Nuclear Proliferation Prevention Project (NPPP)

Working Paper # 1

# Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-assessing the Current "Design Basis Threat" Approach

by Lara Kirkham[1]
with Alan J. Kuperman, Ph.D.

Nuclear Proliferation Prevention Project
LBJ School of Public Affairs
University of Texas at Austin
www.NPPP.org

**August 15, 2013**

[1] This working paper was researched and written primarily by Lara Kirkham, a graduate research assistant at the NPPP, supplemented with editing and contributions by Prof. Alan J. Kuperman, coordinator of the NPPP. It was prepared as part of a larger inter-disciplinary study at the University of Texas at Austin for the Office of the Secretary of Defense, which provided financial support for the research. The authors thank Matthew Bunn of Harvard University and Alex Athey of the University of Texas at Austin for their helpful comments on an earlier draft.

## I. INTRODUCTION

This report reviews the current thinking on threat assessment at nuclear facilities in the United States. It surveys and compares the risk assessment methods used by the Nuclear Regulatory Commission (NRC), the Department of Energy (DOE), and the Department of Defense (DOD), and it explores alternative and complementary approaches. All three agencies rely on some form of the design basis threat (DBT) as the foundation of their physical protection strategy. We identify shortcomings in the DBT approach, but also in the proposed alternatives.

This report focuses principally on the threat assessment tools used by the NRC because more information is publically available about its methods. We believe the analysis could help the DOD evaluate its own approach to nuclear security and risk assessment because many of the problems associated with securing nuclear material are universal, such as developing a postulated threat based on past attacks and current resources of potential adversaries. The report first surveys the primary threats to nuclear facilities, and their consequences. The threats are divided into four main categories, with each agency facing some combination of these dangers. We then discuss the specific DBTs used by the three agencies, comparing and contrasting their particular approaches. This is followed by a critique of the DBT's posited attack and a critique of the DBT's theoretical underpinnings. We then explore proposed alternatives to the DBT approach, analyzing their theoretical and practical shortcomings as well. The report closes with recommendations for revising the DBT and the U.S. government's approach to nuclear security.

We conclude that despite shortcomings of the DBT approach, alternative approaches including game theory might not necessarily lead to more efficient resource allocation due to theoretical and practical limitations. If the DBT approach is retained, the report's main recommendation is for the DBT to be made uniform for all nuclear facilities posing risks of catastrophic nuclear terrorism – which includes nuclear power reactors and facilities containing nuclear weapons or significant quantities of fissile material – aiming to reduce the risk of successful terrorist attack on such facilities as close to zero as possible in light of available resources. The report argues that the U.S. government lacks the reliable information that would justify varying the DBT between these facilities – such as the likely relative consequences of attacks on different facilities, or their relative value to adversaries. The report criticizes the current variation in the DBT between U.S. government agencies on grounds that it leads to indefensible outcomes such as variation in the level of security at facilities that contain identical or functionally equivalent nuclear assets. The report acknowledges that NRC licensees might be unable to provide adequate security measures to satisfy such a uniform DBT, due to economic or statutory constraints, but argues that the solution is for the government to provide the necessary supplementary security, which currently does not occur in many cases, rather than to reduce artificially the posited threat as now is done.

## II. THREATS AND CONSEQUENCES

Despite the relatively low probability of a nuclear terrorist attack,[2] the consequences of such an attack justify efforts to further minimize risk. In particular, a terrorist detonation of a nuclear weapon would be locally devastating in addition to potentially initiating complex and catastrophic responses from world nuclear powers.[3] Terrorists could potentially buy, steal, or construct such a nuclear weapon. Alternatively, they could sabotage nuclear facilities to damage the reactors or spent fuel pools and release radioactive material into the environment. These major threats and their consequences are detailed below. This report does not consider the threat from radiological dispersion devices – also known as "dirty bombs" – which would have much less devastating physical consequences. The report focuses mainly on U.S. nuclear assets and approaches to nuclear security, but its analysis and insights are also applicable to protection of foreign nuclear assets, which typically may be more vulnerable to terrorist attack and thus a priority for security upgrades.

### A. Theft of nuclear weapons

The U.S. nuclear arsenal includes approximately 5,000 active and inactive nuclear warheads.[4] These weapons are stored at 21 locations in thirteen states and five European countries, with an average of 450 warheads at each location.[5]

---

[2] Even among scholars, there is a great range of estimates of the likelihood of nuclear terrorism. One skeptic puts the likelihood that a terrorist group will acquire a nuclear weapon at "very substantially less than one in a million." John Mueller, "Reactions and Overreactions to Terrorism: The Atomic Obsession" paper presented at the Annual Meeting of the American Political Science Association, Chicago, Illinois, August 31-September 3, 2007. On the other end of the spectrum, Harvard University professor Graham Allison estimates a 50 percent chance of a nuclear terrorist attack on U.S. soil in the next decade. Graham Allison, "Nuclear Deterrence in the Age of Nuclear Terrorism," *Technology Review* (November/December 2008), http://www.hks.harvard.edu/news-events/news/hks-in-the-news/nuclear-deterrence-in-age-of-terrorism.

[3] Robert Ayson, "After a Terrorist Nuclear Attack: Envisaging Catalytic Effects," *Studies in Conflict and Terrorism* 33 (2010).

[4] Donna Miles, "U.S. Declassifies Nuclear Stockpile Details to Promote Transparency," *American Forces Press Service,* May 3, 2010, accessed March 1, 2012, http://www.defense.gov/news/newsarticle.aspx?id=59004.

[5] Hans M. Kristensen, "Estimated Nuclear Weapons Locations 2009," *Federation of American Scientists Strategic Security Blog*, November 25, 2009, http://www.fas.org/blog/ssp/2009/11/locations.php.

There are no known cases of terrorists successfully stealing a nuclear weapon,[6] and few known attempts.[7] The multi-layer detection and security systems in place at permanent nuclear weapons storage facilities presumably make theft of a complete nuclear weapon one of the least probable pathways for committing nuclear terrorism.[8] Even if terrorists could steal a nuclear weapon, they would confront safety features that inhibit unauthorized use or detonation, which could be difficult for terrorists to bypass.[9]

Some argue that as soon as a terrorist acquired a nuclear weapon, he would be compelled to detonate it quickly to avoid interception by authorities.[10] The possibility of the detonation of a nuclear weapon by a terrorist has spawned a number of doomsday scenarios. Certainly the local devastation would be immediate and catastrophic, as illustrated by the WWII attacks on Hiroshima and Nagasaki. Additional consequences would depend in part on where it were detonated, with state responses ranging from no action at all to retaliation with nuclear force against a country erroneously presumed to have initiated the attack.[11] One scenario contemplates an escalation leading to a massive military exchange between states armed with considerable nuclear arsenals.[12] A nuclear exchange of that magnitude, in the worst case, could result in environmental devastation and global famine.[13]

Alternatively, though less likely, a terrorist might hold on to a stolen nuclear weapon for deterrent or coercive purposes. In this case, the nuclear weapon could be used as a form of "nuclear compellence" to pressure foreign occupiers to depart holy or important lands, or even as a "proxy nuclear capability" for the local state harboring the terrorist.

---

[6] Belfer Center for Science and International Affairs, "Nuclear Security Summit Background Material: Nuclear Terrorism Fact Sheet," John F. Kennedy School of Government, Harvard University, April 2010, 2.

[7] Matthew Bunn, "A Mathematical Model of the Risk of Nuclear Terrorism," *The Annals of the American Academy of Political and Social Science* 607 (2006), 109.

[8] Matthew Bunn et al., "The U.S.-Russia Joint Threat Assessment on Nuclear Terrorism," Report for the Belfer Center for Science and International Affairs, Harvard Kennedy School, Institute for U.S. and Canadian Studies, 2011, 16-17.

[9] Bunn, "The U.S.-Russia Joint Threat Assessment," 17.

[10] Bunn, "The U.S.-Russia Joint Threat Assessment," 16.

[11] Ayson, "After a Terrorist Nuclear Attack."

[12] Ayson, "After a Terrorist Nuclear Attack," 583.

[13] A war fought with the deployed U.S. and Russian nuclear arsenals would inflict catastrophic environmental damage that would make agriculture impossible and cause mass starvation. Owen B. Toon , Alan Robock, and Richard Turco, "Environmental Consequences of Nuclear War," *Physics Today* 61 (2008), 41.

Retaining, rather than using, the nuclear weapon might be perceived to boost the prestige of the terrorist organization or its host state.[14]

## B. Theft of SNM

Nuclear material suitable for use in weapons – primarily, plutonium or highly enriched uranium (HEU) – is often called fissile material or special nuclear material (SNM).[15] A subset of this is considered "strategic" special nuclear material (SSNM), meaning its isotopic content is especially suitable for weapons, the amount is above a threshold, and it is in specified forms (e.g., nuclear weapons, nuclear weapons components, metals, and oxides). The theft of SNM, particularly HEU, is a serious threat for its potential use in an improvised nuclear weapon. The United States has an HEU inventory estimated at more than 600 metric tons (MT) – sufficient for at least 24,000 warheads.[16] This material is stored and used across the country in sites operated by the DOE, DOD, and NRC. The bulk is stored at DOE facilities, with the remainder distributed across DOD facilities and NRC-licensed facilities.

