, that non-alarming containers are spot-checked by radiography and/or cleared to exit port, and that all alarming containers are inspected by radiography, and suspect anomalies are scanned with an isotope identifier and interrogated with active neutron interrogation.

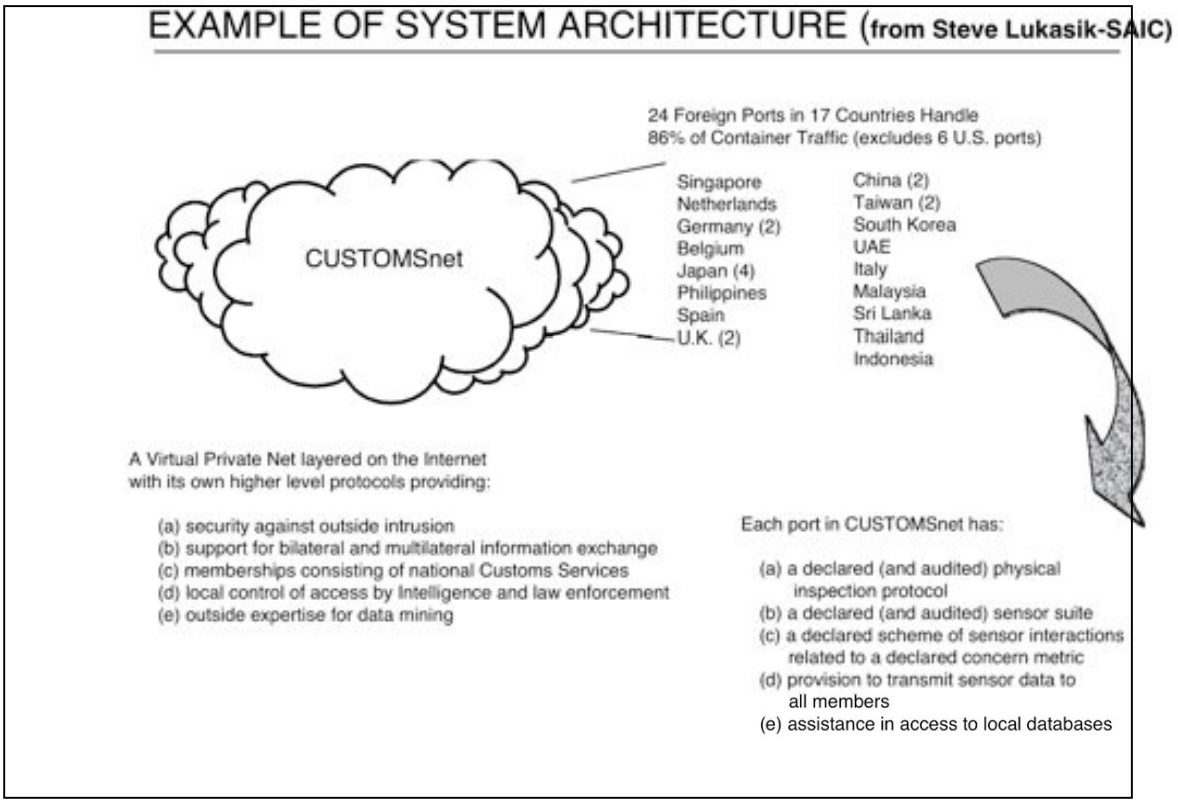

Figure 8: A Possible System Architecture For Data Fusion

Continuous Information Monitoring and Data Fusion

An information and data fusion system is an essential component of a comprehensive container security system. Only through continual operation and monitoring can suspect shipments be reliably identified, proper action taken, and system faults identified and corrected. One possible system architecture devised by Steve Lukasik is shown in Figure 8.

The data system would incorporate and fuse information from multiple human and technical sources, including:

- Sensor information (radiation levels, radiographs, etc.) wherever taken;
- Readouts from intrusion sensors and records of alarms;
- Cargo manifests;
- Inspection information;
- Information about original loading point, travel routes (verified to the extent possible by logs from the multi-function device attached to the container);
- Relevant intelligence information about shippers, other shipping agents, ports and countries involved; and
- Information gathered by human agents about deviations from normal shipping or other patterns.

Other desirable system features include compatible data storage for all categories of information, coupled with some level of real-time analysis incorporating data mining algorithms that will highlight problematic features of any particular container, and promptly retrievable archiving.

The goal of the information and data fusion component of the system is to help decision-makers in the United States pinpoint suspect containers, and, in extreme cases, to decide whether particular container ships should be prevented from entering U.S. territorial waters. Once established, the system will permit American officials to delay or detour suspect shipments, if such action is required. Finally, for the information produced by the system to be relevant, there must be appropriate connectivity to groups that may be expected to take action on the basis of the information gathered such as the Coast Guard, the Customs Service, the FBI, and others.

Again, only experience can demonstrate the full range of characteristics that will be required of an information system. Whatever information system is originally selected should remain highly adaptable throughout the testing and early deployment period, and should be reviewed regularly thereafter.

VI. Desirable Government Initiatives

Lead Government Technical Integrator

The federal government needs a lead technical integrator to coordinate nuclear container security initiatives. Depending on the final structure of the Department of Homeland Security, either it or the NNSA will be best equipped to assume this role. The leader should draw on related agencies, particularly the Defense Threat Reduction Agency and the Office of the White House Science Advisor. The leader should also participate in all interagency working groups addressing container security, at a high level. In addition to technical integration, this agency will fund analyses of the economic impact of various security architectures, including the conditions under which direct government subsidies become justified.

Technology Development Grants

Funds should be allocated for research and development of technologies for radiation detection, tamper detection, X ray and gamma-ray imaging, and information integration. Funds should be made available to applicants from academia, the national laboratories, and industry, and should be awarded by the new DHS in consultation with the Departments of Transportation, Commerce, and Energy. These grants should focus on exploring new technologies, lowering the cost of currently available technologies, and technology transfer.

Incentives for Cooperation between R&D, Test Beds, and Pilot Projects

Integrating technologies into the port environment will be essential. Close cooperation between R&D leaders and available pilot projects and test beds will ensure technologies are tested in realistic conditions during all stages of development. To encourage this, funds should be appropriated for the NNSA, DTRA, and other appropriate departments and agencies, to be used exclusively for expenses related to cooperation with test bed and pilot project facilities. Similarly, the US Customs Service, Coast Guard, and other appropriate departments and agencies, should receive funds to be used exclusively for expenses related to cooperation with groups developing nuclear security technologies.

International Standards for Container Inspection, Securing, Certification, Transport Monitoring, Data Handling and Storage, and Communication Systems

International standards will be essential for the effective functioning of a comprehensive container security system. Institutional participants should include:

- International Organization for Standardization (ISO), the standards bridge between public and private sectors;

- International Maritime Organization (IMO), the UN agency responsible for improving maritime safety and for technical cooperation; and
- International Atomic Energy Agency (IAEA), which should be the lead technical participant in the system.

The U.S. Government should give a single organization responsibility for surveying ongoing international efforts in this area, and for initiating negotiations as early as possible to establish appropriate standards and to develop protocols for authoritative action in the above areas, or in any other area needed for secure shipping.

International Test Bed

The US government should commit funds, in cooperation with other governments and entities, to establish an international test bed for nuclear container security. While pilot projects at individual foreign ports are important, an integrated test be will be essential in troubleshooting proposed systems and technologies and in training workers.

VII. Conclusions and Recommendations

The goal of the system outlined in this report is to improve international supply chain security from the point of containerization to the final port of debarkation within the United States, with minimal interference with flows of legitimate international commerce. Our study of these issues reached the following conclusions:

1. Rigorous testing of any candidate system is essential and should be continued during deployment and in the field.

2. The robustness of the system should be reviewed against the near-certainty that important elements would fail, either during normal operation or due to attack. The objective should be to ensure that elements of the system degrade "gracefully," and not in ways that significantly impair the overall performance of the system. In particular, data systems should be reviewed for their degradation characteristics against intrusion and under various forms of electronic attack.

3. Each element of the system should be designed to generate "actionable intelligence." The technical aspects of this challenge must be considered in tandem with potential economic, legal and political implications of diverting suspect containers from normal traffic or, in extreme situations, halting traffic altogether. Barriers to coordination among the agencies involved, both within the U.S. government and across national boundaries, should not be ignored or minimized.

4. International agreements to coordinate standards and to develop protocols for authoritative action will be essential. A suitable institution with membership that includes the majority of trading states should follow the testing programs and prepare options for such agreements.

5. Plans for system implementation at specific ports should be analyzed for their likely effects on labor agreements, business contracts, insurance liability, etc. Labor disputes resulting in port stoppages should be analyzed for their effects on global flows of goods, and for their wider economic impact. In this regard, insight could be gleaned from an analysis of the economic impact of the 11-day shutdown of 29 ports on the west coast of the United States due to a labor dispute during September and October 2002.

6. Longer-term research and development objectives should be identified and budgeted for, even though deployment of a security system to improve security in the short term is possible using available technologies and equipment. Forward-looking research and

development should be carried out under the supervision of an agency tasked with evolving a comprehensive transportation security system and should not be fragmented according to specific modes of transportation.

Appendix A: Analyzing System Performance With A Simple Queuing Model

This appendix describes a simple queuing system to model the flow of cargo containers through two sequential detection stations (with possibly multiple parallel detection machines at each station). The model can be used to examine the impact of parametric changes on system performance. The following metrics will be computed from the model:

- Time required to inspect a ship-load of containers
- Equipment utilization
- System bottleneck: the probability that certain equipment is idle because of congestion

Modeling environment:

The inspection system at a port is assumed to consist of two layers: a passive neutron or gamma ray detection system (stage 1) and an active X ray or gamma ray radiographic imaging system (stage 2). Containers come in two types: those from certified shippers and those from other shippers. The criteria for a container to earn a "certified" label are discussed in the main body of this report. All containers pass through stage 1. All non-certified containers also pass through the stage 2 inspection, along with any certified container that does not pass the passive detection layer according to some pre-specified selection criteria. Of the certified containers that pass stage 1, a randomly selected fraction are also imaged in stage 2. Containers subject to stage 2 scanning will proceed to an available radiographic machine. If no radiographic machine is available, the container will wait in a holding area. If the holding area is full, the container stays at its current location (meaning that a passive neutron/gamma detection machine will remain idle). The scan time at stage 2 depends on container label and the result of stage 1 examination but is generally around 5-10 minutes. The detection time for stage 1 inspection is on the order of 10 seconds. After completion of stage 2 scanning, the container will exit from our system (our model boundary). Additional search/examination after stage 2 is outside the scope of this simple model. It is assumed that an alert will be issued and other procedures will be followed should the test results warrant it.

Input parameters:

Physical parameters:

n: the number of containers to be examined
N(pd): the number of passive detection machines available at stage 1
N(rs): the number of radiographic scanner available at stage 2
K: the holding capacity immediately before stage 2 stations

Design (or soft) parameters:

F(c): fraction of containers that are certified
PC(pass): probability that a certified container passes stage 1 test
PN(pass): probability that a non-certified container passes stage 1 test
FE(c): % of certified containers (passing stage 1 test) exempted from stage 2 scanning
FE(n): % of non-certified containers (passing stage 1 test) exempted from stage 2 scanning
(The notional container screening system discussed in this report assumes FE(n) is zero)

Processing time parameters: processing time at various stages will depend on container status (certified or not, passing or failing stage 1 test). Longer processing time may be desired if a container fails stage 1 test and/or that it is non-certified.

T1: processing time for each container at stage 1
T2(c-p): stage 2 processing time for a certified container passing stage 1 test
T2(c-f): stage 2 processing time for a certified container failing stage 1 test

T2(n-p): stage 2 processing time for a non-certified container passing stage 1 test
T2(n-f): stage 2 processing time for a non-certified container failing stage 1 test

What is the model?

A queuing model requires three input elements:

1. The arrival process: how often and how random are the arrivals of "customers" (containers) to the queuing system;
2. The service process: how many "servers" (detection/scanning machines) are available, how long is the processing time to "serve" each customer"; and
3. The service discipline/configuration: how are customers "selected" to be served, how many holding spaces are configured if all servers are busy.

The situation we are considering does not suggest itself as a "ready-made" queuing system: all the n containers are immediately available to be examined, thus making the arrival process a bit tricky to model.

Modeling the "arrival" process:

We model the "output" from stage 1 as the arrival process feeding into stage 2, which will derive its randomness (of inter-arrival time) from the variability of the service process at stage 1. Some of the containers leaving stage 1 will exit the system (those which are exempted from stage 2 examination), which will modify (reducing) the "arrival" rate into stage 2. The numbers of machines at stage 1 will also determine the "output" from stage 1, thus the arrival rate into stage 2.

The service process:

The service time can be determined from (1) the percentage of containers of different classifications (certified or not, pass/fail from stage 1), and (2) the service time specified from system design for different classifications.

The service configuration:

The number of holding spaces in front of stage 2. More holding spaces will reduce the probability that stage 1 machine(s) is blocked from working (container completing stage 1 examination cannot leave).

The computation:

With the above specifications, we model our queuing system (very crudely to provide rule-of-thumb insight) as a simple M/M/a/b queuing model. The first two specifications (M/M) assume a Markovian model for both the arrival as well as service processes (Poisson arrivals and exponential service time), which we recognize as a simplifying assumption. The parameter "a" specifies the number of scanners at stage 2, while "b" represents the number of holding spaces. A simple spreadsheet model is constructed to compute the probability that the system is in various "states." In this simple model, a state is defined as the number of containers at stage 2, those being scanned plus those waiting in the holding area. Once the probabilities are computed, we can compute the metrics as specified earlier.

First order sensitivity considerations:

Table A1 provides qualitative impact of system metrics (columns) when we change the value of system parameters (rows). A "plus" sign in the matrix indicates that an increase in the system parameter will result in an increase in the corresponding metric. A "minus" sign indicates the opposite effect. The exact magnitude of the change depends on the preset values of the other system parameters.

Table A1: Qualitative Model Response Matrix

	Processing time for all containers	Utilization of stage 2 machines	Blocking probability when all stage 2 machines are busy
# of containers	+	+	+
# of stage 1 machines	-	+	+
# of stage 2 machines	-	-	-
Holding capacity	-	+	-
Certified containers %	-	-	-
Prob (C-containers pass stage 1)	-	-	-
Prob(NC-containers pass stage 1)	-	-	-
% of C-P containers exempted	-	-	-
% of NC-P containers exempted	-	-	-
T1: stage 1 time	+	-	-
T2(C-P): stage 2 time	+	+	+
T2(C-F): stage 2 time	+	+	+
T2(NC-P): stage 2 time	+	+	+
T2(NC-F): stage 2 time	+	+	+

Container classification: C: Certified, NC: Non-Certified, P: Passing stage 1, F: Failing stage 1

Other considerations

There are two types of false alarms:

- False positive: a container is declared a "fail" after stage 2, but that it is a false alarm. False positive creates major disruption in port operation. The exact degree of disruption depends on the designed response, which is outside the scope of this appendix. Such disruption imposes economic cost as well as psychological harm. It may also induce indifferences when the next alert arrives. Therefore, it is desirable to reduce the frequency of its occurrence.
- False negative: a container passes all inspection to leave the system when, in fact, it contains materials we intend to detect. The cost of such event is obvious. Thus, we should minimize the probability of such occurrences.

We can decrease the occurrence probability of these undesirable events by increasing the processing time at both stages. More careful and deliberate attention at both detection/scanning stages provides better discrimination between the presence and absence of the materials we intend to detect. However, increasing container inspection time at the two stages will contribute to the increase in overall processing time of a shipload of containers, as indicated in the table above. Table A2 provides a sample strategy to maintain an acceptable level of false alarms while keeping the processing time of a container ship constant. This will obviously result in additional cost in equipment: a tradeoff to be made in the overall system design process. A "plus" entry means an increase in the associate system parameter.

Test Bed:

In order to understand the relationship between false alarm and processing time, we need extensive testing to collect reliable and robust statistical data: how to design an optimal test procedure (minimizing alarm rates with a constant inspection time) and how to determine test sensitivity level to declare whether a container passes or fails inspection. Obviously, a decision to pass or fail a container entails a tradeoff between false positive and false negative event occurrences. A stringent pass criterion will decrease the likelihood of false negative events while increase that for false positive events. A more lax pass criterion will have the reverse effect. Therefore, a careful

tradeoff analysis will need to be performed. Our main report contains a discussion of the need for rigorous experimentation.

Table A2: A Sample Strategy To Minimize False Alarms

	Lowering the level of false alarms while keeping in check system processing time
No. of stage 1 machines	+
No. of stage 2 machines	+
Holding capacity	+
% of C-P containers exempted	-
% of N containers exempted	-
T1: stage 1 time	+
T2(C-P): stage 2 time	+
T2(C-F): stage 2 time	+
T2(N-P): stage 2 time	+
T2(N-F): stage 2 time	+

Container classification: C=Certified, N=Non-certified, P=Passing stage 1, F=Failing stage 1

Optimization:

An interactive optimization approach can be designed to consider and balance the tradeoff amongst various system metrics in the search for a set of optimal system parameters. The tradeoff has to be made between cost, time and false alarm rates. We suggest an interactive optimization platform so that a decision-maker can make intelligent tradeoff when the help of computerized decision support system. Such a decision support system will also allow for the evolutionary design of the monitoring system when new technology emerges or when new tradeoff has to be made. An interactive decision support system also allows an individual port to set its own criteria or to react to emergency situation (e.g., when new intelligence information indicates a high likelihood of smuggled radioactive contraband materials). Another use of an interactive optimization system is to evaluate the impact of policy changes: how desirable is it to increase the percentage of certified shippers? A well-designed system should allow sensitivity analysis of a combination of external as well as internal factors.

Full-scale analysis:

A more detailed and accurate analytical model is needed to examine the interaction of all the system parameters with greater fidelity. Another approach is the development of a full-blown simulation model to follow the flows of containers through the detection system. Such an effort is under way at the Los Alamos National Laboratory. In the mean time, analytical modeling should provide valuable insight and guidelines as we move towards the evolutionary design of such an inspection system.

