CLARK UNIVERSITY
1887

Center for Risk and Security
The George Perkins Marsh Institute

CRS DISCUSSION PAPER 2005-03

DOCKET
11-IEP-1J
DATE
RECD. Aug 02 2011

Potential Radioactive Releases from Commercial Reactors and Spent Fuel*

Gordon R. Thompson
Research Professor

June 2005

CRS DISCUSSION PAPER 2005-03
Center for Risk and Security
The George Perkins Marsh Institute
Clark University
Worcester, MA

* This discussion paper was previously presented by the author during a U.S. Department of Homeland Security sponsored conference, "Working Together: R&D Partnerships in Homeland Security," Boston, Massachusetts, April 27-28, 2005.

DOCUMENT REPRODUCTION
This document is a discussion paper of the Center for Risk and Security (CRS), The George Perkins Marsh Institute, Clark University. CRS Discussion Papers are works in progress and views expressed in this paper are those of the author. CRS allows reproduction of this paper for personal and educational purposes. Any other reproduction of this paper is not permitted without written permission from CRS or its author.

CONTACT INFORMATION
Primary:
Gordon R. Thompson
Center for Risk and Security
The George Perkins Marsh Institute
Clark University
Phone: (617) 491-5177
Fax: (617) 491-6904
Email: gothompson@clarku.edu

Center:
Center for Risk and Security
The George Perkins Marsh Institute
Clark University
950 Main Street
Worcester, MA 01610
Phone: (508) 751-4622
Fax: (508) 751-4600
Email: crs@clarku.edu

SUGGESTED CITATION
Thompson, Gordon R., Potential Radioactive Releases from Commercial Reactors and Spent Fuel, CRS Discussion Paper 2005-03, Center for Risk and Security, The George Perkins Marsh Institute, Clark University, June 2005.

ABOUT THE AUTHOR
Gordon R. Thompson, D. Phil., is a research professor at the George Perkins Marsh Institute and the executive director of the Institute for Resource and Security Studies, Cambridge, Massachusetts, an independent organization that he founded in 1984. He was educated in Australia and the UK, in engineering and science, obtaining his doctorate from Oxford University in 1973. Over the past three decades he has acquired wide experience with natural resource and international security issues. One of his major interests has been the environmental and security impacts of nuclear technologies. Dr. Thompson has coordinated multidisciplinary teams, organized international conferences and provided expert testimony in a variety of contexts.

ABSTRACT

Commercial nuclear reactors and storage facilities for their spent fuel contain large amounts of radioactive material, and are not designed to resist attack. The US Nuclear Regulatory Commission (NRC) has determined, however, that these facilities require only a light defense. This paper shows, without disclosing any sensitive information, that reactors and spent-fuel-storage facilities have vulnerabilities that could be exploited by knowledgeable and determined attackers, yielding atmospheric releases including tens of MCi of cesium-137. To address this threat, measures described here could provide enhanced defense of reactors and spent fuel, thereby reducing the potential for a large release. A high-priority measure would be to equip spent-fuel pools with low-density racks, storing the remaining spent fuel in hardened, dispersed dry-storage modules at the plant site. Adoption of such measures awaits a recognition by the NRC that commercial nuclear facilities can be considered as radiological weapons awaiting activation by an enemy.

INTRODUCTION

This discussion paper was previously presented by the author during a U.S. Department of Homeland Security sponsored conference, "Working Together: R&D Partnerships in Homeland Security," Boston, Massachusetts, April 27-28, 2005, at the conference poster session titled "Radiological/Nuclear and Explosives Countermeasures". The paper shows that the potential for radioactive releases from commercial nuclear reactors and their spent fuel is a significant, but insufficiently recognized, aspect of homeland security. Credible acts of malice or insanity could release from these facilities an amount of radioactive material substantially in excess of the amount that could be released from other sources.

In view of the large potential for maliciously-induced radioactive releases from commercial nuclear facilities, they can be considered as radiological weapons awaiting activation by an enemy. Some strategic analysts have been aware of this threat for many years [7]. The attacks on New York and Washington in September 2001 demonstrated that attackers can be determined, effective, and strategic in their objectives. Nevertheless, the US Nuclear Regulatory Commission (NRC) has determined that US nuclear power plants and their spent fuel require only a light defense [5].