The theft of nuclear material in quantities large enough to construct an improvised fission bomb is a real possibility. It is arguably easier than stealing a complete weapon due to the lower security levels associated with storage of nuclear material, the increased administrative difficulty in accounting for SNM compared to weapons, and the wider dispersal of SNM.[17] For example, the United States for peaceful purposes has exported tons of SNM overseas to dozens of countries, most of which do not apply the same level of physical security as the U.S. government, and some of which do not report to the United States the location or disposition of the material, making it impossible for

---

[14] Ayson, "After a Terrorist Nuclear Attack," 575-577.

[15] SNM includes the following: highly enriched uranium (HEU), that is, uranium enriched in the isotope uranium-235 to 20 percent or greater; uranium-233; and any plutonium containing less than 80 percent of the isotope plutonium-238. Weapon-grade HEU is generally defined as HEU enriched in the isotope of uranium-235 at 90 percent or greater, although the HEU in the Hiroshima bomb had an average enrichment of only 80 percent. U.S. GAO, *Nuclear Nonproliferation: U.S. Agencies Have Limited Ability to Account for, Monitor, and Evaluate the Security of U.S. Nuclear Material Overseas*, GAO-11-920 (Washington, DC: GAO, 2011), http://www.gao.gov (accessed March 1, 2011), 2.

[16] International Panel on Fissile Materials, "Global Fissile Material Report 2011: Nuclear Weapon and Fissile Material Stockpiles and Production," January 10, 2012, http://fissilematerials.org/library/gfmr11.pdf, 9 (accessed May 15, 2012). See also, Project On Government Oversight, "U.S. Nuclear Weapons Complex: How the Country Can Profit and Become More Secure by Getting Rid of Its Surplus Weapons-Grade Uranium," September 14, 2010, http://www.pogo.org/pogo-files/reports/nuclear-security-safety/downblending-heu/nss-nwc-20100914.html#2 (accessed March 1, 2011).

[17] Bunn, "The U.S.-Russia Joint Threat Assessment," 18.

Washington to verify the level of physical security that is applied.[18] If terrorists obtained a sufficient amount of fissile material, they would next face the challenge of fabricating it into a functioning nuclear weapon, or credibly bluffing to have done so if their aim were extortion. Two terrorist groups are currently recognized as having the interest, financing, and organizational sophistication to build a nuclear device – al Qaeda and the Japanese apocalyptic group Aum Shinrikyo.[19]

Unlike theft of a complete nuclear weapon, there are confirmed cases of theft of weapons-usable material.[20] The International Atomic Energy Agency (IAEA) reported eighteen seizures of stolen HEU or plutonium from 1993-2007, but most of these cases involved very small quantities.[21] Another source lists only one known incident involving a substantial quantity of HEU, a 1994 case in Prague involving Czech, Slovak and Russian nationals.[22] Says one analyst, "if you add up all the reported attempts to sell highly enriched uranium or plutonium, even including those that have the scent of security-agency hype and those where the material was of uncertain quality, the total amount of material still falls short of what a bomb-maker would need to construct a single explosive."[23] But, he acknowledges, that does not account for the undetected cases of theft.[24] A separate danger, not covered by this brief, is from radiological dispersion devices, which would inflict only a handful of fatalities but could sow terror. More than one terrorist group has seriously considered such an attack, and in another instance Chechen rebels placed a radiological source in a public park and then alerted reporters, to demonstrate their capability.[25]

---

[18] U.S.-origin HEU and plutonium have accumulated overseas from foreign nuclear research and commercial nuclear power activities. "DOE, NRC, and [the Department of] State are not able to fully account for U.S. nuclear material overseas that is subject to nuclear cooperation agreement terms because the agreements do not stipulate systematic reporting of such information, and there is no U.S. policy to pursue or obtain such information." U.S. GAO, *Nuclear Nonproliferation*, 8. In reality, the U.S. government has made significant progress, especially since 2004, in identifying the location and disposition of much U.S.-origin SNM, especially HEU, in foreign countries.

[19] Zimmerman, "The Bomb in the Backyard," 39.

[20] Bunn, "The U.S.-Russia Joint Threat Assessment," 18.

[21] International Atomic Energy Agency, "IAEA Illicit Trafficking Database: Fact Sheet," 2007, www.iaea.org/newscenter/features/radsources/pdf/fact_figures2007.pdf (accessed March 1, 2011).

[22] P. D. Zimmerman and J. G. Lewis, "The Bomb in the Backyard," *Foreign Policy* 157 (2006), 38.

[23] Bill Keller, "Nuclear Nightmares," *The New York Times*, May 26, 2002.

[24] Keller, "Nuclear Nightmares."

[25] The Chechen rebels placed the container of cesium-137 in a Moscow park in 1995, but the device was not detonated. International Atomic Energy Agency, "Inadequate Control of the World's Radioactive Sources,"

It is generally acknowledged that terrorists could transform stolen fissile material into a workable fission bomb.[26] The capability in a specific instance would depend on the type and amount of fissile material and the sophistication of the terrorists. A device producing any level of fission yield would satisfy terrorists, since even a low fission yield would significantly surpass a conventional explosive yield, offering destructive and coercive potential.[27] They would not have to build a sophisticated, miniaturized warhead to sit atop a missile, but instead could make a crude fission bomb that is deliverable by vehicle or boat.[28] Some skeptics argue that "only the best-resourced, organized, and connected groups would stand any chance of constructing their own device,"[29] even with sufficient fissile material in hand. This is true for certain types of fission weapons – for example, using plutonium in an implosion device, like the Nagasaki bomb. By contrast, it is a relatively trivial challenge to make a gun-type weapon, like the Hiroshima bomb, from fresh weapons-grade HEU in metal form.[30]

---

http://www.iaea.org/newscenter/features/radsources/rads_factsheet.pdf (accessed March 1, 2010), 2. Matthew Bunn and Tom Bielefeld, "Reducing Nuclear and Radiological Terrorism Threats," in Proceedings of the Institute for Nuclear Materials Management 48th Annual Meeting, Tucson, Arizona, 8-12 July 2007 (Northbrook, IL: INMM, 2007), http://belfercenter.ksg.harvard.edu/files/Bunn_Bielefeld_INMM2007.pdf, 1.

[26] Matthew Bunn and Anthony Wier, "Terrorist Nuclear Weapon Construction: How Difficult?" *The Annals of the American Academy of Political and Social Science* 607 (September 2006): 133-149; Zimmerman,"The Bomb in the Backyard," 35-37; Matthew Bunn, "Securing the Bomb 2010: Securing All Nuclear Materials in Four Years," Report Prepared for the Nuclear Threat Initiative, April 2010, 16.

[27] Charles G. Bathke et al., "An Assessment of the Attractiveness of Material Associated with a MOX Fuel Cycle from a Safeguards Perspective," Report Prepared for the INMM 50th Annual Meeting, 2009, 1.

[28] Matthew Bunn, "Terrorist Nuclear Weapon Construction," 139.

[29] Ayson, "After a Terrorist Nuclear Attack, 573.

[30] See the memoirs of Manhattan Project physicist Luis Alvarez, *Adventures of a Physicist* (Basic Books, 1987), p. 125: "With modern weapons-grade uranium . . . terrorists, if they had such material, would have a good chance of setting off a high-yield explosion simply by dropping one half of the material onto the other half. . . . Even a high school student could make a bomb in short order." See also, Matthew L. Wald, "Suicidal Nuclear Threat Is Seen at Weapons Plants," *New York Times*, January 23, 2002, which reports: "Frank N. von Hippel, who is a physicist and a professor of public and international affairs at Princeton, said in a telephone interview that a 100-pound mass of uranium dropped on a second 100-pound mass, from a height of about 6 feet, could produce a blast of 5 to 10 kilotons. The Hiroshima bomb, which used uranium, was 12 to 17 kilotons." Both of these assessments assume that the HEU has a purity, shape, and metallic form suitable for such a weapon. If terrorists obtained HEU without all of these characteristics, they might have to further process the HEU or use a more complex design

The local consequences of such a bomb's detonation include the immediate casualties and damage, plus the effects of radioactive fallout. The exact effects would depend on the specifics of the bomb and location.[31] The lowest yield from a fission explosion – known as the "fizzle yield" – would kill an estimated 10,000 people if detonated in a financial center; a better constructed terrorist nuclear weapon detonated in that location could kill 10 times that number.[32]

### C. Sabotage of reactors

The IAEA defines radiological sabotage as "any deliberate act directed against a nuclear or radiological facility or nuclear or radioactive material in use, storage or transport that could directly or indirectly endanger the health and safety of personnel, the public and the environment by exposure to radiation or release of radioactive substances."[33] In this section, we focus on deliberate sabotage of nuclear facilities, such as by aircraft attacks, vehicle bombs, anti-tank weapons, or the disabling of pumps by an insider or an intruder facilitated by an insider who disables locks and alarms.

Terrorists may commit radiological sabotage to provoke public fear, showcase their ability to inflict societal harm, or potentially induce an energy crisis in areas dependent on power reactors.[34] There have been no recent major attacks against nuclear power plants, leading some to argue that nuclear power plants are low priority targets for terrorists. Various reasons are given for this: conventional acts against non-nuclear "soft targets" may suffice to meet the goals of terrorist groups; the sophistication and resources required for a successful attack against a nuclear facility increase the risk of failure; and the potential political consequences of attacking a nuclear facility are uncertain, thus unattractive.[35] Another reason provided by the 9/11 Commission Report is that an attack on a nuclear plant might not have the desired symbolic value for some terrorists.[36] In

---

to produce a functional fission weapon. See Bunn and Wier, "Terrorist Nuclear Weapon Construction."