Conclusion

We have created a simple queuing model to examine the first order impact of various system metrics when the system parameters are changed. The value of this simple model is to identify critical elements of the system to be isolated for more in-depth examination. More detailed system modeling and analysis is essential in the design of a real inspection system.

RADIATION LITMUS PAPER

Deidre M. Johns, Joseph A. D'Alessio, Kimberly S. Sheafe, and Benjamin P. Warner
Chemistry Division, Los Alamos National Laboratory
Los Alamos, NM, 87545, USA
(505) 665-6962
warner@lanl.gov

SUMMARY
We have developed a colorimetric method for measuring doses of ionizing radiation at low (10^{-4}-10^{-2} Gy) levels. This method uses photographic film as the sensor and amplification method, coupled with developers that are extremely non-fogging and tolerant of acidic conditions, and a pH indicator. The reaction is packaged so that the film can remain unactivated by ambient light while the developer and pH indicator can migrate to a viewing window. The result is a self-developing film badge that provides real-time dose information. This device, called Radiation Litmus Paper (Figure 1), is modeled after the M256A1 Chemical Test Kit (Figure 2) which is manufactured by Anachemia and used by the US military as well as state and local first responders.

Figure 1. Field prototype of Radiation Litmus Paper.

I. BACKGROUND

Colorimetric radiation dosimetry has historically been limited to high dose measurements. Examples include the liquid-phase US Army Tactical Dosimeter, which measures doses from 0.5 Gy to 4.5 Gy; liquid phase Fricke dosimeters that measure approximately from 10 Gy to 500 Gy; and several solid phase systems intended for measuring food irradiation efficiencies.

Low dose colorimetric measurement is difficult to achieve because of the large difference between the number of molecules of a colorant that may be produced by, for example, a 0.1 Gy radiation dose and the number of molecules needed for observation by the human eye. This difference is often a factor of 10^4-10^5. This gap can be partially bridged by using halocarbons as radical chain carriers, but realistic efficiencies of these chain reactions is only a factor of 10-100.

Figure 2. Anachemia M256A1 Chemical Test Kit.

II. APPROACH

Amplifications significantly greater than those provided by halocarbons are required to allow a colorimetric dosimeter that measures doses on the order of 10^{-4} Gy. Photographic film provides the required amplification as well as the required environmental stability. However, film is sensitive to light, and therefore cannot be directly observed without contaminating the results. The reactions that govern photography and radiography are shown in equations 1-5.

$$(AgBr)_{n+m} + RH \rightarrow \text{no reaction} \quad (1)$$

$$(AgBr)_{n+m} + RH + \text{time} \rightarrow \text{fogging} \quad (2)$$

$$(AgBr)_{n+m} + \text{radiation} \rightarrow (AgBr)_n Ag_m + Br^{\bullet} \quad (3)$$

$$(AgBr)_n Ag_m + RH \rightarrow Ag_{n+m} + HBr + R \quad (4)$$

$$Base + HBr \rightarrow BaseH^+ + Br^- \quad (5)$$

Equations 1 and 2 describe the reaction between unexposed film and developer. Equation 1 shows the desired lack of reaction between unexposed film [$(AgBr)_{n+m}$] and a developer [RH]. Typically, n is 10^7-10^9 and m at least 4. Unwanted fogging, which is the thermally activated reduction of silver bromide by a developer, will occur in time, as shown in equation 2.

Equation 3 describes the reaction of a grain of silver bromide with light or ionizing radiation. A small amount of Ag(I) is photoreduced to Ag(0), and the corresponding (but inconsequential from a chemistry perspective) amount of bromine reacts with the gelatin matrix.

In equation 4, the photoreduced silver forms a catalytic spot [Ag_m] on the grain of film [$(AgBr)_n$] that promotes the reaction of the grain of silver bromide and the developer. The products of the reaction are the oxidized form of the developer [R] and acid [HBr].

The acid is reacted with a base, as shown in equation 5. This step is required for most developers, because their activity is seriously attenuated by acid.

Equation 4 forms the basis of photographic images. The reduced silver is used in black-and-white photographs, and the oxidized developer can be reacted to form dyes for color photography. To use these reactions for real-time radiation dosimetry, we had to modify several of the reactions described above. Equation 2 had to be dramatically suppressed, so that it occurred only after tens of hours rather than several minutes. Equation 4 offered a possible colorimetric signal, if the developer changed color when it was oxidized and did not become anchored into the gelatin matrix. The acid-base reaction in equation 5 also offered a colorimetric signal if the base were a pH indicator.

Our approach, therefore, was to design a system where the film would be kept in a light-proof container with a channel that allowed a solution of pH indicator and developer to contact it. The developer/pH indicator solution would be kept in a transparent container, so that the extent of the reaction could be monitored by simple visual inspection. Liquid-phase reagents (developer, pH indicator) and products (oxidized developer, protonated pH indicator) could travel back and forth between the transparent and opaque portions of the dosimeter, while solid-phase materials (film, reduced silver) could not.

The principal chemistry research that was required was to design a developer that did not lead to rapid fogging (equation 2), that was active at neutral pH levels (to allow maximum sensitivity), and that changed color when oxidized. Fe(II) coordination compounds offered these properties.

III. MEASURED DATA

Devices were constructed using Kodak NTB-2 or NTB-3 autoradiography gel as the film source. A solution of Fe(II)EGTA and a pH indicator (typically phenol red, although many indicators worked), with the pH adjusted to just basic of the indicator point. The devices were irradiated with a 5 mCi ^{137}Cs source, and visually examined periodically until the color was judged to have unambiguously changed from red to yellow. The devices also provided intermediate colors that corresponded to measurements of lower doses, but we wanted to avoid the need for fine judgement calls in general. The dosimeter was also tested with AmBe neutrons and ^{90}Sr beta radiation, although no calibrations were performed.

Several factors could control the performance of a Radiation Litmus Paper device. These factors include the volume of the developer/pH indicator solution, the concentration of the pH indicator, the surface area of the film, and the film speed.

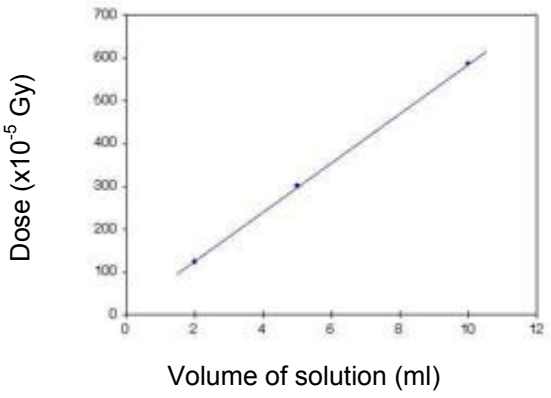

Figure 3. Sensitivity of Radiation Litmus Paper as a function of the volume of the developer/pH indicator solution.

Figure 3 shows the effect of changing the volume of the developer/indicator solution. These tests

were carried out with 0.3 mL of Kodak NTB-3 autoradiography gel with a surface area of 2.27 cm^2. An Fe(II)(EGTA) developer solution with phenol red pH indicator was used. The sensitivity of the devices varied inversely with the volume. The reason for this behavior is that the color changes with acid concentration. Acid is generated by the reactions listed above in equation 4. By varying the amount of water in which the acid is dissolved, we could control the change in pH.

Figure 4 shows the dependence of the devices on the surface area of the silver bromide emulsion. This curve consists of data from devices made with Kodak NTB-3 autoradiography gel (varying amounts), 5 mL of a Fe(II)EDTA/phenol red solution made with a higher concentration of phenol red (upper line) and a lower concentration of phenol red (lower line). This curve shows several dependencies.

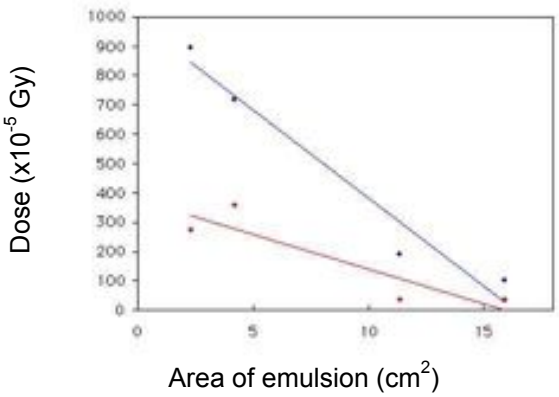

Figure 4. Sensitivity of Radiation Litmus Paper as a function of the area of the silver bromide emulsion and as a function of the pH indicator concentration.

The first dependence is that of the device sensitivity on the surface area of the silver bromide emulsion. A larger sensor clearly will collect more radiation than a smaller one. Capture efficiency is low, and therefore one might expect that the volume of silver bromide would be proportional to surface area. This is not, however, the case. Experimentally, we determined that the sensitivity varied unpredictably with the volume of the silver bromide emulsion at low volumes, but became invariant at higher volumes. By dismantling devices, we found that at low emulsion volumes, our surface areas were irreproducible. At higher silver bromide emulsion volumes we did completely cover the intended areas. However, the developer would only penetrate a small distance into the silver bromide emulsion. We therefore found that the volume of silver bromide that had any effect was determined by the surface area (which we could control) times the developer penetration depth (which we could not affect). We therefore decided to report surface area. We found that we could increase sensitivity by placing channels in the silver bromide emulsion, which allowed greater developer penetration. However, these channels were difficult to reproduce reliably.

The second dependence shown in figure 4 is on indicator concentration. Higher indicator concentrations make the color change more intense, but require more acid to protonate the indicator. Lower indicator concentrations make the color change more faint, but allow for more sensitive devices.

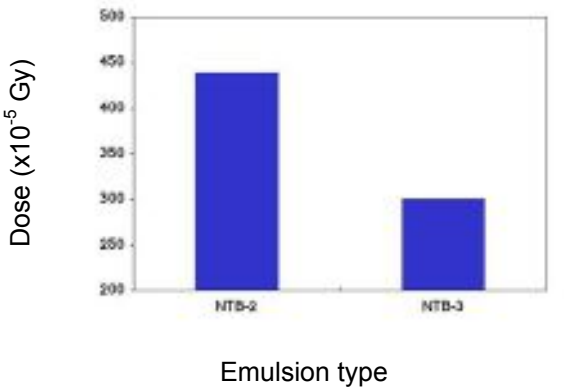

Figure 5. Sensitivity of Radiation Litmus Paper as a function of the area of the silver bromide emulsion and as a function of the pH indicator concentration.

Figure 5 shows the dependence of the devices on the grain size of the silver bromide. These experiments were carried out with 2.27 cm^2 surface area of Kodak NTB-2 and NTB-3 autoradiography emulsion, and 5 mL of Fe(II)(EGTA) developer with dilute phenol red indicator. NTB-2 has an average silver bromide grain size of 0.26 microns, and NTB-3 has an average silver bromide grain size of 0.34 microns. Both grain sizes only require 3-4 atoms of metallic silver to become activated, but the larger NTB-3 grains have approximately 2.2 times the silver bromide. Experimentally, the NTB-2 devices were 1.5 time less sensitive than the NTB-3.

IV. PROBLEMS

The principal problem we encountered was the difficulty of making Radiation Litmus Paper devices for testing. The devices were time-consuming to build, because they had to be constructed by hand in a darkroom. We constructed them typically 20 at a time. The principal difficulty was that if there were a light leak, the device would register a false positive. Light leaks could be discerned by destructively examining the emulsion after a device was tested. A functional device would show an even pattern of developed silver, while a light leak would produce a spot or stripe of heavily developed silver in an otherwise undeveloped emulsion. We believe that these problems are solely a function of hand construction, and that Radiation Litmus Paper is ready for mass production.

V. CONCLUSIONS

By using well-established film chemistry to provide the amplification needed to see a low dose of ionizing radiation, we were able to construct the first low dose colorimetric method for measuring ionizing radiation. Radiation Litmus Paper is intended to function as a simple method for ascertaining possible danger from ionizing radiation for "first responders." It is intended to operate similar to the M256A1 chemical test kit currently used by the US military as well as state and local officials.

ACKNOWLEDGMENTS

Funding was provided by the NNSA NA-22 Proliferation Deterrence Program.

NUCLEAR AND RADIOLOGICAL TERRORISM THREATS FOR INDIA: RISK POTENTIAL AND COUNTERMEASURES

Rajesh M. Basrur

Director, Centre for Global Studies,
5/157 "Bhagyalaxmi"
Sir Bhalchandra Road, Dadar,
Mumbai 400 014
India

Tel: 91-22-2414-3500
e-mail: rmbasrur@hotmail.com

and

Friedrich Steinhäusler

Professor, Institute of Physics and Biophysics
University of Salzburg
Hellbrunnerstr. 34
A-5020 Salzburg
Austria

Tel: +43-662-8044-5701
e-mail: friedrich.steinhaeusler@sbg.ac.at

NUCLEAR AND RADIOLOGICAL TERRORISM THREATS FOR INDIA: RISK POTENTIAL AND COUNTERMEASURES

1. Introduction

In an era characterized by the rising threat of indiscriminate terrorism and the diffusion of instruments of mass destruction, the possibility of nuclear/radiological terrorism, though yet unrealized to a significant degree, is a grave one (Leventhal & Alexander, 1986; Cameron, 1999). India is particularly vulnerable to such threats owing to the wide distribution of nuclear/radiological material and concurrent threats from numerous terrorist groups. Few studies have attempted to gauge the extent of the problem (Leventhal & Chellaney, 1988; Basrur & Rizvi, 2003). In this paper, we attempt to identify possible threat scenarios arising from nuclear/radiological terrorism, the sources of threat, and countermeasures to combat the threat.

2. Terrorist threat scenarios in India

2.1 Radiological terrorism

One of the possible malevolent acts involving radioactive material is its dispersion during an act of terrorism, using a *Radiological Dispersal Device (RDD)*. Such a radiological weapon can be deployed in several manners (e.g., dispersion of radioactive aerosol; detonating radioactive material with conventional explosives ("dirty bomb")).

In addition, diverted strong radioactive sources can also be used to maim or kill a victim by covertly exposing the individual to ionizing radiation for extended periods of time.

Once terrorists have obtained radioactive material, they still have to fulfill several logistical requirements before they actually carry out an act of radiological terrorism, such as: knowledge about the targeted facility; provision of adequate manpower and vehicels to transport the source; access to tools for dismantling the source.

These kinds of attacks would result in a wide range of radiation doses to the victims and First Responders (police, paramedics, and firefighters), though in most cases unlikely to be life-threatening. However, it is questionable whether initially Indian authorities would even be aware of the fact that a terror act involving radioactive materials has occurred, since most first responders are neither trained, nor technically equipped to detect the presence of radiation at the site of a terror attack. It is safe to presume that terrorists in India would have to inform the media first about the deployment of radioactive material in order to achieve the desired level of panic among the general public.

In summary, the impact of a radiological terrorist attack on Indian society will be largely due to mass panic rather than radiation-induced health effects, since the individual radiation doses are likely to be too small to cause acute or somatic radiation syndromes.

However, there will be significant environmental clean-up costs and indirect economic damages, such as devaluation of urban property value and loss of agricultural market share due to stigmatization of the contaminated target area, even after successful clean-up operations.

2.2 Terrorist attacks on the nuclear infrastructure in India

India's nuclear establishment, most of it civilian, is large (Gopalakrishnan, 2002). Despite a high level of security and inherent safety features, there are several security risks for Indian nuclear power plants (NPPs) from terrorists, such as:

- A small team of trained saboteurs gains access to an NPP, possibly with an insider's assistance, and detonates explosives at sensitive points to cause a release of radioactivity; or
- A convoy of suicide truck bombers crashes through the weakest point of entry of an NPP (usually the entry gate for transport), with the surviving truck(s) attacking vital installations of the NPP; or
- A suicide commando hijacks a fully fuelled large civilian aircraft and crashes it into the spent fuel storage pool of the NPP.

The attack mode entailing truck bombs is generally accepted, acknowledging that even a large conventional bomb detonated *outside* the fence barriers surrounding an NPP might cause "unacceptable damage to vital reactor systems", potentially resulting in an uncontrolled, major release of radioactivity (Sandia National Laboratories, 1984).

The degree of vulnerability of an NPP to air attacks is subject of intense investigation worldwide at present. Preliminary results range from affirming that aircraft crashes may result in multiple-failure initiating events ("Massachusetts Congressman Says Nuclear Plants Are Vulnerable," 2002), to negating that a commercial, fully fuelled large airliner could penetrate an NPP and release radioactivity (Nuclear Energy Institute, 2002), or cause a major disaster ("The Canadian Nuclear FAQ – Section D," n.d.b). However, it is not known what effect an aircraft loaded with high explosives might have if it crashes into a typical Indian reactor building. The two VVER-1000 type plants being built by Russia at Koodankulam in the southern Indian state of Tamil Nadu may be inherently vulnerable to an airliner crash. Weaknesses of existing plants of this type include the inadequate strength of walls and roof, the location of the control room at the lower levels of the reactor building (necessitating early evacuation in case of melt-through of the containment), and close proximity of steam lines and isolation valves, creating vulnerability to a single blast (Hirsch, H, 2001).

Besides an attack on the reactor building of an NPP, it is necessary to consider also the consequences of an aerial terrorist attack on the spent fuel storage pool. In India, these facilities typically have strong concrete walls with steel liners to protect against leaks. However, usually the roof structure is not hardened and thereby vulnerable to an aircraft crashing into the storage area. Such pools hold on average up to ten times more long-lived radioactivity than a reactor core. Provided the aircaft crash results in a loss of coolant from the pool and cannot be replced in time, this would expose the fuel elements

to the ambient environment, i.e. a mixture of burning jet fuel, air and steam. If the cooling water - acting as a radiation shield - dropped to about 1 meter above the spent fuel rods, this would result in an excessively high radiation dose for an intervention team, inhibiting them to replenish the coolant in time. Once the fuel rods are exposed to steam and air, the zirconium cladding of the fuel elements would react exothermically with temperatures of about 1,000 degrees C, resulting in a fire and releasing large amounts of radioactivity into the environment.