The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets identifies nuclear power plants as key assets, defined as follows [11]:

> "Key assets represent individual targets whose destruction could cause large-scale injury, death, or destruction of property, and/or profoundly damage our national prestige, and confidence."

This paper relies entirely on information that is widely available in the public domain. It does not reveal any specific point of vulnerability at a nuclear facility, or any other sensitive information.

NUCLEAR FACILITIES AND HOMELAND SECURITY

The first step in understanding the threat of attack on nuclear facilities is to understand the potential attackers and their motives. Potential attackers form a spectrum, ranging from nation-states at one end to disgruntled individuals at the other end. While an overt attack on a US nuclear facility by a nation-state cannot be ruled out, the focus here is on attackers who are commonly described as "terrorists". That word is not, in itself, informative. For present purposes, one can define a terrorist event as an attack by a sub-national group motivated by a political purpose, insanity, or both. The group might be covertly supported by a nation-state. Although insanity might be a motive, the group could not be successful without being rational in its planning.

Attackers whom we view as terrorists might think of themselves quite differently. They might view themselves as soldiers engaged in asymmetric warfare. For present purposes, asymmetric warfare can be defined as armed conflict in which a weaker party seeks to offset its disadvantage by using unconventional means, often involving exploitation of a stronger party's technology.

Political terrorists or asymmetric-warfare attackers would have strategic goals. In general terms, these goals could include: (i) punish a stronger party for a perceived injustice; (ii) strengthen the power of a faction within a weaker party; and/or (iii) undermine a stronger party's commitment to an action opposed by a weaker party.

From the perspective of a rational group that is a committed enemy of a powerful, industrialized country such as the USA, there are two major incentives for attacking a commercial nuclear facility in that country. First, release of a large amount of radioactive material could cause major, lasting damage in the attacked country. Second, commercial nuclear technology could symbolize the attacked country's military dominance through nuclear weapons and associated technologies such as guided missiles; a successful attack on a commercial nuclear facility could challenge that symbolism.

The same group would see three major disincentives for attack. First, nuclear facilities could be less vulnerable than other potential targets. Second, radiological damage from the attack would be indiscriminate, and could occur hundreds of km downwind in non-enemy locations. Third, the attacked country could react with extreme violence.

US COMMERCIAL REACTORS AND SPENT FUEL

There are 103 commercial nuclear reactors operating in the USA at 65 sites in 31 states [9]. Of these 103 reactors, 69 are pressurized-water reactors (PWRs), 9 with ice-condenser containments and 60 with dry containments. The remaining 34 reactors are boiling-water reactors (BWRs), 22 with Mark I containments, 8 with Mark II containments and 4 with Mark III containments. Four of the operating reactors have design features intended to resist aircraft impact. The Limerick Unit 1, Limerick Unit 2 and Seabrook reactors were designed to withstand the impact of an aircraft with a mass of 6 Mg, while the Three Mile Island Unit 1 reactor was designed to

withstand the impact of an aircraft with a mass of 90 Mg. No other US reactor was designed to withstand aircraft impact.

Each reactor periodically discharges spent, highly-radioactive fuel [3]. To date, about 50,000 Mg of spent-fuel assemblies have been discharged from US commercial reactors. Of this quantity, about 44,000 Mg of assemblies are stored under water in high-density racks in pools adjacent to the reactors from which the fuel was discharged. The pools were originally designed to hold a much smaller amount of fuel, but their capacities have been increased by the introduction of high-density racks. Most of the pools now hold an amount of spent fuel that is approaching the pool's capacity. Accordingly, about 6,000 Mg of spent fuel has been transferred to independent spent fuel storage installations (ISFSIs) at reactor sites, and this amount is increasing. At an ISFSI, spent fuel is stored dry in a number of storage modules. The US nuclear industry intends to operate its plants, for the remainder of their lifetimes, with the spent-fuel pools filled nearly to capacity. The remaining spent fuel will be stored in ISFSIs or, potentially, transferred to an offsite location such as the proposed repository at Yucca Mountain.