[31] IAEA, "Inadequate Control of the World's Radioactive Sources," 2.

[32] Zimmerman,"The Bomb in the Backyard," 34.

[33] International Atomic Energy Agency, *Development, Use and Maintenance of the Design Basis Threat*, IAEA Nuclear Security Series No. 10, Implementing Guide (2009), 30.

[34] F. Steinhausler, "Countering Security Risks to Nuclear Power Plants," International Symposium on the Peaceful Applications of Nuclear Technology in the GCC Countries, Jeddah, Saudi Arabia, 2008.

[35] Steinhausler, "Countering Security Risks."

[36] *The 9/11 Commission Report* (2004), 245.

addition, the damage from such sabotage would be regionally concentrated, whereas a terrorist nuclear weapon could be detonated anywhere in the world.[37]

In reality, however, terrorists have considered nuclear power plants as potential targets. There have been reported threats or attempts to blow up or penetrate nuclear reactors in Argentina, Russia, Lithuania,Western Europe, South Africa, and South Korea.[38] According to the 9/11 Commission Report, al Qaeda also considered attacks on a nuclear power reactor as part of its original plan.[39] Research reactors, operated by universities and industry, are particularly vulnerable to sabotage attack because their protection levels tend to be lower than nuclear power plants, but the potential consequences are also considerably smaller.[40] The advent of suicidal terrorists increases the number of potential sabotage targets in nuclear facilities to include components in high-radiation areas because there is no longer a presumption that those areas are inherently "self-protecting."[41]

Radiological sabotage of a nuclear power reactor could have devastating consequences for public health, the environment, and the economy. Edwin Lyman of the Union of Concerned Scientists (UCS) analyzed the consequences of a hypothetical terrorist attack on the Indian Point nuclear power plant located thirty-five miles from New York City. An attack that resulted in a core meltdown and a large radiological release to the environment could cause 44,000 short-term deaths and 500,000 long-term deaths from radiation. He estimated economic damages at $2 trillion.[42]

---

[37] Bunn, "Securing the Bomb 2010," 9.

[38] Matthew Bunn and George Bunn, "Strengthening Nuclear Security Against Post-September 11 Threat of Theft and Sabotage," *Journal of Nuclear Materials Management* (Spring 2002), 3.

[39] *The 9/11 Commission Report* (2004), 245. They ultimately rejected this idea because they mistakenly believed that the airspace around such plants was restricted, so that any attacking aircraft would be shot down prior to impact. This exemplifies the fallacy of the game-theoretic assumption that terrorists possess perfect information, as discussed later in this report.

[40] George Bunn et. al, "Research Reactor Vulnerability to Sabotage by Terrorists," *Science and Global Security* 11 (2003), 89.

[41] Anthony L. Honnellio and Stan Rydell, "Sabotage Vulnerability of Power Plants," *Int. J. Nuclear Governance, Economy and Ecology* 1 (2007), 318.

[42] Edwin S. Lyman, "Chernobyl on the Hudson? The Health and Economic Impacts of a Terrorist Attack at the Indian Point Nuclear Plant," Report Prepared for Riverkeeper, Inc. (September 2004), 5-6.

## D. Sabotage of spent fuel pools

Sabotage of spent fuel pools is related to sabotage of nuclear power plants, which typically store their spent fuel in facilities located on their grounds. Unlike fresh fuel, spent nuclear fuel is highly radioactive but unable to sustain as efficient a nuclear chain reaction. This spent fuel is removed from the reactor and stored in pools of cooling water, and sometimes is subsequently transferred to more permanent dry-cask storage on-site. The pools often lack the shielding and structural protections that the containment provides to the reactor itself, leaving the spent fuel also more vulnerable to sabotage by terrorists.[43]

A 2006 report by the National Academy of Sciences concluded that a successful terrorist attack on spent fuel pools would be difficult, but possible.[44] In the absence of a centralized national storage facility for spent fuel, nuclear power plants often maintain their spent fuel pool inventories at amounts beyond the original design limits of the pool.[45] A terrorist with enough technical knowledge and means could drain a spent fuel pool, triggering a cladding fire that could result in the release of large amounts of radioactive material.[46] This is similar to what occurred in 2011 in Fukushima, Japan, when an earthquake's effects drained the spent fuel pools. According to Beyea, Lyman, and von Hippel, a terrorist attack on a spent fuel pool could cause thousands of deaths from cancer, and economic damages in the hundreds of billions of dollars.[47] In the wake of the NAS report, U.S. utilities reportedly have taken some measures that may somewhat mitigate this risk, but not eliminate it.[48] An attack on dry cask storage would also result in the release of radioactive material, although in smaller amounts due to design differences.

---

[43] Mark Holt and Anthony Andrews, "Nuclear Power Plant Security and Vulnerabilities," RL34331, Congressional Research Service, August 23, 2010, http://www.fas.org/sgp/crs/homesec/RL34331.pdf, 6-7.

[44] National Academy of Sciences, "Safety and Security of Commercial Spent Nuclear Fuel Storage: Public Report," 2006, 3.

[45] F. Steinhausler, "Managing Security Risks to Nuclear Fuel Cycle: Current Knowledge and Challenges Ahead," *Atoms for Peace: An International Journal* 1 (2007), 278.

[46] Kevin Crowley, "Are Nuclear Spent Fuel Pools Secure?" Transcript of First Rountable on Nuclear Security Issues, Council on Foreign Relations Washington DC, June 7, 2005, http://www.cfr.org/weapons-of-mass-destruction/nuclear-spent-fuel-pools-secure/p8967.

[47] J. Beyea, E. Lyman, and F. von Hippel, "Damages from a Major Release of $^{137}$Cs into the Atmosphere of the United States," *Science and Global Security* 12 (2004), 125-136.

[48] Matthew Bunn, personal communication, May 7, 2012. These measures include putting less radioactive fuel assemblies in between more radioactive ones, and improving the ability to refill pools with water in an emergency.

## E. Insider Threat

Implicit in the four threats described above is the possibility of an active or passive insider using knowledge of facilities to assist terrorists in their actions. Passive insiders could provide information about weaknesses in the plant or operations, allowing terrorists to magnify their impact.[49] An active insider could deactivate alarm and emergency safety systems or deliver explosives to sensitive areas of the nuclear facility.[50]

A recent incident highlights the immediacy of the insider threat problem. An American citizen, suspected of al Qaeda membership, worked for five different US nuclear power plants from 2002 to 2008 after passing federal background checks.[51] This incident is particularly disturbing because nuclear power plants depend heavily on their employee screening processes to combat the insider threat.[52] Another incident that allegedly involved insider information was the break-in at the Pelindaba nuclear reactor and research center in South Africa. In November 2007, four gunmen spent 45 minutes inside the heavily guarded facility, eventually breaking into the emergency control center at the middle of the facility. They fled when an alarm was triggered. At the same time, another four men tried but failed to break-in from the other side of the facility, suggesting a coordinated attack. The ease with which the attackers disabled multiple layers of security strongly suggests the use of insider information.[53]

## F. Proven Terrorist Capabilities

Formulating a comprehensive risk assessment strategy entails deciding which terrorist capabilities and attack scenarios are credible. Although the number of terrorist groups with serious nuclear aspirations is thought to be relatively low,[54] recent attacks show

---

[49] Honnellio, "Sabotage Vulnerability of Power Plants," 313.

[50] Bunn et al.,"Research Reactor Vulnerability," 94.

[51] Brian Ross, Rhonda Schwartz, and Megan Chuchmach, "New Terror Report Warns of Insider Threat to Utilities," *ABC News*, July 20, 2011, accessed March 1, 2012, http://abcnews.go.com/Blotter/terror-alert-warns-insider-threat-infrastructure/story?id=14118119#.T1gKTcx99do.

[52] The NRC describes its employee hiring process as much more comprehensive since 9/11. "Potential employees are screened through numerous databases, checked for, among other things, mental-health problems, criminal records and questionable behavior in previous jobs." Bruce Crumley, "Are These Towers Safe?" *TIME*, June 12, 2005, accessed March 1, 2012, http://www.time.com/time/magazine/article/0,9171,1071249,00.html.

[53] Micah Zenko, "A Nuclear Site is Breached," *The Washington Post*, Dec. 20, 2007, accessed March 1, 2012, http://www.washingtonpost.com/wp-dyn/content/article/2007/12/19/AR2007121901857.html.

[54] Ayson, "After a Terrorist Nuclear Attack," 573. There are five terrorist groups that may be capable of acquiring and using nuclear weapons – Al Qaeda, North Caucasus-

terrorist organizations becoming increasingly sophisticated in their planning. An examination of major terrorist incidents sheds light on the operational capabilities of various individuals and groups and the level of threat that nuclear assets should be protected against.

***Mumbai 2008***
Ten armed men conducted a series of shooting and bombing attacks across Mumbai, India, killing 164 and injuring over 300. The Indian Government implicated Pakistan-based Lashkar-e-Tayyiba in the attacks. The gunmen used AK-56 automatic rifles (Chinese versions of the AK-47), 9-mm pistols, hand grenades, and improvised explosive devices. The attacks used multiple assault teams to attack multiple targets simultaneously, differing from previous large-scale Islamic terrorist attacks in that the primary weapon was the gunman, not the suicide bomber.