2.3 Nuclear Weapons, Terrorism, and Inter-State Conflict

One aspect that has received inadequate attention is the relationship between terrorism and the regional politics of nuclear weapons. The region is characterized by the active presence of terrorists who have the potential for indiscriminate mass violence, and by the growth of nuclear tensions, particularly after both countries tested in1998. The long-standing hostility between India and Pakistan has the potential to facilitate nuclear/radiological terrorism in a number of ways.

At the time of writing, both countries are believed to keep their warheads unmated (with delivery vehicles) and unassembled (Cirincione, Wolfstahl & Rajkumar, 2002: 191, 207). However, this may change over time if tensions persist. There may be a shift to crisis deployment or to peacetime deployment The scope for terrorists to determine the course of events in the region parallels the nuclear stances of India and Pakistan. Each form of nuclear posture carries some risk of terrorist involvement.

- *Unassembled weapons* keep the direct risk of war relatively low. However, there is still an element of risk vis-à-vis terrorism. At worst, a nuclear core or subassembly could be stolen or taken by force and used for (a) the making of a nuclear weapon; or (b) the manufacture of an RDD. Alternatively, a nuclear core could be targeted with conventional explosives (CE) and detonated as an RDD.
- *Assembled but undeployed weapons* could be stolen or taken by force. Even if they are not directly usable, the threat to use them would still be "credible." After all, nuclear weapons possessed by states are said to be "non-usable," but still have powerful strategic effects. Terrorists might also choose to use a nuclear bomb thus obtained in conjunction with CE to produce an RDD. Assembled weapons, whether mated with delivery vehicles or not, could be targeted and detonated with CE at the storage site.
- *Weapons components or assembled weapons under transportation during the process of deployment* would be particularly vulnerable in all the respects identified above. Stationary targets are easier to hold secure, moving ones far more difficult to protect. In particular, road and rail transport offer a wide range of choices to attackers.
- *Deployed weapons* would be relatively safer, but only relatively. Weapons deployed at stationary sites such as air bases and silos would still be vulnerable to terrorist attack. Mobile deployment, likely to be activated during a crisis, would increase the level of risk.

- *Attacks using bombs/materials obtained elsewhere* cannot be ruled out. Pakistan and the former Soviet Union are potential sources for such material. Nuclear/radiological attacks on military forces in general, and nuclear forces in particular, could have devastating effects and carry the potential to unleash nuclear war.

The effects of the modes of attack identified above could be very serious. In all cases, the likelihood of a crisis occurring is high. The terrorist attack on India's Parliament brought the two countries close to war. A nuclear/radiological attack could spark off an armed clash. This might happen as a result of an escalating crisis and high-tension nuclear confrontation. Alternately, a nuclear/radiological terrorist attack, particularly at a time of crisis, could be misperceived as an enemy assault. The "response" would likely be quick, and the consequence horrendous.

3. Sources of Threat

3.1. Illegal Acquisition of Nuclear and Other Radioactive Material from India and Abroad

There are multiple possibilities for terrorists to obtain radioactive material in India suitable for an RDD, such as: hospitals (in particular cancer treatment centers); research facilities (e.g., at universities); oil- and gas exploration industry; road construction industry; and steel manufacture. Radioactive materials used for industrial and medical applications are estimated at over 10,000 units, and include 230 telegammatherapy units containing Co 60; 140 brachytherapy units containing Co 60, Ir 192, Cs 137, and Sr 90; 1,100 industrial gamma exposure devices with Ir 192 and Co 60; 7,500 nucleonic gauges containing Am 241, Am-Be 241, Cs 137, and Co 60; and 50 medical and industrial linear accelerators or LINACS with depleted uranium as shielding material (Kumar et al, 2002).

Typically, physical protection at these sites is rather lax, at best comparable to the protection provided at a jeweler shop, i.e., not a real logistical problem for a trained team of adversaries. Even in a highly industrialized country like the US, aiming for a "cradle-to-grave" supervision of radioactive material, on average every year control is lost over about 200 such sources (Dicus, 1999). It is safe to assume that the situation is at best equal in India.

In India, numerous cases of theft have occurred in recent years. For instance, in July 1998, the Central Bureau of Investigation seized over eight kilograms of natural uranium stolen from the Indira Gandhi Centre for Atomic Research (IGCAR) in Chennai ("Uranium Racket Unearthed," 2002). Besides, it is difficult to ensure security over materials that are outside the direct control of the state, such as radiological sources in the possession of hospitals and industries. In July 2002, a gamma radiography camera containing Ir 192 with an activity of 729 GBq was stolen during transportation in the northeastern state of Assam. A disturbing aspect of the incident was that the camera, a highly radioactive device, was left unlocked in the trunk of a public bus in a region plagued by terrorist activity ("Radiation Scare in Assam," 2002). Although Atomic

Energy Commission (AEC) Chairman Anil Kakodkar claimed there was no need to panic, the fact remains that the camera was a powerful potential source for a dirty bomb ("No Chance of N-Material Falling into Wrong Hands, " 2002). Again, in August 2003, a large quantity of Co 60 was stolen from a steel plant in Jamshedpur in . Though the material was guarded by a sophisticated alarm system on the front door, the thieves simply bypassed it by breaking through the rear wall (Murty & Layak, 2003).

Terrorists might obtain nuclear materials and other radioactive material from outside India. A high probability for terrorists to get access to such materials exists in Russia, which has experienced in recent years a combination of terrorist violence, the growth of organized crime, and an abundance of poorly guarded nuclear facilities (Schweitzer & Schweitzer, 2002: 51-81). William Potter has identified seven cases of diversion of significant quantities of nuclear material, and four other possible cases (Potter, 1997). More alarming, a February 2002 assessment by the US National Intelligence Council states that undetected diversion of weapons-grade and weapons-usable materials has taken place from Russian institutes, but "we do not know the extent or magnitude of such thefts" (Wolfsthal & Collina, 2002: 71). Russia is estimated to possess 150 tons of weapons-grade plutonium, 1,000 tons of enriched uranium, and, at the Chelyabinsk complex alone, 685,000 cubic meters of radioactive waste (Cameron, 1999: 2). Given the reality of poor accounting, organizational deterioration owing to adverse economic conditions, and inadequate physical protection of nuclear and other radioactive material, it is not surprising that there are numerous examples of material diversion: 67 thefts and seizures involving nuclear material, and 97 such cases involving other radioactive material have become known in Russia since 1991 (Database on Nuclear Smuggling, 2003). Insiders commit most thefts of nuclear material. Moreover, projections of Russian weapons inventories show that, over the next decade, about 3,500 warheads containing about 84,000 kilograms of fissile material will be removed from deployment (Wolfsthal & Collina, 2002: 73). Despite assistance from the US and from other countries, the potential for leakage remains considerable.

Pakistan too is a significant potential source for acquiring nuclear and other radioactive material (Basrur & Rizvi, 2003: 47-62). Though its overall nuclear infrastructure is relatively small, the possibility of leakage is widely feared because of the general sense of the country as a failing state. Pakistan's main uranium enrichment facility is at Kahuta (Khan Research Laboratories). Smaller uranium enrichment facilities exist at Sihala and Golra, and possibly at Gadwal. Plutonium extraction work is done at the New Lab, Nilhore, and at Khushab in central Punjab. Pakistan has two nuclear power plants. One is located at Karachi, the other at Chasma. Its nuclear weapons are believed to be in an unassembled state, with the fissile core kept separate from the bomb assembly. The bomb components and the wider infrastructure are under military control. In February 2000, a National Command Authority was established. In January 2001, the Pakistan Nuclear Regulatory Authority (PNRA) was created to regulate the civilian infrastructure. Still, given Pakistan's deteriorating law and order environment, the possibility of leakage remains. Bangladesh has also experienced the flow of contraband radioactive material. In July 2003, police seized a package of 225 grams of uranium oxide manufactured in

Kazakhstan from a suspected Islamic militant group, the Jamaat-ul-Mujahideen (Gargi, 2003).

3.2. India's Nuclear Power Infrastructure

India's Atomic Energy Commission (AEC) stands at the apex of an extensive infrastructure that incorporates warhead manufacture, electrical power production (14 reactors, with 6 more under construction), uranium mining, fuel fabrication and reprocessing, waste management, research, and medical and industrial applications. An independent body, the Central Industrial Security Force (CISF), a paramilitary force under the Ministry of Home Affairs, manages the physical security of nuclear installations. The CISF is also responsible for the protection of other high-risk facilities, such as defense production units, space installations, oil refineries and major ports. But little is known about how it actually organizes the security of nuclear facilities. Personal conversations with retired officials indicate that security is tight, enhanced by the fact that the CISF does not fall under the purview of the Department of Atomic Energy. The Bhabha Atomic Energy Research Centre (BARC) has an on-going program for the development of sophisticated security systems, such as a voice-activated phonetic identification system. The Atomic Energy Regulatory Board (AERB) is empowered to regulate all civilian facilities, while the BARC, which controls warheads, has an internal review mechanism for military-related facilities. Though much of the AERB's function is related to preventing and responding to accidents, part of the counter-terrorism function of controlling nuclear plants and other facilities and responding to emergencies would be covered by the same systems. The BARC is designated as a nuclear-weapons laboratory, and warhead components are stored there in an unassembled state (Hawksley, 2003). According to informed sources, the nuclear warheads located at BARC facilities are under military security. A study by P. R. Chari notes that the Indian Army provides air defense cover, security is strict, and access control is maintained by physical barriers and electronic systems (Chari, 1998).

Indian nuclear power plants (NPP) in themselves are characterized by a high level of built-in safety, which indirectly makes them relatively less vulnerable to sabotage. Several of the accident-related safety features of the CANDU reactor design used in India are also relevant to terrorist acts ("The Canadian Nuclear FAQ – Section D" n.d.a). For instance, the subdivision of the core into two thermalhydraulic loops in most CANDU designs and hundreds of individual pressure tubes within each loop localizes a loss-of-coolant incident. The large-volume, low-pressure, low-temperature moderator surrounding the pressure tubes keeps the risk of a fuel meltdown low. The steam generators are positioned well above the core, which promotes natural thermosyphoning (heat movement) in case shut-down cooling is lost. In addition, CANDU plants are enclosed by heavy concrete walls, including a reactor vault of minimum four feet thickness surrounding the nuclear core itself.

3.3. Organizational Vulnerabilities

Organizational vulnerabilities are of two kinds, internal and external. A serious potential

threat to nuclear facilities, whether military or civilian, comes from insiders. The range of possible threats includes theft of materials; support to outsiders by disruption of alarm systems; sabotage of facilities or specific processes (such as cooling systems); and simple acts such as providing building layouts or access codes to terrorists (Hirsch, D, 1987). Most acts of sabotage have been attributed to disgruntled employees expressing their anger by, among other things, cutting electrical cables, setting fires, and destroying security cameras ("Nuclear Terrorism," n.d.). But that does not rule out political motivations. Most nuclear-related organizations are also vulnerable to cyber-security threats: information on any aspect of a nuclear facility from bomb design to security measures can be misappropriated by an insider (Project on Government Oversight, 2001). It is important to recognize that the insider threat applies to military facilities too. Herbert Abrams has illustrated the seriousness of the problem by recording the significant levels of psychiatric disorders and drug and alcohol abuse, as well as of actual violent acts, by military personnel cleared through personnel reliability screening programs (Abrams, 1991). While this study applies to the US armed forces, there is no reason to believe that military personnel elsewhere are significantly different in their behavior patterns. Available information on personnel reliability is scanty. The potential for serious damage is evident from a parallel case: the killing of Indira Gandhi by her own bodyguards.

Externally oriented security encompasses the intelligence network and asset protection. In one sense, there is ground for reassurance, since there are no known cases of significant security failure involving the nuclear infrastructure. But this may be the result of a lack of interest and effort thus far on the part of terrorists. A look at the general security environment and repeated organizational problems is instructive. Terrorists have periodically penetrated zones of high-level military security. Between November 1999 and July 2003, at least half a dozen attacks by terrorists on high-security army camps in the state of Jammu and Kashmir resulted in 92 deaths of soldiers and their families ("Complacency Making Army Vulnerable," 2003). In February 2003, five policemen guarding a vital bridge in Kashmir were divested of their rifles and ammunition by terrorists ("Probe Ordered into Disarming of Cops by Militants," 2003). Such incidents illustrate the relative ease with which areas under high levels of security cover are penetrated by small numbers of determined terrorists. A shocking security breach in a high-threat zone was the assault on India's Parliament by a small team of heavily armed terrorists in a car loaded with explosives in December 2001.

To take a related aspect, between April 2000 and May 2001, as many as six major fires occurred at Army ammunition dumps, some of them very large ones, such as the enormous fire that destroyed some 10,000 tons of ammunition in Bharatpur on April 28, 2000 ("Blowing Up in Our Faces, 2001; Thapar, 2001). In at least some cases, sabotage was involved. The fact that no nuclear facilities have so far been penetrated is not in itself reassuring in this respect. It is also notable that when India's nuclear tests were being carried out in 1998, an unauthorized individual – an Army washerman who had jumped into a military truck with other soldiers because he wanted to help – was discovered at the test site, that too by accident because he had been bitten by a scorpion (Chengappa, 2000: 422). All of this shows that however robust nuclear security may be, the possibility of failure, with its immense potential for disaster, must be accepted as real.

3.4. The Political Sources of Threat

Politics provides the key to gauging accurately the scale of risk, for ultimately, human motivation is the driving factor. What might motivate a terrorist to "go nuclear"? The history of terrorist mass destruction is a relatively sketchy and short one. The resort to nuclear terrorism, with its potential for mass annihilation, appears to have inherent constraints from the rational standpoint. Indeed, there are very few examples of mass killing by terrorists over the past hundred years or so (Falkenrath, Newman & Thayer, 1998: 47). Terrorists have numerous reasons for eschewing a strategy of mass casualty attacks (Falkenrath, Newman and Thayer, 1998: 45-59). They usually want to create fear, not revulsion. Resort to mass killing can alienate not only the public, but members of a terrorist organization as well. Terrorists have numerous alternatives that can accomplish the objective of creating widespread fear with less difficulty, such as bomb attacks on crowded areas, hijackings, and kidnappings.

Nuclear terrorism has never been practiced. However, Osama bin Laden's Al Qaeda is known to have tried (with no success) to obtain nuclear material and technology (Albright, 2002). Bin Laden's exhortation to Muslims in "The Nuclear Bomb of Islam" to do their "duty" and "prepare as much force as possible to terrorize the enemies of God" has to be taken very seriously (Puzzanghera, 2001).

India has a long history of terrorist activity (Marwah, 2002). A recent report states that as many as 32 groups around the country have been officially banned under the Prevention of Terrorism Act ("TNLA, TNRT, ABNES Banned Under POTA," 2002). The genesis of most current terrorist movements has been internal, with motivations ranging from Marxism to ethnicity. The rise of Pakistan- and Afghanistan-based "jihadi" groups espousing militant Islam is a more recent phenomenon. While the domestically based movements have been relatively local in their focus and have shown no inclination toward mass killing, the jihadi groups are of a different character.

Islamic extremists have steadily increased their presence in Kashmir. The number of foreign militants killed by Indian security forces grew from 30 in 1991 to 194 in 1996, and 541 in 2001 (Sahni, 2002: 215). These groups are driven by a Pan-Islamist agenda that seeks to transform the world order through a "war of a thousand cuts" (Sahni, 2002: 185-196). Not all Muslim terrorist groups active in India are connected to this larger enterprise, but some may be driven toward it by the terror and violence unleashed by extremists of the Hindu majority. For instance, the serial bomb blasts that killed some 250 people in Mumbai in 1993 in what was one of the worst cases worldwide of mass attacks by terrorists before September 11, 2001, were apparently designed to avenge the destruction of a famous mosque by Hindu extremists a year earlier. The anti-Muslim riots in Gujarat state in 2002 have been directly linked to bomb blasts in Mumbai in 2003 (Jha, 2003). The threat of nuclear terrorism from such groups cannot be ruled out if they become further radicalized.

India is located in a wider region of political turbulence and militancy characterized by the ubiquitous presence of terrorism and porous borders. In recent years, radical and terrorist movements have flourished in neighboring Afghanistan, Pakistan, Nepal, Myanmar, Bangladesh, and Sri Lanka. Of these, only two sources of terrorism have

shown the potential to engage in mass killing. The Liberation Tigers of Tamil Eelam (LTTE) in Sri Lanka is one. The LTTE has resources, organizing capability and a capacity for suicide attacks, which would facilitate the handling of radioactive materials without much care for self-preservation. However, it seems to have learned from the Rajiv Gandhi assassination that there are political limits to the use of violence. That single act undermined their cause significantly because it deeply alienated the Indian public, including sympathetic Indian Tamils (Subramanian, 2002).

The main source of a nuclear-terrorist threat, therefore, stems from the jihadi groups that have taken up arms in Kashmir, such as the Harkat-ul-Mujahideen (HuM), the Hizb-ul-Mujahideen (HM) the Jaish-e-Mohammed (JeM) and the Lashkar-e-Toiba (LeT). Of these, only HM has some Kashmiri membership. All of them have a commitment to jihad as well as links to Al Qaeda, and all except HM are ideologically and operationally intertwined with Al Qaeda (Gunaratna, 2002: 208-209). The latter has made it very clear that India is a target. In December 1999, a fax message to the Voice of America in Washington on behalf of Nazeer Ahmed Mujjaid, military adviser to Al Qaeda, proclaimed the goal of these groups: to fight against "Americans, Russians and Indians," and ensure that "Islam will spread over the entire world" (Gunaratna, 2002: 218). Militant leaders have proclaimed Kashmir as a "gateway to India" and established links with fundamentalist and terrorist organizations in different parts of the country, notably in southern India (Sahni, 2002: 212-213).

The politics of the region is conducive to a sustained threat from Al Qaeda and its affiliates. Afghanistan appears to have witnessed the revival of Islamic radicalism. The production of opium has risen dramatically ("Opium Crops Cloud Afghan Recovery," 2003). A third of it is expected to go through India (Sen, 2002). This increases the scope for terrorist activity in the region as there is a close linkage between organized crime, especially the drug trade, and terrorist groups (Raman, 2002).