THE SCALE OF RADIOLOGICAL HAZARD

The radioactive isotope cesium-137 provides a useful indicator of the radiological hazard associated with nuclear facilities [9]. This isotope has a half-life of 30 years. Being comparatively volatile, it is liberally released from damaged fuel. It accounts for most of the offsite radiological exposure from the Chernobyl reactor accident of 1986. That event released about 2.4 MCi (27 kg) of cesium-137 to the atmosphere. For comparison, fallout of cesium-137 from atmospheric tests of nuclear weapons was about 20 MCi (220 kg).

To illustrate the amount of cesium-137 in commercial nuclear facilities, consider San Onofre Units 2 and 3 [8]. These are PWRs in Southern California, whose spent-fuel pools are expected to be filled by 2007-2008. The core of each reactor, consisting of 217 fuel assemblies, contains about 7.7 MCi (85 kg) of cesium-137. The spent-fuel pool at each unit will, when filled to its capacity of 1,325 fuel assemblies, contain about 68 MCi (750 kg) of cesium-137. An ISFSI has been established at the San Onofre site. A typical dry-storage module at this ISFSI, holding 24 fuel assemblies, will contain about 1.2 MCi (13 kg) of cesium-137.

SOURCES OF VULNERABILITY OF NUCLEAR POWER PLANTS AND ISFSIs

Nuclear power plants and ISFSIs have vulnerabilities that arise from intrinsic factors and from design choices. The intrinsic factors derive from the basic processes and structures needed to harness nuclear fission. Notably, spent fuel from a fission reactor necessarily contains biologically harmful and heat-producing radioactive material (e.g., cesium-137). Also, reactor structures and nuclear fuel employ chemically-reactive materials. In the case of PWRs and BWRs, the fuel cladding is made of zirconium alloy that can react exothermically with air or steam. The latter reaction yields hydrogen that can form an inflammable or explosive mixture.

The intrinsic vulnerabilities have been exacerbated by design choices. Two policy decisions have been especially important in this respect. First, resistance to attack has not been a design goal. Second, the NRC has allowed the nuclear industry to employ cost-saving measures that have created vulnerabilities.

Four examples illustrate the combined influence of these factors on the vulnerability of present US nuclear facilities, as follows:

• Example #1
Loss of water from a spent-fuel pool with high-density racks could cause a runaway zirconium-air or zirconium-steam reaction; the resulting heat production and fuel degradation would release a large amount of radioactive material to the atmosphere [3].

• Example #2
Fires, radiation fields and other effects of an attack could preclude operation of active safety systems or implementation of damage-control measures (e.g., provision of water makeup or spray to a drained spent-fuel pool), leading to cascading failures.

• Example #3
At a BWR with a Mark I or II containment, the reactor vessel and the spent-fuel pool are high above ground level, thus improving an attacking group's prospects of damaging the reactor or draining the pool.

• Example #4
Safety systems are typically active rather than passive, and rely on AC or DC electric power; achieving grid disconnect could be easy for attackers, forcing reliance on potentially vulnerable onsite power sources [6].

POTENTIAL MODES AND INSTRUMENTS OF ATTACK ON A NUCLEAR POWER PLANT

A determined, sophisticated group planning an attack on a nuclear power plant could employ a variety of modes and instruments of attack. Table 1 (see next page) shows some potential modes of attack, and the corresponding defenses that are currently provided by nuclear-power-plant licensees in the USA pursuant to NRC requirements [8].

Table 1
Potential Modes and Instruments of Attack

Mode of Attack	Characteristics	Present Defenses at Nuclear Power Plants in USA
Commando-style attack	• Could involve heavy weapons and sophisticated tactics • Successful attack would require substantial planning and resources	Alarms, fences and lightly-armed guards, with offsite backup
Land-vehicle bomb	• Readily obtainable • Highly destructive if detonated at target	Vehicle barriers at entry points to Protected Area
Anti-tank missile	• Readily obtainable • Highly destructive at point of impact	None if missile launched from offsite
Commercial aircraft	• More difficult to obtain than before 11 September 2001 • Could destroy larger, softer targets	None
Explosive-laden smaller aircraft	• Readily obtainable • Could destroy smaller, harder targets	None
10-kilotonne nuclear weapon	• Difficult to obtain • Assured destruction if detonated at target	None

AN ILLUSTRATION OF VULNERABILITY

To illustrate the vulnerability of nuclear facilities to attack, consider the potential for penetration of reinforced-concrete structures. Such penetration could be sought in some attack scenarios. Reactor containments and spent-fuel pools are relevant structures. At a typical PWR, the reactor vessel and associated components are inside a cylindrical, reinforced-concrete containment with a wall about 1 m thick. BWRs have more complex containments, with points of vulnerability. A typical spent-fuel pool (PWR or BWR) has walls about 2 m thick.