***London 2005***
Four suicide bombers struck in central London in 2005, killing 52 people and injuring more than 770. The attackers detonated four homemade bombs, targeting civilians using the public transportation system. The four men were deemed to be homegrown Islamic terrorists, working in isolation from any organized terrorist group.

***Madrid 2004***
Ten bombs on four commuter trains were remotely detonated using mobile phones, killing 191 people and injuring 1,800. The Spanish government attributed the attack to a group of local Islamic extremists inspired by radical Islamic websites and perhaps by al Qaeda propaganda. Recent evidence, however, connects the bombing to senior al Qaeda leadership in Pakistan.[55]

***New York City / Washington DC 2001***
Nineteen al Qaeda terrorists hijacked four commercial jets, crashing two into the World Trade Center, one into the Pentagon, and one into a field in rural Pennsylvania (due to passenger intervention). Total dead and missing numbered almost 3,000. Operating as four well-coordinated teams, the terrorists used box cutters and mace to seize control of the planes and direct them to the intended targets in three of four cases. The simultaneous attacks were unprecedented in their scope and lethality.

***USS Cole, Yemen, 2000***
Two suicide bombers used a small boat armed with explosives to attack the US Navy destroyer while it was refueling in Aden, Yemen. The explosion killed 17 crewmembers, injured 38, and caused serious damage to the ship. The attacks have been linked to al Qaeda.

---

based separatists, Lashkar-e-Tayyib, Hezbollah, and the Taliban. Belfer Center, "Nuclear Terrorism Fact Sheet."

[55] Seth G. Jones, "The Future of al Qaida," RAND, May 2011, 7.

The above survey of terrorist attacks illustrates the past reliance of terrorists on conventional, fairly low technology tools, although in creative ways to maximize their symbolic and lethal effect. As one analyst put it, "it seems to be a general historical regularity that terrorists tend to prefer weapons that they know and understand, not new, exotic ones."[56] This is somewhat overstated, however, because 9/11 demonstrated that terrorists could use box cutters to transform a jumbo jet into a weapon of mass destruction. Terrorists in Japan and elsewhere have also attempted chemical weapons attacks, another major technological innovation. Disturbingly, as elucidated below, the NRC's design basis threat (DBT) does not even posit that terrorists would have some of the conventional weapons that they have used in the past.[57]

In 2008, the head of the CIA identified al Qaeda as the agency's "number one nuclear concern." After the death of Osama bin Laden, al Qaeda has become an even more diffuse and global organization, and there is some debate regarding the particular threat al Qaeda now poses to the United States. Some contend that because U.S. forces have eliminated much of the al Qaeda leadership in Afghanistan and Pakistan, the organization has shifted from an operational role to a mere ideological and motivational inspiration for smaller autonomous cells and individuals.[58] Under this theory, homegrown "micro-actors" pose the most serious threat to the United States because they "may be new to the terrorism landscape, may be technologically savvy and small, decentralized, and without regular communication with other groups or cells" [SIC].[59] These micro-actors are more likely to use conventional weapons like bombs and bullets, rather than exotic alternatives, it is argued.[60] A contending theory is that al Qaeda leadership now based in Pakistan poses a serious potential threat to the United States.[61] Many of the attacks described above can be linked to al Qaeda or its allies operating out of Pakistan, at least as inspiration.[62] Under this theory, al Qaeda continues to pose a credible threat to U.S. security.

This discussion raises at least two questions. First, how should counter-terror resources be divided between more probable conventional threats and less likely but potentially catastrophic nuclear threats? Second, should the DBT posit only the lesser capabilities that micro-actors would bring to the table, or the greater capabilities that Al Qaeda has demonstrated repeatedly since the late 1990s?

---

[56] Mueller, "Reactions and Overreactions to Terrorism."

[57] See subsequent section of this paper: "IV. A. Nuclear Regulatory Commission."

[58] Raphael Perl, "Trends in Terrorism: 2006," RL33555, Congressional Research Service, updated March 12, 2007, 6.

[59] Perl, "Trends in Terrorism," 6.

[60] Perl, "Trends in Terrorism," 6.

[61] Jones, "The Future of al Qaida," 6.

[62] Jones, "The Future of al Qaida," 6.

## III. CURRENT DBT – COMPARING U.S. AGENCY APPROACHES

Three U.S. government agencies are charged with maintaining security over the nation's nuclear assets – the Nuclear Regulatory Commission (NRC), the Department of Energy (DOE), and the Department of Defense (DOD). All three agencies follow similar procedures for developing physical protection requirements, but interestingly do not end up with the same requirements. Each agency starts from a threat assessment based on intelligence analysis, next establishes a comprehensive list of attributes for potential insider/outsider adversaries – the Design Basis Threat (DBT) – and then attempts to ensure that physical protection measures can defend against that threat.

It is important to remember that the DBT, by definition, is only the level of threat against which facility operators themselves are required to design protections. The government may believe that the credible level of threat is greater and, if so, may or may not take additional measures to address that greater threat. In practice, the DBT typically comprises a lower level of threat than the credible, worst-case threat to a facility, which presumably would require the country's other defensive assets to address, as discussed further below.

All three agencies derive their initial threat assessments from National Intelligence Estimates issued by the Director of National Intelligence. These estimates enumerate the current and projected threats to U.S. nuclear assets. The threat assessment provides a list of adversary capabilities organized by type of actor: foreign states, non-state foreign actors, and domestic threats. The three agencies use this broad threat assessment to tailor their assessment of local threats. This tailoring includes removing or downgrading threats deemed unlikely for a particular region and adding local threats not considered in the national assessment. This approach produces a posited threat that is useful in the following ways: it provides a baseline for assessing the effectiveness of proposed changes to physical protection systems; it creates a threat profile to compare against subsequent information about actual adversaries, which could lead to updating the threat profile; and it standardizes the level of protection required for nuclear facility physical protection systems, at least within each agency.[63] The following is an overview of each agency's approach to threat assessment.

### A. Nuclear Regulatory Commission

The U.S. Nuclear Regulatory Commission is an independent government agency charged with regulating the civilian use of nuclear materials, including special nuclear material (SNM).

#### *Asset characterization*

The NRC regulates the following in the United States: 104 commercial nuclear power reactors and 32 licensed nuclear research and test reactors; the production of nuclear fuel for these reactors; the storage, transportation, and disposal of spent fuel and other

[63] Steinhausler, "Countering Security Risks to Nuclear Power Plants."

radioactive waste; and the transportation of other radioactive materials. Additionally, the NRC is responsible for licensing and inspecting the spent fuel storage facilities used by commercial nuclear power plants. Included in its above responsibilities, the NRC regulates the physical security of substantial quantities of DOE's SNM, when that material is under contract to an NRC-licensed facility, such as a company that fabricates HEU fuel for research or naval propulsion reactors,[64] or an NRC-licensed research reactor.

***Threat Assessment***

The Commission produces the Design Basis Threat (DBT) based on a domestic threat assessment by NRC staff.[65] The DBT is a general-level overview of the potential threats of theft and sabotage, whether at fixed sites or in transit. The unclassified version of the DBT is codified in Chapter 10, Part 73 of the Code of Federal Regulations. The most recent DBT amendment was adopted in 2007, and provides heightened standards in response to the terrorist attacks of September 11, 2001. The DBT divides threats into two major categories: theft of special nuclear material and radiological sabotage.[66]

Unlike power reactors, NRC-licensed research and test reactors are not required to protect against this DBT.[67] This has some logic for the risk of radiological sabotage because the potential consequences of such an attack are orders of magnitude greater at a power reactor. But it is illogical for the risk of theft, because the consequences of terrorists obtaining fissile material may be identical whether stolen from a research reactor or power reactor.

The latest revision of the DBT assumes the following attributes of an adversary force:

---

[64] The two such companies are Babcock & Wilcox and Nuclear Fuel Services. Annually, these two companies process an estimated two tons of HEU for naval reactor fuel alone. Chunyan Ma and Frank von Hippel, "Ending the Production of Highly Enriched Uranium for Naval Reactors," *The Nonproliferation Review* (Spring 2001): 92.

[65] U.S. GAO, *Nuclear Power Plants: Efforts Made to Upgrade Security, but the Nuclear Regulatory Commission's Design Basis Threat Process Should be Improved*, GAO-06-388 (Washington, DC: GAO, 2006), http://www.gao.gov (accessed March 1, 2011), 12.

[66] 10 C.F.R. § 73.1.

[67] See, Edwin Lyman and Alan Kuperman, "A Re-Evaluation of Physical Protection Standards for Irradiated HEU Fuel," paper presented at the 24th International Meeting on Reduced Enrichment for Research and Test Reactors (RERTR), Bariloche, Argentina, 5 November 2002, http://www.nci.org/02NCI/11/rertr2002.pdf. See also, Bunn et al., "Research Reactor Vulnerability to Sabotage," 89: "The NRC is inhibited from imposing strict regulations on research reactors by the U.S. Atomic Energy Act, which allows the NRC to impose 'only such minimum amount of regulation. . . as will permit the Commission to fulfill its obligations under this Act . . .'" As a result, research reactors generally do not have to protect against radiological sabotage or provide an armed response to an attack.

multiple groups attacking from multiple entry points; willing to kill or be killed; possessing knowledge about target selection; aided by active and/or passive insiders; employing a broad range of weapons and equipment, including ground and water vehicles. The DBT does not require nuclear power plants to defend against aircraft attacks.[68] The NRC requires facilities to provide site-specific plans to address the DBT. Prior to the enhanced DBT of 2007, these plans typically comprised a "10-member armed response force to deter an external attack, a background investigation program for employees to protect against the insider threat, and strict measures to control access of individuals and vehicles near 'vital' areas of the reactor," according to George Bunn and co-authors.[69]

## B. Department of Energy

DOE's National Nuclear Security Administration (NNSA) works in conjunction with the Department of Defense to develop, transport, and secure the U.S. stockpiles of nuclear weapons and of special nuclear materials for both weapons and naval propulsion reactors. DOE is also responsible for its own research reactors, including two at Idaho and Oak Ridge National Laboratories that still use HEU fuel.