Pakistan's links to terrorism and Islamic radicalism are well known (Chalk, 2001). Support for terrorists operating in India has been a useful, low-cost instrument to put India under constant pressure. After September 11, 2001, when President Musharraf turned against the radicals, radical Islam has been on the rise, carrying with it a "jihadi culture" of violence hat poses a long-term threat to the region (Cohen, 2003). Al Qaeda is believed by American and Pakistani intelligence services to have set up base in Pakistan (Lumpkin, 2002). Under pressure from India and the US, Musharraf cracked down on terrorism, but by early 2003, most arrested terrorists had been released and the cross-border flow of jihadis into Kashmir was on the rise again (Lancaster & Khan, 2003). The threat environment from the Indian standpoint is aggravated by evidence of the presence of Al Qaeda in Bangladesh. The Harkat-ul-Jihad-al-Islami (HUJI) leader, Abdul Salam Muhammad, also known as Fazlur Rahman, was one of the six constituents of the World Islamic Front for the Jihad against the Jews and the Crusaders announced in 1998 (Gunaratna, 2002: 219).

Given the widespread evidence of Islamic extremists in South Asia, the cause for concern is strong. Immediately after the September 11 attacks, Sheikh Jamilur Rehman, leader of the Tehrik-ul-Mujahideen, explicitly threatened to target Indian nuclear facilities (Pandit,

2001). While this may have been mere rhetoric, there is a real fear arising from Al Qaeda's known interest in acquiring nuclear capability. Qualified personnel are also available in the region. At least two Pakistani nuclear scientists were approached by Osama bin Laden for help in making a bomb (Albright, 2002). While none of this is strong evidence of the advent of nuclear terrorism to South Asia, it does paint a disturbing picture of a potential threat that cannot be ignored. After September 11, 2001, the realm of the possible has been greatly expanded.

3.5. Strategic Sources of Threat

Since India and Pakistan publicly adopted nuclear weapons strategies in 1998, the tension between them has increased, leading to the onset of crises in 1999 and 2001-02 (Koithara, 2003). Pakistan's strategy of subconventional intervention in Indian-held Kashmir, mainly by way of support to terrorist groups, was intensified in the belief that its nuclear deterrent paralyzed India militarily. India, in turn, sought to overcome its perceived paralysis in the face of a rising tide of terrorism by threatening and mobilizing for war. The two predominant features of this spiraling animosity are that the risk of nuclear confrontation, hitherto restrained, has increased; and the capacity of terrorists to generate crises has grown.

The potential for nuclear/radiological terrorism arises from four inter-related sources: the presence of terrorist groups with a proclivity for indiscriminate mass destruction, the high level of tension between and crisis-proneness of India and Pakistan, the steady growth of nuclear arsenals, and the possible change in nuclear posture by both countries. The first factor has already been shown to exist above. So long as groups like Al Qaeda and its affiliates abound in the region, the potential for nuclear/radiological terrorism remains high. India-Pakistan relations, riddled with crises since the 1980s, have become still more unstable since the advent of nuclear weapons. Under the cover of nuclear deterrence, Pakistan has sought to coerce India into negotiation on the disputed state of Jammu & Kashmir by encouraging terrorist groups engaged in "jihad" there (Siddiqa-Agha, 2001: 178-183). This has enhanced the role of terrorists in the region. India, for its part, has attempted to break out of the restraint inherent in the nuclear standoff with Pakistan by threatening to launch an unspecified form of "limited war" against that country (Basrur, 2002). The consequence of the ten-month-long mobilization and confrontation that occurred in 2001-2002 has been prolonged tension and the specter of war, possibly a nuclear one. As a result of these developments, nuclear weapons have been in the forefront of the region's politics. Both India and Pakistan have proclaimed their commitment to "minimum deterrence." This implies the recognition that not many nuclear weapons are required to deter an adversary. But it is not at all clear that there is a lucid understanding of the concept on either side. The fact that they have tested numerous types of warheads and are developing diverse launch vehicles indicates a lack of clarity as to what exactly "minimum" means.

The level of vulnerability to nuclear/radiological terrorism will grow significantly if nuclear weapons inventories expand, and if there is a shift from non-deployment to deployment. All of the risks associated with terrorism are proportionate to the size of an arsenal (though other factors like technical sophistication do matter). The larger a nuclear force, the greater its vulnerability to terrorist assault. This is because more weapons offer

more targets to terrorists; and because an expanding structure has more points of vulnerability to organizational problems of the kind highlighted above. The growth of a nuclear force may be driven by the growth of "operational" concerns as nuclear organizational systems crystallize, by changing perceptions of threat, by bureaucratic interests, or merely by inertia of motion. Above all, it will be hard to resist if the level of tensions, interspersed with crises, remains high. Furthermore, if the trend toward greater diversity – for instance, by the development of a triad – is sustained, numbers will almost certainly go up, since there will be a felt need to ensure that each leg has a "sufficient" number of weapons. The notion that there must be "enough" weapons to make a second strike capability "credible" will inevitably apply to each leg, and the number of weapons – and targets for terrorists – expand accordingly. Whatever the reason, growth in the number of nuclear weapons in an arsenal will increase vulnerability to terrorists.

Deployment is another crucial issue. The continuing hostility between India and Pakistan over Kashmir, punctuated as it has been by frequent crises, portends the possibility of deployment, perhaps at first during a crisis, possibly on a more sustained basis. This increases the scope for a nuclear terrorism-nuclear strategy linkage. Even if the number of weapons remains constant, vulnerability will increase because their distribution will create more opportunities for terrorists. Once a decision to deploy is taken, weapons will be placed in diverse locations, and will be attached to different kinds of missiles, aircraft and, in the more distant future, submarines. Dispersal will create more opportunities for terrorists by offering a range of target choices. It will also create more points at which a security system to protect warheads from attack could fail. The process of transportation will perhaps be the weakest point at which they may be able to strike, since moving assets are likely to be harder to protect. Deployment during a crisis would have the advantage of giving little time for terrorists to target weapons. Against this, when times are not normal, the probability of security failure is higher.

6. Countermeasures

6.1 Logistical countermeasures

Regulatory aspects: The currently applied physical protection practices in India need to be checked objectively with regard to compliance to the *IAEA Convention on Physical Protection of Nuclear Material (CPPNM)* and the *IAEA INFCIRC/225/Rev.4* (IAEA, 1999). Despite their inherent limitations and urgent need for strengthening, these documents provide the only presently existing, internationally acknowledged framework. Such an objective review could be achieved through the services of the *IAEA International Physical Protection Advisory Service (IPPAS)*, which has a proven track record for impartial assessment in a confidential environment involving national security issues.

Security culture: The awareness level for the potential of nuclear and radiological terrorism in India needs to be raised. Internationally operating strategic terrorism will eventually search for the weakest link in *any* nuclear industry world wide, i.e., even if the actual terror attack may not be directed against India, its nuclear infrastructure could be

misused for the diversion of nuclear or other radioactive material, or even a nuclear device. In this regard, the issue of the *insider threat* warrants particular attention, since the majority of cases of fissile material diversion recorded worldwide to date have involved an insider (Zaitseva & Hand, 2003).

Indian Design Basis Threat: The presently applied concept of physical protection needs to be reviewed to ensure that it reflects the significant changes that have resulted from the terror attacks in the US on September 11, 2001 (Steinhausler, Braun & Bunn, 2003). This review process is currently ongoing in many countries and international cooperation is recommended.

Training: Adequate training of customs, border guards, and first responders is essential to regain control, once nuclear or other radioactive material has been diverted. This will require significant investments in terms of updating presently available training courses and the provision of adequate equipment to these groups. As part of this effort, it will be useful to establish also a nation-wide interdepartmental electronic database on incidents involving nuclear and other radioactive materials, ranging from illicit trafficking to criminal misuse of such materials in India.

6.2 Political countermeasures

Strategic Planning: Above all, there is a need for meticulous strategic planning to tackle the nuclear terrorism menace, which has elements of local, national and international security. A task force should be appointed to assume charge of the assessment, planning and execution of a comprehensive strategy. This would include prevention as well as response to a nuclear/radiological terrorist threat. In particular, continuous oversight of the nuclear infrastructure by an independent authority, say a statutory body, is essential to ensure the highest level of security.

Domestic Political Restraint: Notwithstanding the role played by external actors (terrorist groups, states) in terrorism within India's national borders, it is undeniable that domestic groups play a critical role in facilitating the former. At a political level, therefore, it is essential that the links between domestic and external actors be minimized. This involves not only preventive measures such as intelligence, but ensuring that domestic forces which stimulate terrorism are curbed. In this respect, it is incumbent on the state to ensure the prevalence of the rule of law, and to protect minority rights so as to prevent the emergence of disaffected groups that might join hands with, or facilitate the activities of, terrorists bent on wreaking mass destruction.

International Cooperation: Nuclear terrorism is inherently an international problem because the groups that have the potential to perpetrate it span national borders. India has already recognized this by increasing cooperation with agencies like the IAEA and a large number of states, notably the United States and Israel. As a result, it has been able to incorporate best practices and obtain advanced equipment. Further cooperative action through the Proliferation Security Initiative would enhance security by increasing the chances of interdicting the international movement of contraband nuclear/radioactive material. India should also persist with efforts to stabilize its relationship with Pakistan.

After all, both countries have a common interest in preventing acts of nuclear/radiological terrorism.

Nuclear Restraint: Regardless of Pakistan's response to the above, India needs to exercise nuclear restraint by means of a clear understanding of the fundamentals of minimum deterrence, which requires neither large arsenals nor the deployment of weapons to ensure "credibility" (Basrur, 2003). A small, undeployed arsenal would maximize strategic stability and keep to a minimum the scope for terrorists to perpetrate an act of nuclear/radiological terrorism that could have devastating consequences.

References

Abrams, Herbert L., 1991, "Human Reliability and Safety in the Handling of Nuclear Weapons," *Science & Global Security*, 2, pp. 1-26.

Albright, David, 2002, "Al Qaeda's Nuclear Program: Through the Window of Seized Documents," *Policy Forum On-line*, Special Forum No. 47, November 6, Nautilus Institute, Berkeley, CA
< http://www.nautilus.org/fora/Special-Policy-Forum/47_Albright.html>.

Basrur, Rajesh, 2002, "Kargil, Terrorism, and India's Strategic Shift," *India Review*, vol.1, no. 4 (October), pp. 39-56.

Basrur, Rajesh, 2003, "Nuclear India at the Crossroads," Arms Control Today, vol. 33, no. 7, (September), pp. 7-11.

Basrur, Rajesh & Rizvi, Hasan-Askari, 2003, *Nuclear Terrorism and South Asia*, Occasional Paper 25, Cooperative Monitoring Center, Sandia National Laboratories, Albuquerque, NM, February.

Bhushan, Ranjit, 2001, "Shock Therapy," *Outlook*, December 24.
<http://www.outlookindia.com/full.asp?fodname=20011224&fname=Cover+Story&sid=1>.

"Blowing Up in Our Faces," 2001 *Hindustan Times*, May 2.

Cameron, Gavin, 1999, *Nuclear Terrorism: A Threat Assessment for the 21st Century* (Basingstoke & London: Macmillan; New York: St. Martin's Press).

"The Canadian Nuclear FAQ – Section D: Safety and Liability, D 1. Why is the CANDU Design One of the Safest in the World?" (n.d.a)
<http://www.nuclearfaq.ca/cnf_sectionD.htm#q> (accessed on February 15, 2003).

"The Canadian Nuclear FAQ – Section D: Safety and Liability, D 11. How Are Nuclear Plants Protected from Terrorist Attacks?" (n.d.b) <http://www.nuclearfaq.ca/cnf_sectionD.htm#q> (accessed on February 15, 2003).

Chalk, Peter, 2001, "Pakistan's Role in the Kashmir Insurgency," *Jane's Intelligence Review*, September 1, reproduced on the RAND web site <http://www.rand.org/hot/op-eds/090101JIR.html> (accessed on February 14, 2003).

Chari, P. R., 1998, "Protection of Fissile Material: The Indian Experience," *ACDIS Occasional Paper*, Program in Arms Control, Disarmament and International Security, University of Illinois at Urbana-Champaign, September, p. 6.

Chengappa, Raj, 2000, *Weapons of Peace* (New Delhi: HarperCollins).

Cirincione, Joseph, Wolfsthal, Jon B. & Rajkumar, Miriam, 2002, *Deadly Arsenals: Tracking Weapons of Mass Destruction* (Washington, DC: Carnegie Endowment for International Peace).

Cohen, Stephen Philip, 2003, "The Jihadist Threat to Pakistan," *Washington Quarterly*, Vol. 26, No. 3 (Summer), pp. 7-25.

"Complacency Making Army Vulnerable," 2003, *Hindustan Times*, August 3.

Database on Nuclear Smuggling, Theft and Orphan Radiation Sources (DSTO), 2003, Institute of Physics and Biophysics, University of Salzburg, Salzburg, Austria.

Dicus, Greta J., 1999, "USA Perspectives - Safety and Security of Radioactive Sources", *IAEA Bulletin*, Vol. 41, No. 3, pp. 22-27.

Falkenrath, Richard A., Newman, Robert D. & Thayer, Bradley A., 1998, *America's Achilles Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack* (Cambridge, MA & London: MIT Press).

Gargi, M., 2003, "Uranium Heist," Institute for Peace and Conflict Studies, no. 1077, July 9 <http://www.ipcs.org/ipcs/whatsNewArticle1.jsp?action=showView&kValue=1086&status=article&mod=b>.

Gopalakrishnan, A., 2002, "Evolution of the Indian Nuclear Power Program," *Annual Reviews Energy & the Environment*, 27, pp. 369-395.

Gunaratna, Rohan, 2002, *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press).

Hawksley, Humphrey, 2003, "India's Nuclear Muscle," *BBC News*, January 13, <http://news.bbc.co.uk/1/hi/world/south_asia/2646979.stm>.

Hirsch, Daniel, 1987, "The Truck Bomb and Insider Threats to Nuclear Facilities," Nuclear Control Institute, 1987 <http://www.nci.org/g-h/hirschtb.htm>.

Hirsch, Helmut, 2001, "Vulnerability of VVER-1000 Nuclear Power Plants to Passenger Aircraft Crash," WISE, November 2001 <http://www.antenna.nl/wise/terrorism/112001vver.html>.

IAEA, 1999, International Atomic Energy Agency, *Convention on Physical Protection of Nuclear Material*, 1980 <http://www.iaea.org/worldatom/Documents/Legal/cppn.shtml> and INFCIRC/225/Rev. 4 (corrected), *The Physical Protection of Nuclear Material and Nuclear Facilities*, 1999. <http://www.iaea.org/worldatom/Programmes/Protection/inf225rev4/rev4_content.html>.

Jha, Prem Shanker, "The Genesis of Terror," 2003, *Outlookindia.com*, September 8, <http://www.outlookindia.com/full.asp?sid=11&fodname=20030908&fname=Cover+Story>.

Koithara, Verghese, 2003, "Coercion and Risk-Taking in Nuclear South Asia," Center for International Security and Cooperation, Stanford University, Stanford, CA, March.

Kumar, Arun, Agarwal, S. P., Nandakumar, A. N., Kannan, R., and Bhatt, B. C., 2002, "Training Programmes in India for Safety and Security of Radioactive Sources," International Conference on Physical Protection, Salzburg, Austria, September 8-13 <http://www.numat.at/list%20of%20papers/arunkumar.pdf>.

Lancaster, John and Khan, Kamran, 2003, "Extremist Groups Renew Activity in Pakistan," *Washington Post*, February 8.

Leventhal, Paul & Alexander, Yonah, 1986, eds., *Nuclear Terrorism: Defining the Threat* (McLean, VA: Pergamon-Brassey's International Defense Publishers).

Leventhal, Paul & Chellaney, Brahma, 1988, *Nuclear Terrorism: Threat, Perception and Response in South Asia*, Nuclear Control Institute, Washington, DC, October 10.

Lumpkin, John J., 2002, "Al-Qaida [sic] Leaders Said in Pakistan," *Washington Post*, November 11.

Marwah, Ved, 2002, "India," in Yonah Alexander, ed., *Combating Terrorism* (Ann Arbor: University of Michigan Press).

"Massachusetts Congressman Says Nuclear Plants Are Vulnerable," 2002, *New York Times*, March 25.

Murty, Vijay & Layak, Suman, 2003, Radioactive Material Stolen from Jamshedpur Tisco Plant," *Hindustan Times*, August 17.

"No Chance of N-Material Falling into Wrong Hands, " 2002, *Hindu*, July 21.

Nuclear Energy Institute, 2002, *Evaluation of Aircraft Impact on Nuclear Power Plant Structures,* Report NEI-02-04.

"Nuclear Terrorism," n.d., *Three Mile Island Alert* <http://www.tmia.com/sabter.html> (accessed on February 15, 2003).

"Opium Crops Cloud Afghan Recovery," 2003, *BBC News*, September 22 < http://news.bbc.co.uk/go/pr/fr/-/2/hi/business/3127864.stm>.

Pandit, Sharvani, 2001, "Terrorists Vow to Hit Indian N-Sites," *Rediff.com*, September 12 <http://www.rediff.com/news/2001/sep/12ter.htm>.

Potter, William, 1997, "Less Well-Known Cases of Nuclear Terrorism and Nuclear Diversion in the Former Soviet Union," Nuclear Threat Initiative, August. <http://www.nti.org/db/nisprofs/over/nuccases.htm>.

"Probe Ordered into Disarming of Cops by Militants," 2003, *Times of India*, February 15.

Project on Government Oversight, 2001, *U. S. Nuclear Weapons Complex: Security at Risk*, Washington, DC, October.

Puzzanghera, Jim, 2001, "Possibility for Nuclear Terror Too Real to Be Ignored," *Mercury News Washington Bureau*, October 14, reproduced in *ci-ce-ct.com* (web site) < http://www.ci-ce-ct.com/article/showquestion.asp?faq=14&fldAuto=1219> (accessed on February 15, 2003) .

Raman, B., 2002, "Control of Transnational Crime and War against Terrorism: An Indian Perspective," *Outlookindia.com*, May 6 <http://www.outlookindia.com/specialfeaturerem.asp?fodname=20020506&fname=raman&sid=1>.