An informed attacker is likely to consider a shaped charge as an instrument for penetrating a structure of this kind [10]. It is, therefore, noteworthy that the US government has published a design of a shaped-charge, cruise-missile warhead intended to penetrate rock or concrete. The

warhead's purpose is to open a pathway for entry of a second, tandem-mounted charge. This warhead has a diameter of 71 cm, a length of 72 cm, and a total mass of 410 kg. When tested in 2002, it created a hole of 25 cm diameter in tuff rock to a depth of 5.9 m [citation withheld].

One means of carrying such a device would be a general-aviation aircraft operated remotely or by a suicidal pilot. There are many suitable aircraft. For example, a Beechcraft King Air 90 will carry a payload of up to 990 kg at a speed of up to 460 km/hr. A used King Air 90 can be purchased for US$0.4-1.0 million. Note that there are more than 19,000 airports in the USA. Also, during the period 1998-2003, about 70 aircraft were stolen from general-aviation airports in the USA [8].

POTENTIAL ATMOSPHERIC RELEASES OF RADIOACTIVE MATERIAL, AND THE RESULTING OFFSITE IMPACTS

A successful attack on a reactor or a spent-fuel pool could release radioactive material to the atmosphere by exploiting mechanisms that would be powered by energy sources within the facility -- stored heat, radioactive decay heat, and exothermic chemical reactions (e.g., zirconium-air or zirconium-steam). At a spent-fuel pool, the release could include 10-100 percent of the cesium-137 in the pool, together with other radioactive isotopes [1]. Analyses of reactor accidents suggest that a successful attack on a reactor could also achieve a cesium-137 release fraction of 10-100 percent [6]. The reactor release would, in addition, include short-lived radioactive isotopes such as iodine-131.

An attack on a dry-storage module of an ISFSI could potentially achieve a cesium-137 atmospheric release fraction of 10-100 percent. However, achieving this outcome would require the use of an incendiary device to trigger a zirconium-air reaction, and the availability of air to feed that reaction.

The offsite impacts of an atmospheric release of radioactive material can be estimated, if a variety of assumptions are made. A group of analysts considered a hypothetical release of 35 MCi of cesium-137 at each of five nuclear-power-plant sites in the USA. The five-site average of offsite economic damage was $400 billion [2]. That estimate would rise substantially if reasonable, alternative assumptions were used in the analysis.

PROVIDING ENHANCED DEFENSE OF NUCLEAR POWER PLANTS AND ISFSIs

Various measures are available to provide enhanced defense of nuclear facilities. This defense could be provided remotely or locally. Measures implemented remotely will typically seek to defend many targets, not just nuclear facilities, and are of two types. First, measures can be taken to intercept or deter attackers. Second, other measures can address underlying issues that promote attacks on the USA.

For an existing nuclear facility, an enhanced defense could be provided by locally-implemented measures of the following types [8]:

• Site-security measures
The potential for attackers to reach a facility and implement destructive acts could be reduced by a variety of measures; these could include air defense by an active system (e.g., Phalanx) or a passive system (e.g., poles and nets).

• Facility-robustness measures
Measures could be taken to improve the ability of a facility to experience destructive acts without releasing a large amount of radioactive material to the environment; a high-priority measure of this kind would be to equip spent-fuel pools across the USA with low-density racks, storing the remaining spent fuel in hardened, dispersed, onsite ISFSIs [1, 9].

• Onsite damage-control capability
Damage-control measures could reduce the potential for a release of radioactive material following damage to a facility; for example, new systems could be installed that could provide emergency cooling water to reactors and spent-fuel pools for days or weeks in a high radiation field.

• Offsite emergency-response capability
Improved measures of offsite emergency response could reduce radiation exposure in the event of a radioactive release.