### *Asset characterization*

NNSA conducts operations at eight sites across the country. Three are DOE national laboratories that engage in nuclear weapons-related work including the following: support of stockpile stewardship; development, testing, and production of non-nuclear components; and maintaining safety and reliability of the nuclear explosives package in nuclear weapons. The five other sites are used to sustain the nuclear arsenal, entailing tasks such as the following: producing weapons materials, rehabilitating older weapons, and simulating weapons tests. Six of the sites contain SSNM that must be protected against theft.[70]

### *Threat Assessment*

DOE revised its DBT four times between 2003 and 2008, ultimately renaming it the Graded Security Protection (GSP) policy in November 2008. The GSP, although conceptually identical to DOE's previous DBT, reportedly posits a smaller and less capable threat against sites possessing SSNM.[71] There is currently no deadline for implementing the new GSP, and sites are still required to defend against the 2003 DBT while they plan for implementation of the 2008 revision. The 2003 DBT requires most of

---

[68] 10 C.F.R. § 73.1.

[69] Bunn et. al, "Research Reactor Vulnerability to Sabotage," 90.

[70] Pantex, Savannah River Site, Los Alamos, Y-12, Nevada Test Site, Idaho National Laboratory.

[71] U.S. GAO, *Nuclear Security: DOE Needs to Address Protective Forces' Personnel System Issues*, GAO-10-275 (Washington, DC: GAO, 2010), http://www.gao.gov (accessed March 1, 2011), 7.

the DOE sites to maintain "denial protection strategies" to protect SSNM. Specifically, the standard is most stringent for sites that store nuclear weapons and for SSNM in transit, where attackers must be prevented from achieving hands-on access to the material. For SSNM at fixed sites, DOE requires a slightly laxer standard, in which attackers must be denied adequate time to complete "malevolent acts." Finally, if attackers do gain access to SSNM, DOE requires that forces be available to engage in recovering the material.[72]

## C. Department of Defense

Within the Department of Defense (DOD), most of the nuclear assets -- nuclear weapons and HEU fuel – are under control of the Air Force and Navy.

***Asset characterization***

The Air Force's nuclear assets are controlled by four major commands, with nuclear weapons in the United States and abroad. One command controls three installations to maintain ICBM fields and missile silos located in five U.S. states. Another has authority over two installations for the storage and maintenance of nuclear weapons used on B-2 and B-52 aircraft. A third maintains an underground storage and maintenance facility for nuclear weapons. The fourth is responsible for U.S. nuclear weapons located on installations at a handful of bases in Europe. The Navy oversees two weapons facilities to maintain the nuclear missile inventory for the submarine platform. The Navy also takes possession from DOE of HEU fuel for the reactors that propel its nuclear submarines and aircraft carriers. The Army also has one HEU-fueled research reactor, and the Navy has several HEU-fueled training reactors.[73]

***Threat Assessment.***

DOD issues the Nuclear Security Threat Capabilities Assessment (NSTCA), its DBT equivalent. Navy and Air Force operational commands take this national-level guidance and tailor it to reflect local threats at the installation level. The NSTCA focuses principally on "threats from international terrorist groups, state actors, and domestic groups acting solely within the United States."[74] Based on historical precedent, the NSTCA lists the adversaries deemed to be credible threats to the nuclear weapons held by DOD. DOD divides these adversaries into classes of threat based on their known capabilities. These distinctions enable DOD to identify which classes of threat the facilities should be required to protect against, in contrast to greater threats that are the

---

[72] U.S. GAO, *Nuclear Security*, 18.

[73] On this last point, see Matthew Bunn & Eben Harrell, "Consolidation: Thwarting Nuclear Theft," Harvard University, March 2012, http://belfercenter.ksg.harvard.edu/files/Consolidation_Thwarting_Nuclear_Theft_corrected.pdf, 18-19.

[74] U.S. GAO, *Homeland Defense: Greater Focus on Analysis of Alternatives and Threats Needed to Improve DOD's Strategic Nuclear Weapons Security,* GAO-09-828 (Washington, DC: GAO, 2009), http://www.gao.gov (accessed March 1, 2011), 14.

responsibility of the U.S. defense community as a whole.

## IV. PREVIOUS CRITIQUES OF DBT'S POSITED ATTACK

### A. Nuclear Regulatory Commission

The NRC views nuclear security as a balancing of risks and costs, with the understanding that achieving a "zero" level of risk is impossible.[75] Since 2001, the U.S. nuclear industry has spent over $2 billion on security enhancements to their physical protection systems.[76] However, it is difficult to know if those enhancements have been adequate. As Matthew Bunn writes, "no one really knows how clever a plan, with how many attackers, what weapons, or what capabilities, terrorists might be able to bring to bear."[77] The NRC ostensibly attempts to estimate that through its DBT. But criticism of the NRC's DBT focuses on the number of adversaries, their weapons, and the exclusion of air attacks and some sea attacks.

***Number of adversaries: insiders, outsiders, separate groups coordinating***
Prior to the revisions following September 11, 2001, the NRC's DBT assumed one team of three individuals, aided by a passive insider who provided information but did not participate in the attack. The numbers were kept relatively low because intelligence agencies generally assumed that they themselves were capable of detecting conspiracies of more than a few members.[78] This assumption was proven wrong by the events of 9/11 when 19 hijackers, acting in four independent teams, planned and executed a plot without prior detection by authorities.

Although the details of the revised DBT are classified, one source reports that the assumed number of attackers was only increased to "less than double the old figure and a fraction of the size of the 9/11 group" of 19 hijackers.[79] Another source specifies it as "five or six well-armed terrorists, possibly working in conjunction with an insider or

[75] NRC News, "Risk Management and Security," Prepared Remarks for NRC Commissioner Dale Klein, Raleigh Grand Challenge Summit 2010, North Carolina State University (March 5, 2010).

[76] Rebecca Mowbray, " Nuclear Security Upgrades Continue: Entergy's Post-9/11 Work Still Underway," *Times-Picayune (New Orleans)*, March 28, 2010, E01.

[77] Matthew Bunn, "A Mathematical Model of the Risk of Nuclear Terrorism," *The Annals of the American Academy of Political and Social Science* 607 (September 2006), 111.

[78] Edwin S. Lyman, "Security Since September 11th" *Nuclear Engineering International* (March 2010), 16.

[79]Crumley, "Are These Towers Safe?"

two."[80] This number reflects the NRC's assumption that only one terrorist cell would attack a plant.[81] The Nuclear Energy Institute (NEI), a nuclear industry lobbying group, defends this assumption on grounds that the 9/11 attacks represent four separate attacks of three or four terrorists each, not an attack by nineteen terrorists.[82] Critics say this does not adequately represent the present threat, which should take into account the size of the entire 9/11 attack force, and at a minimum posit an attack from a "squad size" of adversaries (12-14 personnel).[83]

The insider threat is downplayed in two ways, say critics. First, although the revised DBT reportedly does consider one or two active (i.e., violent) insiders working with outside attackers, it does not contemplate a larger conspiracy of insiders, which is a common phenomenon in past thefts from highly secure, non-nuclear facilities.[84] Second, when the NRC evaluates the adequacy of security measures at power reactors by requiring force-on-force tests, these exercises may not simulate even the tiny number of active insiders contemplated by the revised DBT.[85] (A related criticism is that at research reactors licensed by the NRC, no force-on-force tests at all are conducted, even if the sites contain HEU, because such facilities are not required to defend against the DBT.)[86] Thus, according to critics, the U.S. government both underestimates the insider threat and

---

[80] Alexandra Marks, "Nuclear-plant security: Is It Enough?" *Christian Science Monitor*, April 4, 2006.

[81] Danielle Brian, "Statement to the House Subcommittee on National Security, Emerging Threats and International Relations, Hearing on Nuclear Security: Has the NRC Strengthened Facility Standards Since 9/11?" April 4, 2006.

[82] Marks, "Nuclear-plant security."

[83] Danielle Brian, "Statement to the House Subcommittee."

[84] Robert Reinstedt and Judith Westbury, *Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs*, N-1498-SL (Santa Monica, CA: RAND, 1980). Bruce Hoffman et al., *Insider Crime: The Threat to Nuclear Facilities and Programs*, R-3782-DOE (Santa Monica, CA: RAND, 1990). Matthew Bunn, "Setting Priorities: A Risk-informed Approach to Reducing the Global Danger of Nuclear Theft," unpublished paper, December 31, 2008.