Sahni, Ajai, 2002, "Extremist Islamist Terror & Subversion," in K. P. S. Gill and Ajai Sahni, eds., *The Global Threat of Terror: Ideological, Material and Political Linkages* (New Delhi: Bulwark Books).

Sandia National Laboratories, 1984, *Investigation of Truck Bomb Threats at Nuclear Facilities,* unpublished report, Albuquerque, NM.

Schweitzer, Glenn E. & Schweitzer, Carole Dorsch, 2002, *A Faceless Enemy: The Origins of Modern Terrorism* (Cambridge, MA: Perseus Publishing).

Sen, Sudhi Ranjan, 2002, "Lion's Share of Afghan Opium Headed for India," *Hindustan Times*, December 1.

Siddiqa-Agha, Ayesha, 2001, *Pakistan's Arms Procurement and Military Buildup, 1979-99* (Basingstoke & New York: Palgrave).

Srivastava, D. N., 2000, "Hi-Tech Computerized Security Management," *Nuclear India*, 34, 3-4 (September-October) <http://www.dae.gov.in/ni/nioct00/nioct00.htm>.

Steinhausler, F., Braun, C. and Bunn, G., 2003, "Strengthening Security at Nuclear Power Plants Against Aircraft Attack," *Journal of Physical Security*, Special Issue, June.

Steinhausler, F., and Bunn, G., 2003, "Protecting the Source: Securing Nuclear Material and Strong Radiation Sources," *IAEA Bulletin*, vol. 45, no. 1 (June), pp. 17-20.

Subramanian, Nirupama, 2002, "It's No More Tiger Country," *Hindu*, July 28.

Thapar, Vishal, 2001, "Ammo Fires: Not Quite Accidental," *Hindustan Times*, August 5.

"TNLA, TNRT, ABNES Banned Under POTA," 2002, *Hindustan Times*, July 3.

"Uranium Racket Unearthed," 2002, *Indian Express*, July 23.

Wolfsthal, Jon B. and Tom Z. Collina, "Nuclear Terrorism and Warhead Control in Russia," *Survival*, vol. 44, no. 2 (Summer), pp. 71-83.

Zaitseva, L., & Hand, K., 2003, "Nuclear Smuggling Chains: Suppliers, Intermediaries, and End-Users," *American Behavioral Scientist*, vol. 46, no. 6, (1 February), pp. 822-844

Approaches to Quantitative Risk Assessment with Applications to Physical Protection of Nuclear Material

Gebhard Geiger
Technische Universität München
Fakultät für Wirtschaftswissenschaften
Munich, Germany

and

Anselm Schaefer
Institute for Safety and Reliability GmbH
Garching, Germany

Abstract

Violations of physical protection combined with threats of misuse of nuclear material, including terrorist attack, pose increasing challenges to global security. In view of this situation, we exploit recent advance in theoretical and applied risk and decision analysis to attain methodological and procedural improvements in security risk management, especially quantitative risk assessment and the demarcation of acceptable risk. More precisely, we employ a recently developed model of optimal risky choice to compare and assess the cumulative probability distribution functions attached to safety and security risks. Related problems such as the standardisation of risk acceptance criteria frequently used in physical protection can also be approached on this basis. With regard to nuclear and radiological threats, the paper suggests possible applications of the improved methods to the safety and security management of nuclear material, cost efficiency of risk management practices, and the harmonisation of international safety and security standards of physical protection. An example selected from the security risks of spent nuclear fuel transport will be presented in some more detail to demonstrate the practical force of the approach.

1. Introduction

During the past decade, the need for improving physical protection (PP) of nuclear material has been felt increasingly in science and international security. Concerns about the security of nuclear material have been raised in view of a wide distribution of orphan radiation sources (Ortiz *et al*. 1999) and a dramatic increase in the illicit trafficking of nuclear materials worldwide, doubling the 1996 annual rate of reported incidents in less than half a decade (Nielsson 2001), with threats of international nuclear terrorism rapidly developing (IAEA 2001; Committee on Science and Technology for Countering Terrorism 2002, Chap. 2).

We consider the physical protection (PP) of nuclear and radioactive material as a security risk assessment and management task. While "nuclear safety" means the prevention of nuclear accidents or mitigation of accident consequences, the term "security" refers to measures to prevent the loss, theft or unauthorised transfer or use of radiation sources or radioactive materials. We specifically address the problem that security risks are difficult to approach within the framework of quantitative risk analysis since potential violations of PP are hard to predict and assess in probabilistic terms.

Exploiting recent advance in theoretical and applied risk and decision analysis, we begin with the outline of a suitable model of quantitative risk assessment. Our approach offers methodological and procedural advantages for the demarcation of acceptable risk, and the management of nuclear safety hazards and security threats. More specifically, we employ a recently developed model of optimal risky choice to compare and assess the cumulative probability distribution functions attached to nuclear safety and security risks. We then proceed to argue that related problems such as the standardisation of risk acceptance criteria frequently used in PP can also be approached on this basis. With regard

to nuclear and radiological threats, possible applications of the improved methods will be discussed. They include the safety and security management of nuclear material, the cost efficiency of risk management practices, and the harmonisation of international safety and security standards of PP. An example selected from the security risks of spent nuclear fuel (SNP) transport will be presented in some more detail to demonstrate the practical force of the approach.

Our analysis intersects with a variety of approaches to risk analysis and its applications to nuclear safety and security that have been developed in the literature. They include probabilistic risk analyses and empirical studies of individual and societal risk perception and acceptance patterns, risk-benefit analyses, approaches to nuclear risk management, and applications to the risks of nuclear facilities and SNF transport (McCormick 1981; Royal Society Study Group 1992; Jorissen and Stallen 1998; Fullwood 2000; Committee on High-Level Radioactive Waste 2001). However, for the sake of definiteness, we do not discuss our approach within the broader contexts of the available theories of individual and societal risk bearing in detail here. As for a review of these issues and the relevant literature, we refer to Geiger (2001, 2002a, c). More narrowly circumscribed problems of this kind associated with the assessment and management of nuclear and radiological risk will be mentioned below within the particular contexts into which they belong.

2. Probabilistic Risk Analysis and Non-Expected Utility Theory

2.1 Utility theory as a risk assessment framework

The risk of a random event E is often defined, in quantitative terms, as the probabilistic expectation of damage or loss from E. However, in experimental contexts, this definition

makes sense only if E occurs repetitively in a series of trials so that the relative frequency of E is likely to approach the probability of E ("law of large numbers"). In applied risk analyses, a broader definition of risk is required, adequately characterising probabilistic events that may occur in a non-repetitive fashion. In fact, many security risks in science and society arise within the contexts of one-shot decision tasks. An example involving a potential terrorist attack on a single SNF shipment has been described by Múnera *et al*. (1997).

Utility models of decision making under risk provide suitable approaches to this sort of problem, with many applications in economics and the engineering sciences, including transport risks of hazardous material (Chankong and Haimes 1983, Chap. 3; French 1988; Evans and Verlander 1997). Utility theory conceptualises risky choice as the acceptance or rejection of lotteries offered to a person. The possible outcomes x of any such lottery are values of a numerical random variable, with gains $x \geq 0$, losses $x \leq 0$, and probability $p(x)$ or, equivalently, cumulative probability distribution $F(x) = \Sigma_{y \leq x} p(y)$, and analogously for continuous distributions with probability densities $f(x)$. In particular, we ambiguously use the symbol "p" to denote probability functions and the risks, or risky courses of action, they represent. The gains (losses) involved can be amounts of money, fatalities prevented (incurred), radiation doses averted (received), or multiple relations between them (Keeney and Raiffa 1976; Chankong and Haimes 1983). The decision maker is further supposed to assess the likely gains and losses x in terms of the utility u, which will depend exclusively on x only in idealised cases, however. In applied risk analyses, assessments of the outcome x in utility terms rather tend to vary with p and the probability ε that p gets resolved within a given period of time which is characteristic of the decision problem in point. Accordingly, the concept of utility must be defined in terms of a parameter family of suitable probability-dependent utility functions $u_\varepsilon(p, x)$. A simple

and empirically realistic account of utility developed by one of us (Geiger 2001; 2002a, b) uses the following parameters to specify $u_\varepsilon(p, x)$:

Aspiration level x_0: The outcome is evaluated as a gain ($x \geq x_0$) or loss ($x_0 \geq x$) with reference to some neutral point x_0 (Kahneman and Tversky 1979) which may be positive, negative or zero. For instance, in radiological applications such an aspiration level x_0 may be the maximum admissible effective radiation dose or dose rate per person specified by a nuclear regulatory agency. For computational purposes it is often convenient to transform the outcome axis $x \rightarrow x - x_0$ so that

$$x_0 = 0 \qquad (1)$$

Reference risk s, or *status quo* (Pratt 1988): Depending on the particular application, the *status quo* is the actor's present state of wealth or health involving some degree of uncertainty (economics, health care, etc.), or extant risk of injury or fatality (natural hazards, hazardous technologies) with probability distribution $s(x)$. For example, in radiological applications s may be chosen as the individual life-time dose risk or dose rate of exposure to natural radiation.

Persistence ε of the status quo s: If a risk p is assessed against a given reference risk s, it may be important for the decision maker to know which of the two is likely to be resolved first. A suitable estimate is provided by the probability ε that p gets resolved prior to the resolution of s ($0 \leq \varepsilon \leq 1$). Conversely, $1-\varepsilon$ is the probability of persistence of p in the presence of the *status quo* risk s.

The overall utility U_ε of a risk p is the average of the utilities of the likely gains and losses $x_1, ..., x_n$,

$$U_\varepsilon(p) = \Sigma_{i \leq n} p(x_i) u_\varepsilon(p, x_i), \qquad 0 \leq \varepsilon \leq 1,\ n \geq 1 \qquad (2a)$$

$$U_\varepsilon(x) = u_\varepsilon(p, x), \qquad p(x) = 1,\ p(x') = 0 \text{ for } x \neq x'. \qquad (2b)$$

In the special case $u_\varepsilon(p, x_i) = u_\varepsilon(x_i)$ in which the utility function does not explicitly depend on p, $U_\varepsilon(p)$ reduces to the familiar expected utility (EU). Otherwise, the expression (2a) is non-linear in the probabilities (generalised expected utility, or non-EU; see Fishburn 1988; Quiggin 1993).

We first infer a few of its general properties before we specify $u_\varepsilon(p, x)$ for particular parameter values below. Figure 1 illustrates the concept of "decreasing marginal utility", meaning that $u_\varepsilon(p, x)$ is strictly increasing in x and concave. $U_\varepsilon(p)$ is the average of a two-component probability distribution p defined for x_1, x_2, with the mean $\mu(p) = x_1 p(x_1) + x_2 p(x_2)$ and the so-called *certainty equivalent* $c_\varepsilon(p)$ lying on the x-axis between x_1 and x_2. As indicated in the figure, the certainty equivalent is implicitly defined by

$$U_\varepsilon(p) \;=\; u_\varepsilon(p, c_\varepsilon(p)) \;=\; U_\varepsilon(c_\varepsilon(p)) \qquad (3)$$

meaning that you are indifferent between receiving either the lottery p with possible monetary prizes x_1 and x_2, or the sure amount c_ε of money. Similarly, one has $c_\varepsilon(p) < \mu(p)$ in Figure 1, that is, you prefer receiving a sure amount of money c', $c_\varepsilon(p) < c' < \mu(p)$, to the lottery p although c' is smaller than the expected value $\mu(p)$ of that lottery ("risk aversion"). Equality $c_\varepsilon(p) = \mu(p)$ obtains in case of vanishing risk aversion, or risk neutrality, where the utility curve is a straight line. The certainty equivalent is thus a measure of the decision maker's attitude toward risk. The important point here is that in the utility approach to risk assessment a risk p is uniquely mapped into its certainty equivalent so that random (risky) and non-random (riskless) outcome variables are consistently assessed in a common quantitative framework. In particular, one has $U_\varepsilon(p) > U_\varepsilon(q)$ exactly if p is preferred to q (i. e., $c_\varepsilon(p) > c_\varepsilon(q)$), and $U_\varepsilon(p) = U_\varepsilon(q)$ exactly if p and q are indifferent (i. e., $c_\varepsilon(p) = c_\varepsilon(q)$).

2.2 An approach to non-EU

Scaling the outcome axis according to (2) and considering (3b), one has (Geiger 2002a, b),

$$u_\varepsilon(p, 0) = 0, \qquad 0 \le \varepsilon \le 1 \qquad (4a)$$

$$U_\varepsilon(s) = U_\varepsilon(0) = u_\varepsilon(s, c_\varepsilon(s)) = c_\varepsilon(s) = 0, \qquad 0 \le \varepsilon \le 1 \qquad (4b)$$

$$u_0(p, x) = u_0(s, x) = \text{constant in } p \qquad (4c)$$

$$u_\varepsilon(s, x) = u_0(s, x), \qquad 0 \le \varepsilon \le 1, x \in \_. \qquad (4d)$$

Equation (4b) means two things. First, the utility of receiving nothing with certainty is $U_\varepsilon(0) = 0$. Second, doing nothing and, thus, remaining in the *status quo*, amounts to receiving nothing with certainty so that $U_\varepsilon(s) = U_\varepsilon(0) = 0$. The certainty equivalent of s accordingly vanishes for all ε. The utility indifference of s and 0 (or x_0) is consistent with the notion that decision makers maximise the utility of changes in wealth rather than that of wealth levels and that such changes are assessed relative to the aspiration level (Kahneman and Tversky 1979). Correspondingly, a risks p is referred to as *neutral* if p and s are indifferent.

Since $\varepsilon = 0$ obtains in the application considered below, we only need to determine the x-dependence of $u_\varepsilon(p, x)$ in the special case (4c) here. The calculation of $u_0(p, x) = u_0(s, x)$ draws upon the following result which holds in a broad class of generalised expected utility models for all ε, $0 \le \varepsilon \le 1$ (Geiger 2002a, b),

$$U_\varepsilon(p) = U_\varepsilon(q) \quad \Leftrightarrow \quad u_\varepsilon(p, x) = u_\varepsilon(q, x), \qquad x \in \_. \qquad (5)$$

The equivalence (5) means that indifferent probability distributions have identical utilities as functions of x. This result has some fortunate practical consequences. Once $u_\varepsilon(p, x)$ has been determined for some p, the utility functions $u_\varepsilon(q, x)$ of all distributions q indifferent to that p are known as well. One can exploit this situation by restricting the analysis to gambles p with only two possible outcomes x_1, x_2 to determine $u_\varepsilon(q, x)$ for all multi-component probability distributions q indifferent to p. To see this, let $x_1', ..., x_n'$ be the

possible outcomes of q and observe that although p and q have finite numbers of outcomes, the functions $u_\varepsilon(p, x)$ and $u_\varepsilon(q, x')$ are respectively defined for all real x and x'. If now the decision maker is indifferent between p and q, he only needs to know $u_\varepsilon(p, x)$ to calculate $U_\varepsilon(q)$,

$$\Sigma_{i\le m} q(x_i')u_\varepsilon(p, x_i') \;=\; \Sigma_{i\le m}\, q(x_i')u_\varepsilon(q, x_i') \;= U_\varepsilon(q) \qquad (6)$$

To determine $u_0(p, x)$ according to (4c), assume first that s is a two-outcome lottery involving a loss $x_1{}^s < 0$ and gain $x_2{}^s > 0$ respectively obtained with probabilities $s_1 > 0$ and $s_2 = 1 - s_1 > 0$. Define the (negative) standard score of the neutral point x_0 in the normalisation (1),

$$z(s) \;=\; \frac{\mu(s) - x_0}{\sigma(s)} \;=\; \frac{\mu(s)}{\sigma(s)} \;=\; \frac{\mu(s)}{\Delta^s\sqrt{s_1\, s_2}}\,, \qquad \Delta^s = x_2{}^s - x_1{}^s > 0 \qquad (7)$$

where σ is the standard deviation. If, however, the *status quo* is a multi-component risk, it is always possible to use (2a), (5) and (6) to construct, by numerical approximation, a two-component probability distribution s' so that s and s' are indifferent (Geiger 2002a, App. B). Hence, (7) describes the general case of a *status quo* risk. Now put $z(s) = z_0$ (the lower index "0" in the parameters z_0 and x_0 denotes universal constants and has nothing to do with the particular $\varepsilon = 0$). One then has for arbitrary p and $x \ge 0$ (Geiger 2002a),

$$\begin{aligned} u_0(p, \pm x) \;&= u_0(s, \pm x) \\ &= -\,u_0(s, \_1)\,\frac{2x + z_0{}^2\,(1+x) - \sqrt{z_0{}^4(1+x)^{\,2} + 4z_0{}^2 x}}{2 + z_0{}^2(1+x) + \sqrt{z_0{}^4(1+x)^{\,2} + 4z_0{}^2 x}}\,, \end{aligned} \qquad (8a)$$

with $u_0(p, 0) = 0$, and the negative branch of the utility function

$$-\,\frac{u_0(p, -x)}{u_0(p, x)} \;=\; \frac{\sqrt{1+z_0{}^2} + z_0}{\sqrt{1+z_0{}^2} - z_0} \;=\; A_0. \qquad (8b)$$

Figure 2 shows $u_0(p, x)$ normalised to $u_0(p, -1) = -1$ for $z_0 = 0.33$. The gross pattern of the utility curve is S-shaped, that is, concave (risk averse) for gains and convex (risk prone) for losses. The exception is a small neighbourhood of the origin (encircled) in which the converse is the case, that is, convexity (risk proneness) for gains and concavity (risk aversion) for losses. The curve is steeper for losses than for gains, corresponding to $z_0 > 0$ and

$A_0 > 1$ in (8b). Figure 2 is in conspicuous qualitative agreement with broad evidence from experimental decision analysis (Luce 2000; Starmer 2000).