• Altered mode of operation
Altering a facility's mode of operation could reduce the potential for an attack-induced release of radioactive material; for example, the power level of a reactor could be reduced at times of alert.

For a new nuclear facility, there would be many opportunities to incorporate enhanced defense into the design of the facility [4]. Three complementary approaches would be available. One approach would be to design the facility for passive safety. For example, a reactor could be designed so that the fission rate naturally declines at high temperature and heat is dissipated by radiation, conduction and natural convection. A second approach would be to harden the facility by employing thick barriers made of concrete, steel, earth, gravel, etc. A third approach would be to limit the size of a given unit and disperse the units spatially.

THE CURRENT THREAT ENVIRONMENT

The current threat environment for nuclear power plants and spent fuel cannot be objectively determined. Subjectively, it has three major features. First, the technical capacity for a successful attack is widely distributed. Second, deeply-felt grievances are common around the world, and many grievances are held against the USA. Third, the US government is seeking

security through military dominance, potentially exacerbating the threat of attack. These judgments suggest that an enhanced defense of US commercial nuclear facilities is required. By contrast, the NRC has determined that the present light defense of these facilities is adequate.

CONCLUSIONS

Commercial nuclear reactors and storage facilities for their spent fuel represent potentially attractive targets to enemies of the USA. Reactors and spent-fuel-storage facilities are not designed to resist attack, and have vulnerabilities that are partly attributable to cost-saving design choices. Knowledgeable and determined attackers could exploit these vulnerabilities, yielding atmospheric releases including tens of MCi of cesium-137. Enhanced-defense measures are available that could substantially reduce the potential for such releases. Adoption of such measures awaits a recognition by the NRC that commercial nuclear facilities can be considered as pre-deployed radiological weapons awaiting activation by an enemy.

REFERENCES

[1] Alvarez, Robert, Jan Beyea, Klaus Janberg, Jungmin Kang, Ed Lyman, Allison Macfarlane, Gordon Thompson, Frank N. von Hippel, "Reducing the Hazards from Stored Spent Power-Reactor Fuel in the United States", *Science and Global Security*, Volume 11, 2003, pp 1-51.

[2] Beyea, Jan, Ed Lyman and Frank von Hippel, "Damages from a Major Release of 137Cs into the Atmosphere of the United States", *Science and Global Security*, Volume 12, 2004, pp 125-136.

[3] Committee on the Safety and Security of Commercial Spent Nuclear Fuel Storage, Board on Radioactive Waste Management, National Research Council, *Safety and Security of Commercial Spent Nuclear Fuel Storage: Public Report* (Washington, DC: National Academies Press, 2005).

[4] Hannerz, K., *Towards Intrinsically Safe Light Water Reactors* (Oak Ridge, Tennessee: Institute for Energy Analysis, February 1983).

[5] Nuclear Regulatory Commission, *Protecting Our Nation Since 9-11-01, NUREG/BR-0314* (Washington, DC: US Nuclear Regulatory Commission, September 2004).

[6] Nuclear Regulatory Commission, *Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, NUREG-1150* (Washington, DC: US Nuclear Regulatory Commission, December 1990).

[7] Ramberg, Bennett, *Nuclear Power Plants as Weapons for the Enemy: An Unrecognized Military Peril* (Berkeley, California: University of California Press, 1984).

[8] Thompson, Gordon, testimony before the Public Utilities Commission of the State of California regarding Application No. 04-02-026, 13 December 2004. (This testimony addressed the provision of an enhanced defense of Units 2 and 3 of the San Onofre Nuclear Generating Station.)

[9] Thompson, Gordon, *Robust Storage of Spent Nuclear Fuel: A Neglected Issue of Homeland Security* (Cambridge, Massachusetts: Institute for Resource and Security Studies, January 2003).

[10] Walters, William, "An Overview of the Shaped Charge Concept", paper presented at the 11th Annual ARL/USMA Technical Symposium, 5 and 7 November 2003. This symposium was sponsored by the Mathematical Sciences Center of Excellence at the US Military Academy (USMA) and hosted by the US Army Research Laboratory (ARL) and USMA.

[11] White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, DC: The White House, February 2003).