[85] Edwin S. Lyman, Union of Concerned Scientists, testimony submitted to the Subcommittee on Clean Air, Climate Change and Nuclear Safety, Committee On Environment And Public Works, U.S. Senate, May 26, 2005, p. 11. "Protective strategies should be developed with due consideration to the damage that could be caused by an active insider in any capacity, and those strategies should be fully tested in the FOF [force-on-force] program." http://www.ucsusa.org/assets/documents/nuclear_power/lyman_testimony_5-26-05.pdf.

[86] Edwin Lyman, Union of Concerned Scientists, "Using Bilateral Mechanisms to Strengthen Physical Protection Worldwide," paper prepared for meeting of the Institute of Nuclear Materials Management, 2004, http://www.ucsusa.org/nuclear_weapons_and_global_security/nuclear_terrorism/technical_issues/strengthening-protections-for.html.

fails to assure protection against even that underestimated threat. But a U.S. nuclear-industry representative has responded, regarding the force-on-force tests at power reactors, that "in the exercises we assume there will be insider support. We provide adversaries with inside information."[87] This suggests that the tests do contemplate at least a passive insider.

The NRC also takes a graded approach to security by requiring a higher level of protection for sites considered to have greater potential consequences from an attack. As a result, the DBT for theft of nuclear material assumes a greater threat than for radiological sabotage. Additionally, the NRC believes terrorists require greater capabilities to commit theft than sabotage, since theft necessarily implies defeating security measures to both enter and exit the facility. Sabotage by a suicidal attacker only requires defeating security measures to enter.[88]

Until the NRC requires licensees to guard against a 9/11-sized attack force, critics argue, the NRC is effectively depending on protection by other government forces, but these other forces may not be available or sufficient.[89] For example, according to the Project on Government Oversight (POGO), timelines of the DOE indicate that it would take approximately 1.5 to 2 hours for a SWAT team to respond and fully engage against an on-site attack, which could be too late to avert theft or sabotage.[90] At several NRC-licensed research reactors that still use HEU fuel, the primary threat is theft. At power reactors and other research reactors, the main threat is radiological sabotage. The Union of Concerned Scientists projects that a team of well-trained terrorists, after gaining access to a power reactor site, could cause enough damage within a matter of minutes to produce a core meltdown that could disperse enormous amounts of radiation.[91]

---

[87] Philip Leggiere, "Counternarcotics, Terrorism & Intelligence Infrastructure Security: The Lessons of Fukushima," *Homeland Security Today*, July 13, 2011, quoting Chris Earls, director of security at the Nuclear Energy Institute, http://www.hstoday.us/focused-topics/counternarcotics-terrorism-intelligence/single-article-page/infrastructure-security-the-lessons-of-fukushima/41674de9c0fa1835682e6e630da29821.html.

[88] U.S. GAO, *Nuclear Power Plants,* 19.

[89] David Lochbaum and Edwin Lyman, "UCS Comments on NRC's 'Design Basis Threat' Rule," January 23, 2006, http://www.ucsusa.org/assets/documents/nuclear_power/designbasisthreatcomments.pdf (accessed March 1, 2012).

[90] Danielle Brian, "Statement to the House Subcommittee."

[91] Edwin Lyman, "Statement to the Senate Committee on Energy and Natural Resources, Hearing on S. 512, The Nuclear Power 2021 Act, and S. 1067, The Nuclear Energy Research Initiative Improvement Act of 2011," June 7, 2011.

***Weapons***

The latest revision of the DBT did not include two weapons commonly used by sub-state adversaries – rocket-propelled grenades and 50-caliber sniper rifles – which were originally on a list of weapons that intelligence staff proposed to require nuclear facilities to protect against.[92] When the NRC finalized this revised DBT, however, it eliminated these two weapons, reflecting industry input.[93] POGO argues that this decision was based on pressure from the nuclear industry to keep down costs.[94] If the weapons were retained in the DBT, nuclear facilities would have had to upgrade their existing defenses. For example, bullet-resistant ballistic shield currently used at power reactors is inadequate against a 50-caliber rifle with armor-piercing rounds.

POGO notes that rocket-propelled grenades can be purchased cheaply and quickly in international weapons markets and shipped with relative ease to the United States, making them a very plausible weapon for a terrorist attack on U.S. nuclear facilities. POGO contends that this weapon was removed from the DBT not due to changing intelligence assessments but rather the prospective cost to industry of protecting against them. "This is not a debate over what the intelligence community believes, it is a debate over how much the nuclear industry should have to pay."[95] The nuclear industry's trade association, NEI, responds that the reported removal of this weapon from the DBT would not increase the vulnerability of nuclear power reactors because their existing containments provide protection against rocket-propelled grenades, but that ignores the use of such weapons to gain access to a plant to stage additional attacks.[96] If nuclear power plants already were able to defend against attacks using this weapon, the NRC would have had no reason to remove it from the proposed DBT when the industry complained.

***Airborne & seaborne attacks***

Existing US nuclear power plants were designed to withstand extreme environmental events like hurricanes and earthquakes, but their design analysis did not consider deliberate attacks using fuel-laden airliners.[97] The NRC deems aircraft attacks beyond the DBT and thus does not require nuclear plants to take additional steps to protect against them, despite the precedent of 9/11. The NRC excludes aircraft from the DBT "because the weaponry needed to defend against such a threat, surface-to-air missiles or fighter aircraft, cannot be possessed by the private security forces that protect commercial nuclear plants. The responsibility for such a threat belongs with the U.S. government."

---

[92] Lyman, "Security Since September 11th," 16.

[93] U.S. GAO, *Nuclear Power Plants*, 20-21.

[94] Danielle Brian, "Statement to the House Subcommittee."

[95] Danielle Brian, "Statement to the House Subcommittee."

[96] Marks, "Nuclear-plant security."

[97] Holt, "Nuclear Power Plant Security and Vulnerabilities," 4.

According to the NRC, "the active protection against airborne threats is addressed by other federal organizations, including the military."[98]

This is consistent with the "enemy of the state" doctrine, established in U.S. regulations in 1967. Under this principle, the nuclear power industry is not responsible for protecting against "(a) attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other person, or (b) use or deployment of weapons incident to U.S. defense activities."[99] The doctrine clarifies that private nuclear facilities are not responsible for "defending against attacks that typically could only be carried out by foreign military organizations,"[100] which are the responsibility of the federal government. The industry thus relies on elements of the government, like the FAA and North American Aerospace Defense Command, to detect, deter, and defend against airplane attacks.[101] The NRC argues that these agencies offer sufficient protection, precluding any requirement for plant operators to take additional protective measures.[102]

But the Commission also offers another, somewhat contradictory explanation for the DBT's exclusion of aircraft attacks, asserting that the "NRC has already required its licensees to take steps to mitigate the effects of large fires and explosions from any type of initiating event."[103]

Also somewhat contradictory, the NRC has required that all future power reactors be designed to mitigate attacks by commercial aircraft, but has not required existing reactors to make retrofits to address that threat.[104] Given that the NRC deems aircraft attacks as outside the DBT, it describes the additional requirement for future reactors as merely adding an additional safety margin. "The objective of this rule is to require nuclear power plant designers to perform a rigorous assessment of design features and functional

---

[98] NRC, "NRC Proposes Adding Plane Crash Security Assessments to New Reactor Design Certification Requirements," News Release No. 07-053, April 24, 2007. NRC, "NRC Approves Final Rule Amending Security Requirements," News Release No. 07-012, January 29, 2007.

[99] 10 C.F.R. § 50.13.

[100] NRC, "Design Basis Threat," *72 Federal Register*, March 19, 2007, 12714. The doctrine originated to address concerns that Cuba might launch attacks against nuclear power plants in Florida.

[101] NRC, "NRC Approves Final Rule Amending ABWR Reactor Design Certification to Include Consideration of Aircraft Impacts," News Release No. 11-207, November 1, 2011.

[102] Danielle Brian, "Statement to the House Subcommittee."

[103] NRC, "NRC Approves Final Rule Amending Security Requirements," News Release No. 07-012, January 29, 2007.

[104] Holt, "Nuclear Power Plant Security and Vulnerabilities," 5.

capabilities that could provide additional inherent protection to avoid or mitigate, to the extent practical and with reduced reliance on operator actions, the effects of an aircraft impact."[105]

A nuclear policy analyst at Greenpeace cites a 1982 study by Argonne National Laboratory to argue that an airliner could, contrary to NRC claims, actually penetrate the containment of a nuclear power plant.[106] NRC counters that the Argonne study is old and flawed, and that new studies done with better computer models show the plants are safe.[107] If the NRC's claim is correct that existing containments make power reactors immune from aircraft attack, it not clear why the commission would require enhanced protections in the design of future reactors.

The NRC's response to the threat of airplane attacks reflects logical inconsistencies that likely result from pressure by the nuclear industry to limit costs. The fact that future power plant designs must protect against aircraft attacks is an acknowledgement by the NRC that the threat is credible. Despite this, the Commission has not required existing plants to take similar protections. Existing power plants are required to have plans in place to combat fires and damage caused by an airplane crash, but this would not guarantee against a core meltdown or radiological releases. Since the NRC obviously believes that an aircraft attack against a power plant is plausible and cannot necessarily be prevented by the U.S. government, that threat should logically be included in the DBT for existing reactors too.