For arbitrary two-outcome gambles p, one defines the parameter $z(p)$ in a fashion analogous to (7)

$$z(p) = \frac{\mu(p)}{\sigma(p)} = \frac{\mu(p)}{\Delta\sqrt{p_1 p_2}}, \qquad \Delta = x_2 - x_1 > 0 \tag{9}$$

Given s and z_0 as above, one straightforwardly verifies that

$$\mu(p) - z_0\sigma(p) = 0 \;\Rightarrow\; U(p) = 0 \tag{10}$$

For each pair x_1, x_2 of possible outcomes with $x_1 < 0 < x_2$, the particular p^0 satisfying (10) is obtained by solving $\mu(p^0) = z_0\sigma(p^0)$ for p^0,

$$p_1{}^0 = \frac{2x_2 + z_0{}^2\Delta - z_0\sqrt{z_0{}^2\Delta^2 - 4\,x_1x_2}}{2\Delta(1 + z_0{}^2)} \tag{12}$$

Considering Equation (6) and the result that arbitrary risks are characterised by the properties of their two-component counterparts to which they are indifferent, we can now give a simple characterisation of risk acceptance on the basis of (10) and (11). Since (10) implies $U(p) = 0$ and, hence, a vanishing certainty equivalent for p if $\mu - z_0\sigma = 0$, one has $z_0 > 0$ or

$z_0 < 0$ depending on whether the decision maker is risk averse or risk seeking, and $z_0 = 0$ for risk neutrality. The agent's neutral point of risk tolerance is thus implicitly defined by (10), why neutral risks may be called *marginally acceptable*. We refer to the particular value $z(p^0) = z_0$ as the agent's *limit of acceptable risk*, or, briefly, *critical risk acceptance*. Similarly, p is called *acceptable* (*unacceptable*) exactly if $z(p) \geq z_0$ ($z(p) < z_0$). In this sense the various acceptability properties of risks are evaluated with reference to the decision maker's aspiration level and *status quo.* Moreover, the decision maker's attitude toward risk is not a constant, but generally varies with p even for fixed parameters x_0 and z_0. This variability is further increased if $\varepsilon \neq 0$. It corresponds to the observed coexistence of different risk attitudes in decision makers (aversion, proneness, neutrality towards risk) even for one and the same set of possible outcomes (Geiger 2002a).

Although the preceding conceptualisations have been introduced within the context of a probabilistic model of individual utility-oriented choice, they are in surprising qualitative and quantitative agreement with familiar social risk acceptance attitudes (Geiger 2001, 2002c) such as arise in voluntary and involuntary exposure to, and perceptions of the social costs of, collective and catastrophic risks (Starr *et al*. 1976; Okrent 1981; McCormick 1981, Chaps. 17, 18; Stallen *et al*. 1996).

3. Nuclear and Radiological Security Risk Analysis

3.1 Comparative and quantitative risk assessment

The non-EU model outlined thus far involves three governing parameters x_0, z_0 and ε which in applied risk analyses can often be measured or at least estimated with some confidence (see Sec. 4). They confer considerable flexibility on the model, which is not even fully exploited below when we restrict the analysis to $\varepsilon = 0$. In fact, once x_0, z_0 and ε

have been fixed, the utility function $u_\varepsilon(p, x)$ and, hence, the certainty equivalent $c_\varepsilon(p)$ can be determined for arbitrary risks p in each particular application. Risks can thus be quantitatively and consistently assessed and compared not only for one given set of parameters, but also in different decision contexts, with different x_0, z_0 and ε. For instance, dose risks of radiation from a given amount of one and the same radioactive material may be evaluated in different countries with reference to different tolerability limits (aspiration levels), or on the basis of different population densities making an impact on the *status quo* risk. Such country-specific differences will lead to different certainty equivalents. The corresponding differences in dose risk assessment of one and the same radioactive source are made explicit and precise in this way. Accounting for such differences may be instructive and useful in harmonising international radiological safety and security standards.

3.2 Standardisation of risk acceptance limits

Measures to mitigate the consequences of rare, severe catastrophic events have often been chosen to keep the risk of damage below cumulative life-time exposures to relevant comparable risks. In the area of radiation protection, for instance, international standards have been developed which assure that measures with major impact on public life are only taken if the doses averted are comparable to, or higher than, the average cumulative life-time exposure to natural radiation (ICRP 1991).

Such cumulative life-time risk concepts can also serve as a basis for judgements on the tolerability of risks related to the vulnerability of systems of physical protection by very unlikely but extreme actions such as terrorist attacks. Moreover, their use within a methodological framework of decision and utility theory provides new possibilities for

defining tolerability thresholds, for developing protection standards, and for optimising solutions in physical protection.

Below we apply this new approach to an example of risks from severe accidents with, and attacks against, shipments of highly radioactive material. Our reasoning is based on a dose limit approach that can be straightforwardly extended to include life-time natural radiation doses. It is further based on the use of risk profiles from state of the art probabilistic risk analysis, and the evaluation of such information in terms of non-EU. The example indicates that the approach is viable in principle and that it may be used to translate radiation protection requirements into judgements about the tolerability of risks and the need for standardisation and improvement.

3.3 Cost efficiency of risk management measures

A similar argument applies to measurements of cost efficiency of risk management practices (McCormick 1981, Chap. 17; Royal Society Study Group 1992, Sec. 6.3). As an example, consider the problem of minimising the risk of transporting SNF by suitably rerouting highway shipments (Glickman and Sontag 1995). The operating costs per number of assemblies shipped are generally known. Further assume that the accident probabilities associated with each alternative route can be estimated (Sprung *et al*. 2000, Chap. 8). Then the difference between the certainty equivalents of any two transport risks gives the amount of risk reduction that can be achieved by changing from a less expensive, more risky route to a safer, or more secure, though more expensive one. In more general terms, the trade-off in risk reduction per dollar invested can be assessed by calculating and comparing the certainty equivalents of risks that are managed at different costs at different safety (security) levels.

It should be emphasised that although in this example SNF transport risk is assessed in utility terms, the relevant quantity measuring risk and risk reductions is the certainty equivalent, contrary to the conventional approach in terms of averages of radiological incident consequences (e. g., McCormick 1981, p. 359). It is commensurate to dose (rem, Sv) rather than utility, which after all is a dimensionless and purely theoretical (i. e., non-observable) quantity. It is one of the practical advantages of the present non-EU approach to risk analysis that it turns risk directly and consistently into a measurable quantity that can be priced, that is, whose monetary trade-off can be uniquely specified.

3.4 Mean value vs. certainty equivalent

The present non-EU theory admits an approach to risk assessment more subtle than the one provided by the probabilistic expectation of loss. To see this, let x_0 be a given maximum admissible radiation dose per person per unit time, and let μ_0 be the mean effective dose received by individuals per unit time of exposure to the normal *status quo* radiation. In our example below, μ_0 is the average dose risk per person per shipment of the incident-free truck transport, along a given travelling route, of a given number of assemblies of SNF. One generally has

$\mu_0 < x_0$. However, to make the example compatible with the conceptualisations of Section 2, one rescales the radiation dose x received,

$$x \rightarrow -x + x_0 \qquad (13)$$

so that $x_0 = 0$, $x < 0$ for doses "larger" than admissible (i. e., detriment is negative), and $\mu_0 > 0$. Accordingly, $z_0 > 0$ for the critical risk acceptance. The situation is shown in Figure 3. The risk p with mean $\mu(p) > 0$ and $c_0(p) > 0$ is acceptable, that is, $z(p) > z_0 > 0$, whereas p' has positive mean value but is marginally acceptable. There is also a parameter regime $z_0 > z(p'') > 0$ within which risks with mean $\mu(p'') > 0$ are nonetheless unacceptable. The

average outcome is above the aspiration level, but the utility $U_0(p'')$ and the certainty equivalent $c_0(p'')$ are negative in those cases. The various situations depicted in Figure 3 demonstrate that it may indeed be misleading to compare simply mean doses with the acceptance limit and incident-free case to assess the tolerability of radiological risks.

3.5 Security risk management

In contrast to the safety risks of technical systems, security risks are notoriously hard to specify in probabilistic terms since they involve intentional human action. Nevertheless, one can take a "What-if" approach to the assessment and management of security risks to which the non-EU model may apply. The approach is based on the distinction between probabilities for scenarios, or security incidents, and probabilities for their likely consequences (cf. Kaplan and Garrick 1981; Múnera *et al*. 1997). One arbitrarily sets the probability of any such incident equal to 1, and concentrates on the probabilistic assessment of its consequences. Our utility model can then be employed to assess the potential loss or damage that may arise provided the incident occurs. This kind of restricted security risk analysis is a useful risk management approach, especially one to assess the cost efficiency of risk mitigation and damage prevention measures (Valentin 1999). Here we use it to draw, in a systematic fashion, conclusions from nuclear safety risk analysis to nuclear security risks.

4. Application: SNF Transport Security Risks

4.1 Modelling security risks

SNF transport has repeatedly been considered to be a potential target of terrorism (Múnera *et al*. 1997; Chapin *et al*. 2002). Yet the security risks associated with shipments of

nuclear and radioactive material are hard to evaluate quantitatively since in applications the probability of an attack cannot usually be specified in any meaningful way, not even in instances in which terrorist attacks on highway or railway traffic are frequent (Múnera *et al*. 1997). Since probabilistic assessments of spent fuel security risks would nevertheless be highly desirable from a risk management perspective, we choose an approach which is somewhat more restricted in scope than the attempt to assign probabilities to attacks. We concentrate on the assessment of the likely consequences conditional on the occurrence of a security incident. We start from the available quantitative analyses of the safety accident risks of SNF transport. We further assume that the probabilities of the radiological consequences of a terrorist attack on a truck or train shipment of nuclear material are, to some extent at least, similar to those of potential transport accidents so that, in first approximation, the former can be modelled by the latter. The assumption is based on the fact that the impact on the population of the bombing of, or use of anti-tank weapons against, a transport cask is subject to the same random constraints as those of safety accidents such as weather conditions, route parameters and geographical variations in population number. It is this impact to which the present approach applies. On the other hand, the radiation dose and amount of nuclear material released from a "successful" bombing of a spent fuel shipment may be larger than the ones released even from severe transport accidents (Lyman 1999). Experts have repeatedly disputed this hypothesis (e. g., Chapin *et al*. 2002). But even if the critics are right, it should be subject to probabilistic analysis for the same reason and in the same way as the SNF accident risks.

Now the impact of an increased amount and modified inventory of the radioactive material released from an attack can be adequately treated by modifying the source term magnitude and fractions of failed rods and released radionuclide inventory in the computer calculations of the dose risk probabilities (cf. Sprung *et al*., 2000, Sec. 2.5). Detailed

specifications of the source terms are beyond the scope of our consequence analysis, however. But we can determine the certainty equivalent as a function of the probability that an accident will be severe enough to cause a spent fuel cask to fail and release radioactivity to the atmosphere. Sufficiently large values of that probability then provide a quantitative estimate of the radiation exposure of the public, and its probabilistic distribution, arising from a successful attack. In this way, security risk management measures suitable to decrease this probability can also be assessed with regard to the dose risk reduction they allow.

4.2 The governing parameters

To provide an example of applied PP security risk analysis, we use the data, parameters and results of Sprung *et al.* (2000) on spent fuel truck and rail transport in the US, and related US NRC documents. These results give a detailed probabilistic account of incident-free and accident dose risks, or complementary cumulative distribution functions (CCDFs), to which our approach can be directly applied. Recall that the CCDF is defined as $F_c(x) = \Sigma_{x<y} p(y) = 1 - F(x)$, where x is the individual dose received. The calculations of the CCDFs have been based on data and computer models specifying numerous diverse constraints and parameters governing release and exposure such as wind speed and direction, population density, US highway and railway accident statistics, package inventories, and cask structural impact responses, to name a few.

We evaluate, in terms of its (dis-)utility and certainty equivalent, the risk to the population exposed to the plume of radioactive material released in a hypothetical terrorist attack on a generic Type B SNF cask. Of the four Type B casks considered by Sprung *et al*. (2000), we mainly apply our model to the generic steel-lead-steel cask. For the sake of definiteness, we calculate the governing parameters x_0, z_0 and ε required by our approach

for 1 shipment of 1 assembly of pressure water reator (PWR) SNF by truck transport on US interstate highways involving short stops only (refuelling, recreation of crew, meals, but no sleep; see Sprung *et al*. 2000, Chap. 8). Larger packages and numbers of assemblies shipped per truck or railway waggon are assumed to increase the risk of the emitted radiation dose roughly in proportion to the size of the shipment. Risk is measured in units of dose (person rem). It is proportional to the transport route length and decreases inversely with the travelling speed. To calibrate our model in terms of x_0, z_0 and ε, we use the representative route data provided by Sprung *et al*. (2000, Chap. 3) for the incident-free radiation risk, but turn to one of the illustrative real route cases for our security incident analysis (Sprung *et al*. 2000, Sec. 8.10).

Since population doses from SNF truck transport emitted along routes of arbitrary length are proportional to the overall route length, the population dose from a reference route is required. The example of the 420 km-route studied by Mills and Neuhauser (1999) is typical of SNF truck routes in the US. The authors have subdivided the total route into 29 segments of variable length L_i (km), each passing through an urban, suburban or rural area with average near-route number N_i of persons exposed to radiation with dose rate r_0 during time $\_t_i$, where $\_t_i$ is the duration of exposure of the population in the neighbourhood of route segment i while a truck is travelling along segment i, $1 \le i \le 29$ (for further details of the population statistics and distribution along transport routes see also Mills and Neuhauser 1998, 2000). To obtain the maximum admissible dose x_0 from a single shipment, we choose the average dose rate on the basis of the US NRC maximum admissible individual dose rate

$$r_0 = 0.1 \text{ rem person}^{-1} \text{ a}^{-1}$$

so that

$$x_0 = r_0 \Sigma_{i \le 29} \_t_i N_i$$

The average travelling speed of an SNF transport truck has been estimated by Sprung *et al*. (2000, Tab. 3.3, p. 3-7) at 55 mph = 88 km h^{-1}. Hence, $\_t_i$ = L_i/88 km h^{-1} and

$$x_0 = (r_0/88 \text{ km h}^{-1}) \Sigma_{i\leq 29} L_i N_i$$

$$= 0.01 \text{ person rem} \qquad (14)$$

where $\Sigma_{i\leq 29} L_i N_i$ = 76500 km according to Mills and Neuhauser (1999, Tab. II). Altogether, the value of 0.01 person rem for x_0 corresponds to the (hypothetical) overall population dose released by a single SNF truck shipment of 1 assembly emitting at the rate r_0 while the truck covers a route length of 420 km at an average speed of 88 km h^{-1}.

In a similar fashion, we choose the statistical parameters of the *status quo* risk as the incident-free total transport dose risk μ_0 with standard deviation σ_0 for the 420 km-route case (Mills and Neuhauser 1999, Tab. III)

$$\mu_0 = 0.008 \text{ person rem} \qquad (15a)$$

$$\sigma_0 = 0.006 \text{ person rem} \qquad (15b)$$

The use of (15) within our analysis raises the following two problems. First, the population numbers applied to calculate the numerical values (15) are based on detailed geographical population data and, hence, are different from the near-route values N_i entering Equation (14) (see Mills and Neuhauser 1999 for discussion of their Tables II and III). Fortunately, the difference is not significant, however. Mills and Neuhauser applied a Chi-Square test to the dose risk distributions each based on one of the alternative population statistics, with the result indicating that the two distributions are roughly the same. We exploit this insensitivity of the overall population dose risk to the underlying population statistic, approximating the real incident-free dose risk *s* by a two-component distribution $p_1^0 = p_2^0 = 0.5$ with the possible outcomes $\mu_0 \pm \sigma_0$. Then, by construction, p^0 has the mean μ_0 and standard deviation σ_0. The second problem refers to the utility

indifference of s and p^0. As has been mentioned above, the construction of an indifferent two-component probability distribution from an arbitrary discrete *status quo* s requires a numerical iteration procedure describe elsewhere (Geiger 2002a, App. B). Application of this procedure to the data of Mills and Neuhauser (1999, Tab. III) shows that our calculation of p^0 does not improve significantly if it is carried beyond the first approximation step.

The critical risk acceptance z_0 now is

$$z_0 = (-\mu_0 + x_0)/\sigma_0 = 0.33 \qquad (16)$$

Equation (15) means that although (15a) is positive, its contribution to z_0 is negative since doses received are considered to be detriments and, hence, negative. On the other hand, since (15a) is still below the maximum admissible dose (14), $-\mu_0 + x_0$ and z_0 are altogether positive. Observe that in contrast to μ_0, σ_0 and x_0, the parameter z_0 is invariant to changing route length.

In many applications, the degree ε to which an attack would seem more likely than the incident-free case, can be assumed to be very small so that

$$\varepsilon \_ 0. \qquad (17)$$

We once more emphasise that the chance ε that a risk gets resolved prior to the resolution of other risks that have also been committed to can be very important for the assessment of one risk in the presence of others. As for a detailed account of this ε-dependence in terms of two-stage lotteries, see Geiger (2002a). More generally, the problem is treated under the rubric of *status quo*- or background-dependent decision making under risk in the literature (e. g., Pratt 1988).

The utility function $u_0(p^0, x)$ corresponding to Equations (14) to (17) is shown in Figure 2.

4.3 Security incident risk

We first treat the truck transport of a generic steel-lead-steel PWR SNF cask along the illustrative real route of 4800 km with "no sleep" considered by Sprung *et al*. (2000, Tab. 8.7, p. 8-29, and Subsec. 8.10.1). Except for the route length, all parameters and input data to the calculation of the dose risk CCDF are as in the incident-free case. Figure 4 shows various CCDFs from a set of Monte Carlo samples of dose risk including the mean, 5th, 50th (median), and 95th percentile curve of the set (after Sprung *et al*. 2000, p. 8-30). We choose the CCDF of mean values for application. The maximum admissible dose rate x_0 is increased from (14) roughly in proportion to the route length by

4800 km/420 km = 11.4,

$$x_0^* = 0.114 \text{ person rem}$$

The dose risk distribution of Figure 4 is proportional to the truck accident probability which has been estimated at

$$p_{acc} = 1.8\_10^{-3}$$

on the average per trip of 3000 miles, or 4800 km (US NRC 2000, p. 18). Dividing the CCDF values by p_{acc}, one gets the dose risk conditional on the occurrence of an accident or, in our interpretation, a violation of PP.