More broadly, according to POGO, the "enemy of the state" doctrine may be outdated and impractical, because government forces in many cases would be unable to respond quickly enough to avert a disaster.[108] The doctrine might make sense for national-level enemies, such as foreign armies, which could launch attacks on a scale that the private sector obviously could not defend against, but not for sub-state enemies such as terrorist groups. The Union of Concerned Scientists says the reliance on outside agencies to protect against airborne attacks "utterly fails to meet the NRC's fundamental goal of defense-in-depth."[109] Additionally, the NRC reportedly does not require a no-fly zone

---

[105] Nuclear Regulatory Commission, "Final Rule: Consideration of Aircraft Impacts for New Nuclear Power Reactors," Rulemaking Issue Affirmation, SECY-08-0152, October 15, 2008, 2.

[106] "Comments on Committee to Bridge the Gap's Proposed Rule on Nuclear Security and the NRC's Design Basis Threat," Docket No. 73-12, January 24, 2005.

[107] Steve Hargreaves, "The Threat of Nuclear Meltdown: The government says nuclear power is safe, but others say an airplane frontal assault would be big trouble," *CNNMoney.com*, November 12, 2009, http://money.cnn.com/2009/11/12/news/economy/nuclear_security/index.htm (accessed March 1, 2012).

[108] Danielle Brian, "Statement to the House Subcommittee."

[109] Lochbaum, "UCS Comments on NRC's 'Design Basis Threat.'"

around nuclear plants, except during times of elevated threats, because it would impose costs on the aviation industry.[110]

The nuclear industry also persuaded the NRC to reduce the size of the vehicle bomb included in the DBT, on grounds that the original size would not be "reasonable or practical" to defend against.[111]

The Union of Concerned Scientists also criticizes the DBT's approach to the threat of waterborne attacks. Nuclear power plants that use adjacent bodies of water for the cooling of essential equipment and nuclear fuel are vulnerable to such attacks. In such cases, UCS believes that the NRC has taken inadequate measures to protect critical but vulnerable assets such as cooling-water intake structures. By contrast, UCS cites the actions of the Department of Defense, which in response to its DBT required the placement of floating barriers around anchored ships and nuclear submarines.[112] These U.S. Navy protections are presumably to defend against terrorists, such as those who attacked the USS Cole in the year 2000. Terrorists could equally target the critical parts of U.S. nuclear reactors adjacent to bodies of water, which the NRC's DBT does not require to be protected. The operator of one nuclear power plant rejected an offer by the Department of Homeland Security to install free barriers for protection against waterborne threats, apparently based on the costs of maintaining the barriers.[113] By statute, however, the NRC is not supposed to consider economic costs in ensuring the adequate protection of public health and safety.[114]

**B. Department of Energy**

The DOE assumes an attack force three times the size of the NRC's DBT and includes the weaponry rejected by the NRC.[115] But the DOE's DBT reportedly varies by facility, and is more stringent where nuclear weapons or fissile material are stored or transported. Apparently, this is because DOE believes the potential consequences from theft of a nuclear weapon or SNM are greater than those from radiological sabotage, thereby justifying greater defenses.[116] Although this is unarguably true for the "potential" consequences, it is not necessarily true for the "expected" consequences, as elucidated below.

---

[110] Lyman, "Chernobyl on the Hudson?" 7.

[111] U.S. GAO, *Nuclear Power Plants*, 20-21.

[112] Lochbaum, "UCS Comments on NRC's 'Design Basis Threat.'"

[113] Lyman, "Security Since September 11th," 18.

[114] Union of Concerned Scientists v. U.S. Nuclear Regulatory Commission, 824 F.2d 108, 115 (D.C. Cir. 1987); 42 U.S.C.S. § 2232(a).

[115] Danielle Brian, "Statement to the House Subcommittee."

[116] Danielle Brian, "Statement to the House Subcommittee."

POGO has criticized the DOE's most recent DBT – known now as GSP – for being a more malleable standard than its previous DBT. The group contends that the GSP sets a "floating bar" for the posited level of attack that can be raised or lowered depending on the particular site conditions, even for facilities containing the same type of nuclear material. This contrasts with the NRC's DBT, which sets a baseline threat that all facilities must protect against. POGO attributes the change to cost-cutting, asserting that "the GSP emerged after it was clear that several DOE sites could not meet the DBT and did not want to spend the funds to meet it."[117]

**C. Department of Defense**

The DOD's NSTCA requires local commands to tailor the nationally issued threat assessment to reflect specific regional threats. The GAO has criticized DOD for its implementation of the NSTCA at the local level, asserting that the commanders at DOD installations lack the proper guidance and capabilities to tailor the national level threat to individual facilities. Compared to DOE's approach, DOD provides less comprehensive guidance for implementation at the local level, despite the fact that officials at local installations are unqualified to exercise discretion, according to GAO. "Because of the uncertain and unpredictable nature of terrorist threats, installation officials were reluctant to eliminate any threat listed in the national assessment, and individuals developing local threat assessments had limited guidance and were not trained as intelligence analysts."[118] As a result, GAO argues, the threat assessments used by DOD facilities may incompletely reflect the installation's actual vulnerabilities by assuming too great a threat.

The GAO has also criticized DOD for being too "prescriptive" in the implementation of its nuclear weapons security policies, by barring consideration of suitable alternatives.[119] For example, DOD specifies that the barrier constructed around installations must be seven feet tall and made from chain-link material, permitting little flexibility to explore other approaches. When DOD rules do permit consideration of alternatives, according to the GAO, they often do not require a cost-benefit analysis, thereby contributing further to inefficiency.

[117] Project on Government Oversight, "U.S. Nuclear Weapons Complex: How the Country Can Profit and Become More Secure by Getting Rid of Its Surplus Weapons-Grade Uranium," September 14, 2010, http://www.pogo.org/pogo-files/reports/nuclear-security-safety/downblending-heu/nss-nwc-20100914.html#26 (accessed March 1, 2012).

[118] U.S. GAO, *Homeland Defense*, 8.

[119] U.S. GAO, *Homeland Defense*, 10.

## V. ALTERNATIVES TO DBT FOR RISK ASSESSMENT

The DBT has become a standard risk assessment tool for many industries. Critics of the approach fault it for disregarding the strategic nature of terrorists and for being out of touch with the economic reality of defending against an elevated, post-9/11 threat.

### A. Historical Origins

NRC adopted its initial DBT in the 1970s, shortly after the Commission was created in 1974.[120] It developed analogous to a concept in reactor safety called the Design Basis Accident (DBA). The DBA is "[a] postulated accident that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to ensure public health and safety."[121] Early reactor-safety concerns focused on prevention of the "worst-case" scenario, which would definitely cause a loss of primary coolant. This deterministic approach, however, failed to account for event frequencies. It placed too much emphasis on this rare but maximum credible scenario, while neglecting more likely, although less certainly catastrophic, scenarios. Reactor safety eventually evolved to include likelihood assessments via "probabilistic risk assessment" (PRA) methodology. By contrast with the PRA approach to safety, the DBT approach to security, with its emphasis on the maximum posited threat, still retains some of the deterministic roots of the DBA, which some experts criticize.

### B. Critiques of DBT Approach

The DBT approach assumes that terrorists act with some degree of predictability in the method and scope of their behavior.[122] In reality, however, terrorists are intelligent and adaptive and will respond to their knowledge of the defenses that have been implemented. As a result, critics argue, security concepts based on the DBT

[120] Previously, the U.S. Atomic Energy Commission (AEC) oversaw both military and civilian nuclear activities. The 1974 Energy Reorganization Act abolished the AEC, dividing its responsibilities between the NRC, for regulation of civilian nuclear activities, and the Energy Research and Development Agency (ERDA), for nuclear-weapons activities and promotion of civilian nuclear activities. In 1977, ERDA was replaced by creation of the Department of Energy (DOE).

[121] "Design-basis accident," NRC Glossary, accessed March 1, 2012, http://www.nrc.gov/reading-rm/basic-ref/glossary/design-basis-accident.html.

[122] Sergiy Kondratov and Friedrich Steinhausler, "Why There is a Need to Revise the Design Basis Threat Concept," *Int. J. Nuclear Law* 1 (2006), 183.

"incompletely characterize risk, ineffectively identify cost-effective risk management options, and lead to escalating physical protection costs."[123]

The DBT generally does not attempt to account for the strategic nature of terrorists, except as noted above regarding their valuation of various targets. But in practice, boosting defenses against one type of attack might well reduce the likelihood that adversaries would attack in that way, and increase the chance that they would attack in other ways that they perceived to be less well defended. The DBT concept disregards this feedback loop, critics argue, by treating "attack probabilities as exogenous parameters to be specified on the basis of historical data or expert judgment possibly informed by intelligence estimates."[124] As a consequence, the DBT approach may result in an inefficient allocation of resources. An optimal allocation of defensive resources, according to this "operations research" approach, would give the adversary an equal expected outcome from each line of attack.[125]

Critics also argue that, just as with the early version of the DBA for safety, the DBT for security fails to properly account for the likelihood of various scenarios, placing too much emphasis on prevention of the most severe threat, while neglecting more likely but less severe threats, resulting in inefficient allocation of defensive resources.[126]

The DBT concept also is difficult to implement in countries with limited financial resources. The physical protection systems required to fully address a 9/11-level adversary may be prohibitively expensive except in the wealthiest countries. This is one reason that the DOE's Global Threat Reduction Initiative focuses on removing fissile material from most countries that possess it, rather than trying to protect it in place. Insisting on a DBT approach, without adequate funds for the physical protection systems necessary to protect against a maximum credible threat, compels states to artificially reduce the postulated threat below what is actually credible, as even the U.S. NRC does. In the words of Kondratov and Steinhausler, this leads to "the unsatisfactory situation that the threat assessment (provided that such an assessment was indeed carried out) was a compromise between a real threat perception and economic abilities."[127]

---

[123] Edward Blandford, Per Peterson and Robert Powell, "Protecting Critical Nuclear Infrastructure: Strategies for Security," unpublished draft manuscript, CISAC Research Seminar, Stanford University, November 2010, permission obtained to cite.