The CCDF $F_c(x)$ shown in Figure 4 has the mean

$$\mu = 9.53\_10^{-7} \text{ person rem}$$

(Sprung *et al*. 2000, Tab. 8.8, p. 8-36). It is discontinuous at $x = 0$ since by definition $F_c(0) = 1$ while from Figure 4 $\lim_{x\to 0} F_c(x) = F_c^* \_ 10^{-7} << 1$. We first calculate $c_0(F_c)$, which is simply the certainty equivalent of the dose risk from a truck accident, with no security incident being involved. To this purpose, we must give F_c an indifferent two-component representation p similar to p^0 entering (15) so that $U_0(F_c) = U_0(p)$ with the governing parameter $z(p)$. As for the details of the construction of such a p from a

continuous CCDF, see Geiger (2002b). We partition $F_c(x)$ into two components p_1, p_2 respectively summing up the probabilities of all negative and all positive x-values in the normalisation (13),

$$p_2 = F_c(0) - F_c(x_0^*) = 1 - F_c(x_0^*) \_ 1 - 8\_10^{-8} \_ 1 \qquad (18a)$$

$$p_1 = 1 - p_2 \_ 8\_10^{-8} \qquad (18b)$$

with the outcomes $x_1' < 0$, $x_2' > 0$ so that $\mu' = p_1 x_1' + p_2 x_2'$, where dashed symbols denote quantities in the normalisation (13). To determine x_1' and x_2', observe that the area under the mean CCDF in Figure 4 is μ (Sprung *et al*. 2000, p. 8-14). We put $\mu' = -\mu + x_0^* = \mu_+' + \mu_-'$ and $\mu_+' \_ -\mu_+ + x_0^* \_ -x_0^* F_c^* + x_0^*$, with $\mu_+ \_ x_0^* F_c^*$ being the area under the F_c-curve between 0 and x_0^*, that is, the "positive" contribution to μ for doses x smaller than the maximum admissible value x_0^*. We get

$$x_2' = \frac{\mu_+'}{p_2} = \frac{-\mu_+ + x_0^*}{p_2} = \frac{-x_0^* F_c^* + x_0^*}{p_2} \_ x_0^* \qquad (19a)$$

$$x_1' = \frac{\mu_-'}{p_1} = \frac{\mu' - \mu_+'}{p_1} = \frac{-\mu + \mu_+}{p_1} \_ -1 + x_0^* \qquad (19b)$$

and, analogously to (10),

$$z(p) = \frac{-\mu + x_0^*}{(x_2' - x_1')\sqrt{p_1 p_2}} \_ x_0^* p_1^{-1/2} \_ 360 >> z_0 \qquad (20)$$

Equation (20) confirms the conclusion arrived at by Sprung *et al*. (2000, p. 8-18) on the basis of comparison of expected values, namely that, for any truck shipment, incident-free dose risks greatly exceed accident dose risks. It follows that the latter are acceptable in the technical sense of the risk acceptance terminology introduced in Subsection 2.2. Accordingly, from (18a) and $U_0(p) \_ u_0(p, x_2') \_ u_0(p, c_0(p))$,

$$c_0(F_c) = c_0(p) = -x_0^* F_c^* + x_0^* > 0. \qquad (21)$$

Although because of (16) z_0 is risk averse, and $z(p)$ is even more so according to (20), $c_0(p)$ is slightly larger than the risk neutral value $\mu' = -\mu + x_0^*$, which means risk proneness. However, this apparent inconsistency vanishes considering the convexity of the utility curve in the neighbourhood of the origin (x_2' small, p_2 _ 1) that is indicated in Figure 2.

We proceed to assess the dose risk for the case that an accident, or, in our interpretation, a violation of PP has occurred. Assuming that $F_c(x)$ is roughly proportional to the average accident probability, the relevant dose risk distribution function is $G_c(x)$, with

$$G_c(x) = F_c(x)/p_{acc}, \quad x > 0 \qquad (22)$$

$$G_c(0) = F_c(0) = 1$$

$$G_c^* = \lim_{x\to 0} G_c(x) = F_c^*/p_{acc} \_ \; 5\_10^{-5}$$

To calculate $c_0(G_c)$, we proceed as in Equations (18) to (20), everywhere replacing F_c by G_c, and μ by μ/p_{acc}. Observing that p_1 _ 4_10^{-5} and p_2 _ 1, and neglecting small terms, we find

$$z(p) = 16 >> z_0$$

$$c_0(G_c) = c_0(p) = -x_0^* G_c^* + x_0^* > 0.$$

Although $z(p)$ has decreased considerably from (20), it is still larger than the critical value (16), with the certainty equivalent being positive. This means that, provided a violation of PP has occurred, the resulting dose risk is still tolerable when assessed on the basis of the incident-free case.

The situation changes if we make the dependence of the CCDFs on the severity of an attack explicit. Let p_{no} be the probability that the shipment occurs without an incident severe enough to cause a release of radioactivity to the atmosphere. Then $F_c^* = p_{acc}(1 -$

p_{no}) (Sprung *et al*. 2000, p. 8-64). Given $F_c^* \_ 10^{-7}$, the probability of no release of radioactivity is

$$p_{no} = 1 - 5\_10^{-5} \tag{23}$$

However, in the event of a terrorist attack, p_{no} will generally decrease from its accident value (23), and $F_c(x)$ will accordingly increase. We incorporate this effect by introducing the variable η, letting η vary between the accident value (23) $\eta = 1 - p_{no} = 5\_10^{-5}$ (weak attack) and $\eta = 1$ (heavy attack). This procedure implies two things. First, we admit a parallel vertical shift of the CCDF depending on the severity of an attack. Second, to provide a simple PP incident model, we neglect modifications of the source terms that may change the shape of a CCDF in the security incident case. We have estimated the implications of this neglect both qualitatively and numerically in an order-of- magnitude fashion, as will be discussed in some more detail in the concluding section. Altogether, we consider the distribution function

$$H_c(\eta, x) = \frac{\eta}{1-p_{no}} G_c(x), \qquad x > 0 \tag{24}$$

$$H_c(\eta, 0) = G_c(0) = F_c(0) = 1, \qquad 5\_10^{-5} \le \eta \le 1,$$

$$H_c^*(\eta) = \lim_{x\to 0} H_c(\eta, x) = \frac{\eta}{1-p_{no}} \frac{F_c^*}{p_{acc}} = \eta$$

It gives the dose risk conditional on the occurrence of an attack, with the incident severity η, that is, the chance η of release of radioactivity to the atmosphere. This implies $H_c(1, x) = 10^7 F_c(x)$ and $H_c^*(1) = H_c(1, 0) = 1$. Alternatively, if $\eta = 1 - p_{no}$, this leads back to the case $H_c(1-p_{no}, x) \_ G_c(x)$ treated above. Analogously to (18), we get

$$p_2 = 1 - H_c(\eta, x_0^*) \_ 1 - \eta$$

$$p_1 \_ \eta$$

$$z(p) \; \_ \; \frac{-\eta + x_0^*}{\sqrt{\eta(1-\eta)}}$$

The parameter $z(p)$ falls below the critical value (16) for $\eta > 0.02$, but remains positive for $\eta < 0.1$, and so does the mean

$$\mu' = -\frac{\mu\eta}{p_{acc}(1-p_{no})} + x_0^* = -\eta + x_0^*$$

(Fig. 5). For $0.02 < \eta < 0.1$ (shaded area), the certainty equivalent is negative and, hence, the risk H_c unacceptable although the expected dose $\mu\eta p_{acc}^{-1}(1-p_{no})^{-1}$ in case of a successful attack is still smaller than the maximum admissible dose x_0^*_ 0.1 person rem. The certainty equivalent is shown as a function of μ' in Figure 6.

The results shown in Figures 5 and 6 mean that attack risks with low probability $\eta < 2\%$ of severe consequences are acceptable, and attack risks with moderate or high probability $\eta \geq 10\%$ of severe consequences are unacceptable, independently of whether they are assessed in terms of their expected doses or certainty equivalents. The two assessment modes yield contradictory results in the intermediate probability range of the order of a few percent (shaded areas) where risk acceptance attitudes may be particularly controversial in social perceptions of nuclear security threats. The present approach may then prove helpful in clarifying (e. g., public) disputes about the tolerability of the security risks in point. It may also prove useful for calculating the costs that need to be incurred to decrease η below the threshold to non-acceptance.

5. Discussion and Extensions

The previous section illustrates various points we have made with regard to quantitative risk assessment as applied to PP of nuclear material. Above all, conventional estimates of the tolerability of nuclear and radiological risk can be improved beyond what purely statistical analysis can achieve, namely, the comparison of expected dose and admissible dose limit. This conclusion reflects the common knowledge from risk and decision analysis that the expected value of a random variable may be misleading as a risk indicator (neglect of risk aversion, inappropriateness to one-shot decision problems, underrating the importance of tail probabilities, etc.). In particular, between the high and low risk regimes there is an intermediate domain in which mean doses below the admissible limit may nevertheless be non-acceptable. This result is clearly an outcome of the present utility approach which assesses a given risk in terms of the CCDF as a whole rather than on the basis of one single statistical parameter. Intuitively, risks identical by expected value, but different by distribution and, especially, by tail probabilities, are not generally indifferent. Our approach to risk assessment makes the utility differences explicit in a quantitative, realistic, consistent and, after all, computationally simple fashion.

In a sense, security risks are different from safety risks. By this we mean the possibility that one and the same set of likely consequences may be acceptable or not, depending on whether the consequences are elicited by an accident or by a security incident. Within the present conceptual framework, the difference arises from the need to evaluate security risk consequences given the occurrence of an incident, whereas no such need exists for safety risks, at least as long as accident probabilities can be estimated and security incident probabilities cannot. Conditioning CCDFs on the occurrences of hazardous events not only increases the expected value and (dis-)utility of loss, it may also transform risk attitudes qualitatively. To illustrate this conclusion, consider once more the complementary cumulative distribution F_c of Figure 4 and its successive conditionings

(22) and (24). Let $0.02 < \eta < 0.1$. Then F_c , G_c and H_c are all below the admissible dose limit x_0*, with F_c and G_c being acceptable, but not H_c. It is the "What-if" perspective of the present approach to security risk assessment that makes the difference.

The latter result offers an explanation for the common observation that risks with unknown or unspecified probabilities tend to meet with unusually low degrees of tolerance in the public. The effect is often attributed to the risks of rare catastrophic events in general, but may also be specific of security risks such as nuclear terrorism. In situations that are uncertain in the sense of unknown outcomes and unspecified outcome probabilities, people cannot but assess risks from a "What if" perspective, thereby systematically overestimating even low-dose risks that would otherwise be accepted. The significance of this conclusion for risk management, public policy making and international standardisation of nuclear security practices would seem obvious.

The relationship between the incident severity η and certainty equivalent $c_0(H_c)$ depicted in Figure 6 provides a simple framework for cost efficiency estimates of measures to reduce SNF transport security risks. Measures such as rerouting or augmented escorting of SNF shipments, or improving the cask structural impact response behaviour will generally reduce η to an extent that can be quantified with some accuracy, and similarly so for the costs involved. The c_0-curve in Figure 6 then gives the corresponding amount of risk reduction.

A more detailed cost efficiency calculation would include the numerous and complex modifications of the CCDFs that can be achieved by technical and organisational measures to protect SNF shipments. One would then have to compare the certainty equivalents of CCDFs of different shape and axis intercepts. To estimate the effects to be expected from more detailed analyses of this kind, we applied our model to some of the many CCDFs Sprung *et al*. (2000) calculated for different types of spent fuel casks,

transport modes (truck, rail), routes (length, travelling time, regional climate and weather, near-route population numbers, etc.) as well as size and nuclear inventory of shipments (number of SNF assemblies, PWR and BWR SNF, etc.). What we found from a preliminary overview was that the certainty equivalent largely varies with influence factors such as route length and shipment size to which the dose risk is roughly proportional. Thus, when we estimated the certainty equivalents of the risks of different transport modes (truck, rail) for equal route lengths on a per assembly and order of magnitude basis, no significant departures from the certainty equivalent ratios of F_c, G_c and H_c described above could be observed. We therefore conclude that the present treatment of SNF transport security incidents, though computationally simple, covers basic quantitative features of this type of risk of violation of PP of nuclear material.

References

Chankong, V., Haimes, Y. Y., 1983. Multiobjective Decision Making: Theory and Methodology. North Holland, New York-Amsterdam, 1983.

Chapin, D. M., Cohen, K. P., Davis, W. K., Kintner, E. E., Koch, L. J., Landis, J. W., Levenson, M., Mandil, I. H., Pate, Z. D., Rockwell T., Schriesheim, A., Simpson, J. W., Squire, A., Starr, C., Stone, H. E., Taylor, J. J., Todreas, N. E., Wolfe, B., Zebroski, E. L., 2002. Nuclear Power Plants and their fuel as terrorist targets. Science 297, pp. 1997-1999.

Committee on High-Level Radioactive Waste through Geological Isolation, 2001. Disposition of High-Level Waste and Spent Nuclear Fuel: The Continuing Societal and Technical Challenges. National Academic Press, Washington, D.C.

Committee on Science and Technology for Countering Terrorism, 2002. Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. National Academic Press, Washington, D.C.

Evans, E. W., Verlander, N. Q., 1997. What is wrong with criterion FN-lines for judging the tolerability of risk? Risk Analysis 17, pp. 157-168.

Fishburn, P. C., 1988. Non-Linear Preference and Utility Theory. John Hopkins UP, Baltimore.

French, S., 1988. Decision Theory. Ellis Horwood, Chichister.

Fullwood, R. R., 2000. Probabilistic Safety Assessment in the Chemical and Nuclear Industries. Butterworth-Heinemann, Boston.

Geiger, G., 2001. A dynamic account of rational decision making under uncertainty: the case of risk assessment in hazardous technological systems. In: Matthies, M., Malchow, H., Kriz, J. (Eds.). Integrative Approaches to Natural and Social Dynamics. Springer, Berlin, pp. 305-318.

Geiger, G., 2002a. On the statistical foundations of non-linear utility theory: the case of status quo-dependent preferences. European Journal of Operational Research 136, pp. 449-465.

Geiger, G., 2002b. Pragmatic constraints on rationality: an axiomatic approach to non-expected utility theory. Manuscript, submitted for publication.

Geiger, G., 2002c. Risk acceptance from non-linear utility theory. Manuscript, submitted for publication.

Glickman, T. S., Sontag, M. A., 1995. The tradeoffs associated with rerouting highway shipments of hazardous materials to minimize risk. Risk Analysis 15, pp. 61-67.

IAEA, 2001. Nuclear Security & Safeguards. IAEA Bulletin 43, No. 4.

ICRP (International Commission on Radiological Protection), 1991. Principles for Intervention for Protection of the Public in a Radiological Emergency. Annals of the ICRP 22, No. 4.

Jorissen, R. E., Stallen, P. J. M. (Eds.), 1998. Quantified Societal Risk and Policy Making. Kluwer, Dordrecht.

Kahneman, D., Tversky, A., 1979. Prospect theory: an analysis of decision under risk. Econometrica 47, pp. 763-291.

Kaplan, S., Garrick, B. J., 1981. On the quantitative definition of risk. Risk Analysis 1, pp. 11-27.

Luce, R. D., 2000. Utility of Gains and Losses: Measurement-Theoretical and Experimental Approaches. Lawrence Erlbaum Publishers, London.

Lyman, E. S., 1999. A critique of physical protection standards for transport of irradiated materials“. Paper presented at the 40th Annual Meeting of the Institute of Nuclear Materials Management, Phoenix, AZ.

McCormick, N. J., 1981. Reliability and Risk Analysis: Methods and Nuclear Power Applications. Academic Press, New York.

Mills, G. S., Neuhauser, K. S., 1998. Urban risks of truck transport of radioactive material. Risk Analysis 18, pp. 781-785.

Mills, G. S., Neuhauser, K. S., 1999. Statistical evaluation of population data for calculation of radioactive material transport accident risk. Risk Analysis 19, pp. 613-619.

Mills, G. S., Neuhauser, K. S., 2000. Geographical resolution issues in RAM transport risk analysis. RAMTRANS 11, pp. 295-299

Múnera, H. A., Canal, M. B., Muños, M., 1997. Risk associated with transportation of spent nuclear fuel under demanding security constraints: the columbian experience. Risk Analysis 17, pp. 381-389.

Nilsson, A., 2001. Security of material: the changing context of the IAEA's programme. IAEA Bulletin 43, No. 3, pp. 12-15.

Okrent, D., 1981. Industrial risks. Proceedings of the Royal Society of London A376, pp. 133-148.

Ortiz, P., Friederich, V., Wheatley, J., Oresegun, M., 1999. Lost and found dangers: orphan radiation sources raise global concern. IAEA Bulletin 41, No. 3, pp. 18-21.

Pratt, J., 1988. Aversion to one risk in the presence of others. Journal of Risk and Uncertainty 1, pp. 395-413.

Quiggin, J., 1993. Generalized Expected Utility Theory. Kluwer, Boston.

Royal Society Study Group, 1992. Risk: Analysis, Perception and Management. The Royal Society, London.

Sprung, J. L., Ammerman, J. D., Breivik, N. L., Dukart, R. J., Kanipe, F. L., Koski, J. A., Mills, J. S., Neuhauser, K. S., Radloff, H. D., Weiner, R. F., Yoshimura, H. R., 2000. Reexamination of Spent Fuel Shipment Risk Estimates, Vols. 1,2. Sandia National Laboratories, Albuquerque, NM.

Stallen, P. J. M., Geerts, R., Vrijling, H. K., 1996. Three conceptions of quantified societal risk. Risk Analysis 16, pp. 635-644.

Starmer, C., 2000. Developments in non-expected utility theory: the hunt for a descriptive theory of choice under risk. Journal of Economic Literature 38, pp. 332–382.

Starr, C., Rudman, R., Whipple, C., 1976. Philosophical basis for risk analysis. Annual Review of Energy 1, pp. 629-662.

US NRC, 2000. Discussion Draft: An Updated View of Spent Fuel Transportation Risk. US NRC, Washington, D. C.

Valentin, J., 1999. What if? ICRP guidance on potential radiation exposure. IAEA Bulletin 41, No. 3, pp. 45-48.

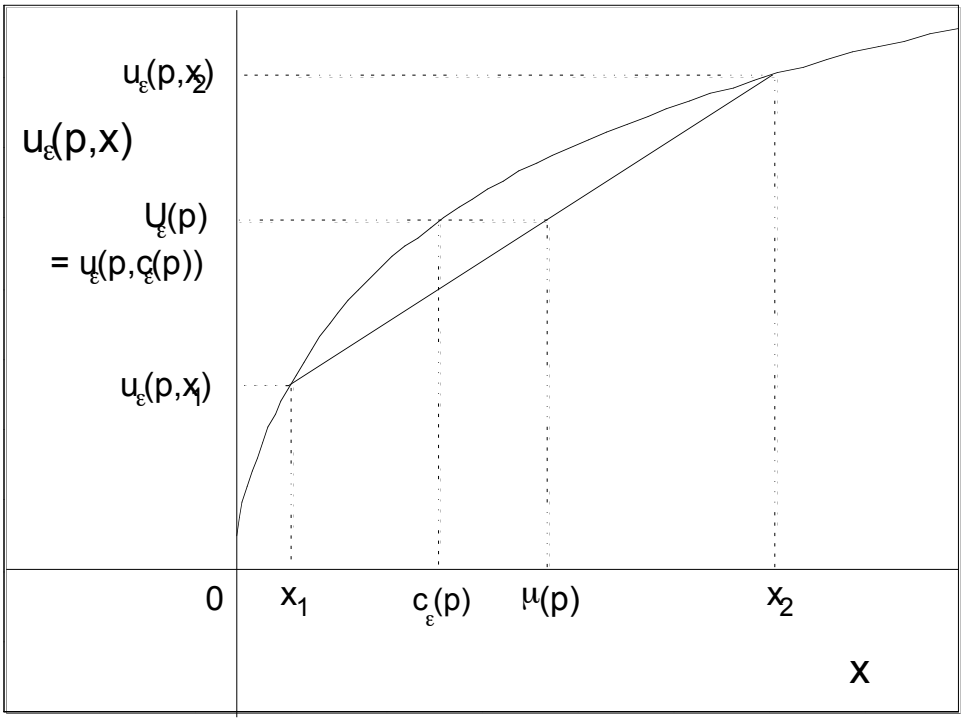

Fig. 1

Fig. 1. Utility function $u\_(p, x)$ and expected utility $U\_(p)$ of a two-point probability distribution p defined for x_1, x_2, with the mean $\mu(p)$ and certainty equivalent $c\_(p)$.

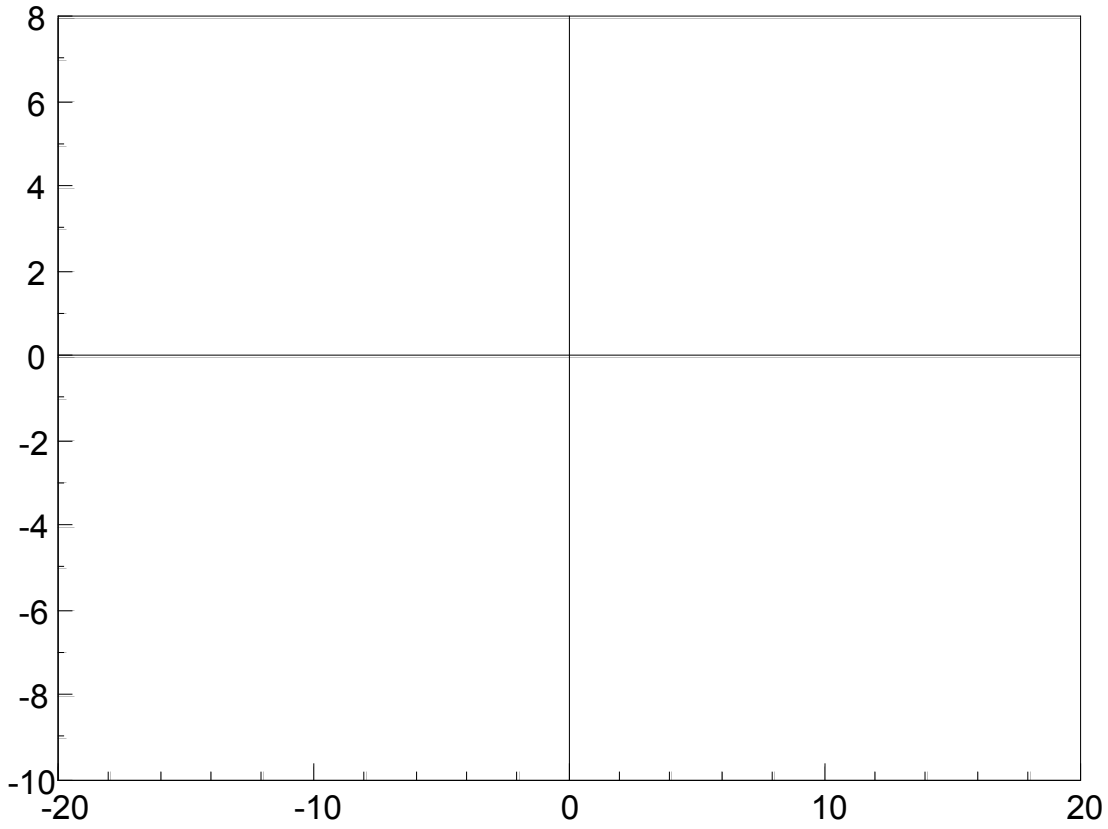

Fig. 2. Utility function $u_0(p^0, x)$ of marginally acceptable risk p^0 with parameter $z_0 = 0.33$.

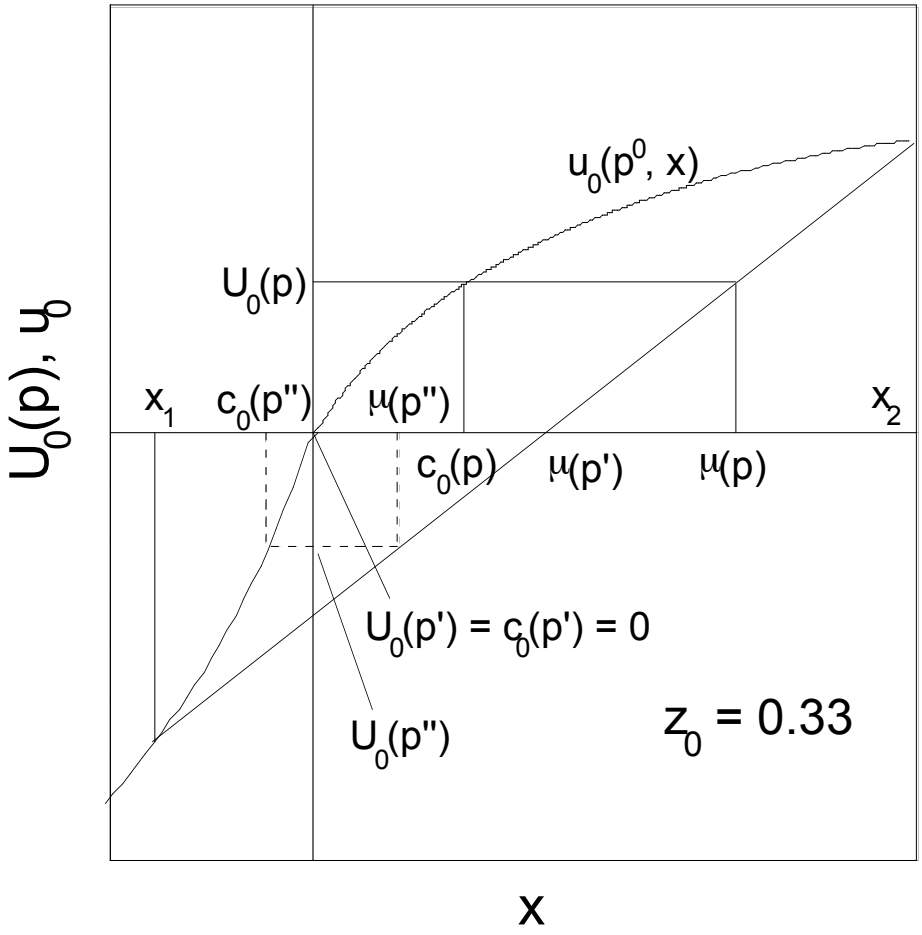

Fig. 3

Fig. 3. Risks with positive mean μ. Positive (solid lines) and negative (dashed lines) certainty equivalent.

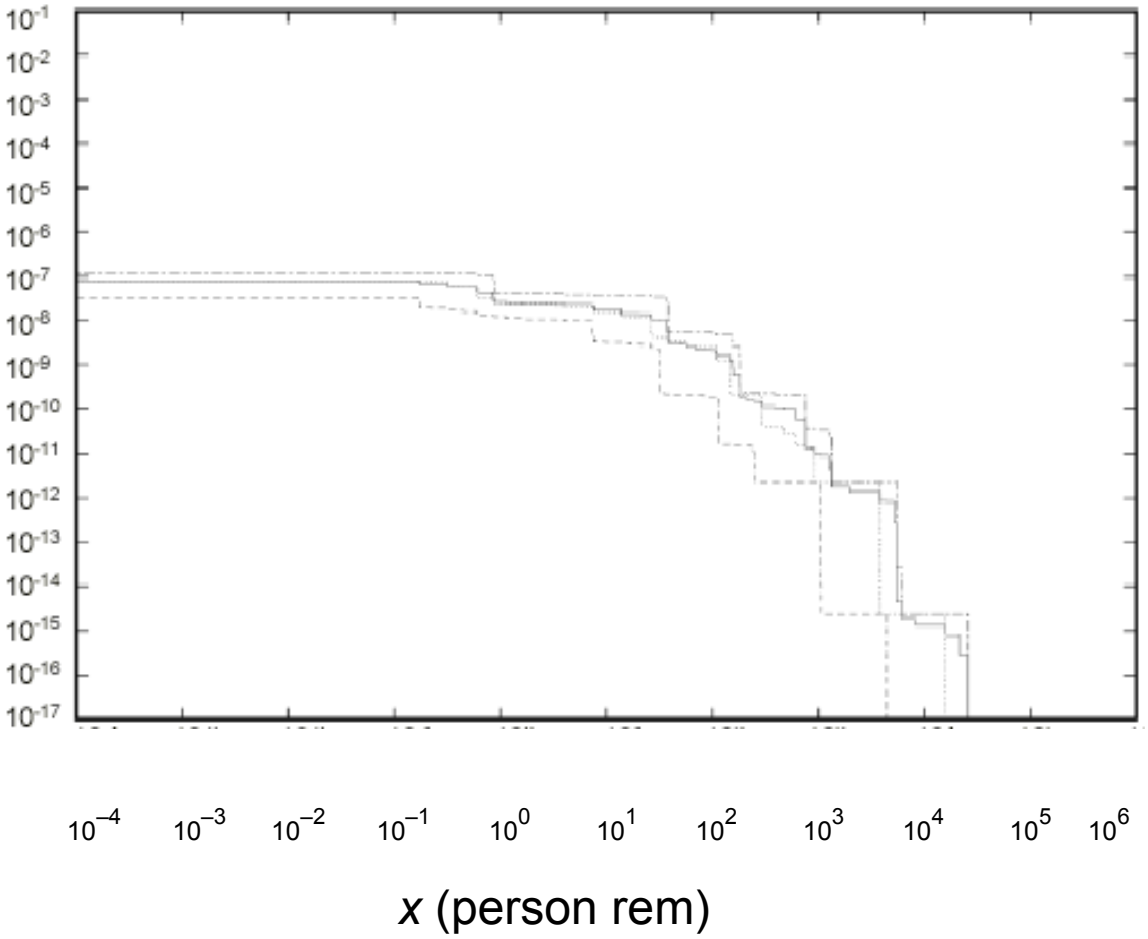

Fig. 4

Fig. 4. CCDFs from a set of Monte Carlo samples of dose risk, with 5th, 50th (median), mean and 95th percentile curve of the set (after Sprung *et al*. 2000, p. 8-30).

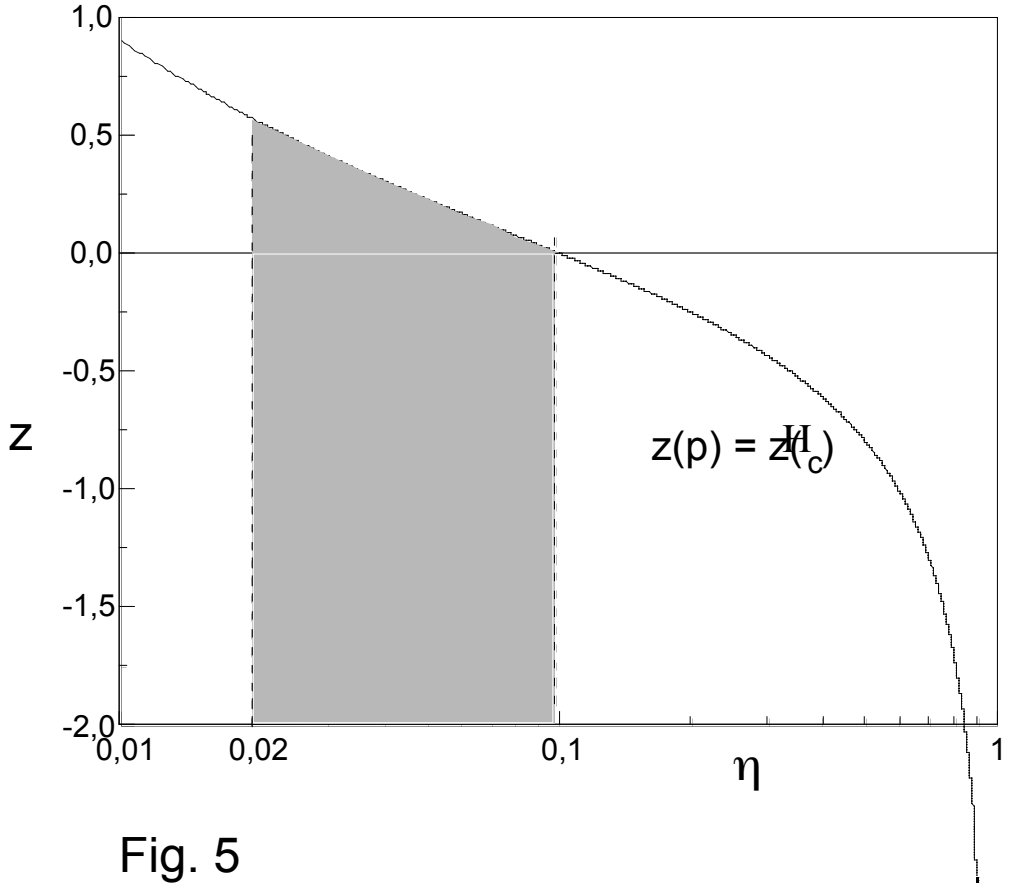

Fig. 5

Fig. 5. Parameter $z(p)$ associated with the risk H_c as a function of incident severity η. For $0.02 < \eta < 0.1$ (shaded area), the certainty equivalent is negative and, hence, the risk H_c unacceptable although the expected dose
$\mu\eta p_{acc}^{-1}(1-p_{no})^{-1}$ is smaller than the maximum admissible dose
x_0*_ 0.1 person rem.

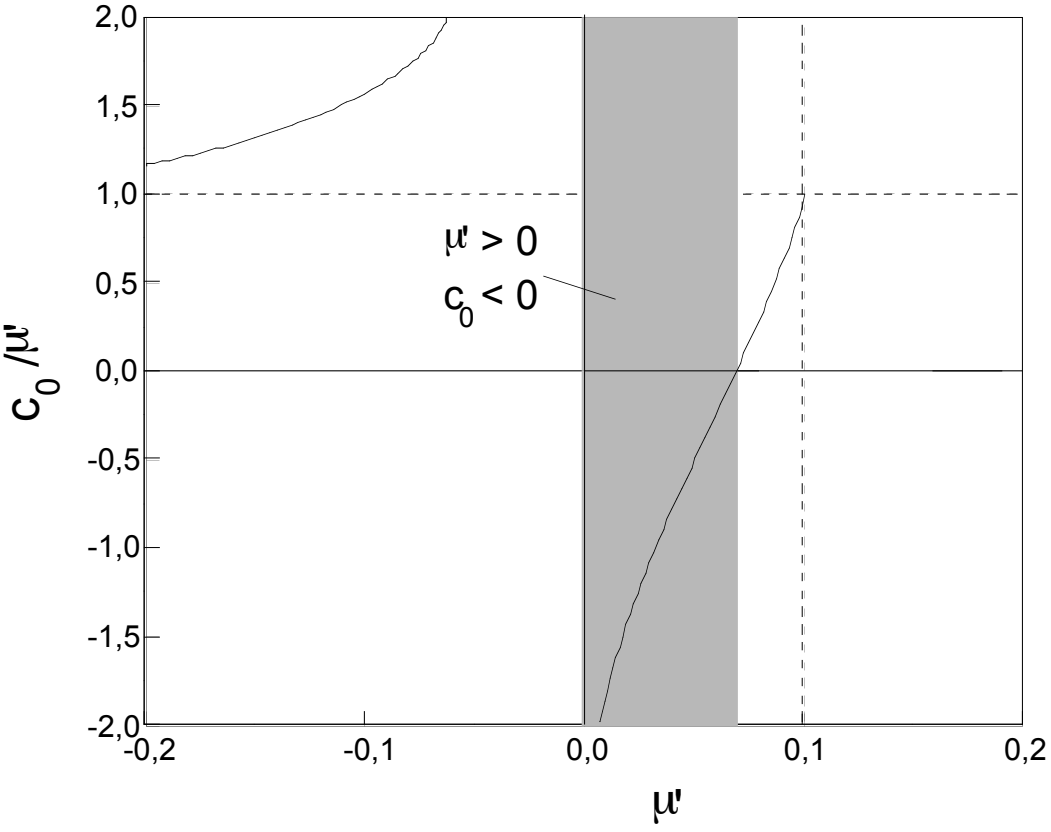

Fig. 6

Fig. 6. Ratio of certainty equivalent c_0 to expected value μ' as a function of μ' in the normalisation (16).