[124] Blandford, et al., "Protecting Critical Nuclear Infrastructure."

[125] Vicki Bier, "Game-Theoretic and Reliability Methods in Counterterrorism and Security," *Modern Statistical and Mathematical Methods in Reliability* (2005), 33. A simple description, and graphic representation, of this approach is contained in Lawrence M. Wein, "A Threat in Every Port," *New York Times*, op-ed, June 14, 2009, http://www.nytimes.com/2009/06/15/opinion/15wein.html?pagewanted=all.

[126] Blandford, et al., "Protecting Critical Nuclear Infrastructure."

[127]Kondratov and Steinhausler, "Why There is a Need to Revise," 184.

## C. Proposed Alternatives and Complements to DBT

At least three changes to the DBT approach to nuclear security have been proposed: (1) modifying the concept via a tiered threat level; (2) supplementing it with modifications in industry culture and training; or (3) replacing it with a game-theory approach.

***Tiered Threat Levels***

Kondratov and Steinhausler call for making more explicit, and addressing rationally, the reality that many countries cannot afford to provide protection against the maximum credible threat. The best answer, he says, is to establish a three-tiered approach, based on a country's resources: [128]

- DBT level I – require protection against the maximum, credible threat from a non-state adversary, as DOE and DOD reportedly do currently;
- DBT level II – require an intermediate protection level that is the most the country can afford to provide.
- DBT level III – require a minimum level of protection to be determined by an international body.[129]

This tiered approach also calls for integrating government and private-sector resources to ensure that all facilities meet the selected level of security. When the private sector cannot afford to provide protections against the selected threat tier, the government must step in to fill the gap.

***Security Culture***

Complementary to the DBT, there are additional means to reinforce the protection of nuclear assets. These approaches differ from conventional notions of hardening facilities, instead emphasizing the empowering of employees at facilities to actively participate in preventing security breaches. They are thus supplemental to the DBT, enhancing the overall level of protection, and are already actively pursued by the United States and some other countries.

Khripunov endorses the idea of a nuclear security culture, arguing that "effective nuclear security is not just about new equipment, but also the effective operation of a linked set of characteristics of an organisation or institution, including its workforce."[130] Security culture focuses on creating effective administrative procedures and encouraging workers to follow those procedures and proactively report anomalies. The key to a successful nuclear culture is creating a set of attitudes in the workplace that promote the notion that security measures truly matter. A workplace that views threats as credible and serious is more likely to actively work toward protecting its vulnerabilities. A facility's

[128]Kondratov and Steinhausler, "Why There is a Need to Revise," 187.

[129]Kondratov and Steinhausler, "Why There is a Need to Revise," 187-88.

[130]Igor Khripunov, "Nuclear Security Culture: a Generic Model for Universal Application," *Int. J. Nuclear Governance, Economy and Ecology* 1 (2006), 152.

management should spearhead the effort to create vigilance, avoid complacency, and foster collective behavior toward a high standard of security culture.

Sandia National Laboratories is developing a comprehensive international nuclear training curriculum that will assist states in meeting nuclear security objectives. The Sandia program takes a holistic approach to nuclear security, targeting a broad audience for education on both fundamentals of security and specific problems facing practitioners. The scope of these efforts aims to reduce internationally the risk of nuclear theft and sabotage by building "an indigenous cadre of security professionals" around the world.[131]

***Game Theory***

Game theory replaces conventional risk analysis by taking into account the strategic nature of terrorists. In other words, it starts from the assumption that a terrorist will pick a target based on the expected payoff of that attack to the terrorist, relative to other potential targets. One implication, as Powell explains, is that the most likely threat actually depends on the allocation of defense resources, since that spending affects expected payoffs.[132]

Indeed, a terrorist's expected payoff from an attack is actually a function of three factors: the probability that this attack will succeed, the consequences if this attack is successful, and the value of those consequences to the terrorist. Under this approach, the role of intelligence shifts to determining the payoffs to potential adversaries of various attacks, which is no easy task. The first two components of this calculus are more objective – the probability and consequences of a successful attack – although still difficult to estimate. But the third factor is entirely subjective: the value to a particular terrorist of each potential successful attack, relative to other potential successful attacks.

Modeling the interaction between attacker and defender as a game reveals that the optimal allocation for defensive resources is one that minimizes the maximum payoff of an attacker. This idea calls for establishing a "threshold of expected terrorist gain," a baseline measurement of payoff that dictates when resources should be allocated to decrease the vulnerability of a given asset. If a facility lies above the threshold – i.e., the terrorist's expected gain exceeds the baseline – defensive resources should be allocated until the reduced vulnerability causes the payoff level to drop below the threshold. One implication is that high-consequence targets that are sufficiently hardened should not continue to be hardened. That differs from the mainstream assumption that higher consequence targets should always be the priority, and it shifts the focus to lowering the vulnerability of other targets.[133]

---

[131] Dori Ellis, John Matter and Ruth Duggan, "Training Programmes for the Systems Approach to Nuclear Security," *Int. J. Nuclear Knowledge Management* 3 (2008), 8.

[132] Robert Powell, "Defending Against Strategic Terrorists Over the Long Run: A Basic Approach to Resource Allocation," Institute of Governmental Studies, UC Berkeley, September 7, 2006.

[133] Blandford, et al., "Protecting Critical Nuclear Infrastructure."

The game-theory approach has two fundamental theoretical weaknesses. First, it is difficult for the state to estimate the payoffs to terrorists of various attacks, because this depends on three factors that are difficult for the state to measure: the chance that an attack will succeed, the consequences of success, and value of those consequences to various potential adversaries. Second, game theory typically is based on the assumption that terrorists have perfect information about the state's defensive measures and so can adjust their targeting accordingly, which is highly unrealistic. Indeed, states expend considerable resources to ensure that adversaries do not have perfect information. States sometimes exaggerate defensive measures, for deterrent purposes, and at other times underplay their defensive measures to hinder the adversary from developing counter-measures. Given that the perfect-information assumption is so unrealistic, game theory's prescriptions for defense spending are suboptimal, contrary to claims by some proponents. It is possible to relax the assumption in game theory that terrorists have perfect information, but this also significantly reduces its prescriptive precision, ostensibly its main attribute. Considering these theoretical challenges, it is uncertain whether game theory's prescriptions are more or less efficient than those arising from the DBT approach.

In addition to these theoretical concerns, there are practical obstacles to implementing a game-theory approach, stemming from the difficulty of defining the scope of potential targets and adversaries. Even though successful attacks on nuclear assets could have great consequences, game theory says that these dangers must be weighed against the threat to non-nuclear targets that might have greater expected payoffs for terrorists. Doing so would require central coordination of the anti-terrorism budgets of many U.S. government agencies, which is a daunting political and bureaucratic challenge. Similarly, it would be difficult in practice to define rigorously the scope of adversaries. Would certain terrorist organizations be excluded from the realm of possible attackers because their motivations would seem to exclude their targeting nuclear facilities? Drawing such distinctions would be at least as difficult, analytically and politically, as determining the number of attackers to include in the DBT. In practice, government security officials would be reluctant to exclude any real-world adversaries from their posited threat, so that spending on security still would be inefficient by the standards of game-theory advocates themselves.

## VI. ANALYSIS: SHOULD THE DBT VARY?

The above review raises a fundamental question about the U.S. government's current DBT approach to protecting nuclear facilities – namely, should the maximum posited attacking force vary between facilities?

Currently, the posited attack that must be protected against varies between facilities, based on their containing different materials, or having different locations, or being regulated by one or another U.S. government agency. Depending on the underlying assumptions, this could make sense. For example, if the goal is to equalize the expected value of the outcome of an attack on any facility, and the U.S. government has reliable

predictions about the relative consequences of a successful attack, then it makes sense to have greater security at facilities where a successful attack would produce greater consequences. Similarly, if the U.S. government has reliable intelligence about which facilities are more likely to be attacked, then it makes sense to have greater security at those facilities, all else being equal. For private facilities, if government forces provide whatever security the facilities themselves are not required to – in order to defend against a maximum, credible, non-state adversary – then it makes sense for the NRC's DBT to be less robust than those of DOE and DOD.

But these underlying assumptions are unrealistic. First, the ideal goal should be not merely to equalize the expected death and destruction resulting from an attack on any facility, but also to reduce the risk of successful nuclear terrorism as close to zero as possible, in light of available resources. Second, the U.S. government does not have accurate knowledge about the relative consequences of various potential successful attacks. For example, successful theft of a nuclear weapon or fissile material would not necessarily lead to a nuclear detonation, so it is possible that the alternative threat of successful radiological sabotage at a power reactor would have a higher expected consequence, but the opposite is also plausible. Third, intelligence is not reliable about which facilities are likely to be targeted, as demonstrated by a long history of "surprise attack."[134] Fourth, at private facilities, government forces often do not provide the necessary supplementary security, which the facilities themselves are exempted from providing for reasons of cost or law. As a result, in many cases, the combined private and public security at NRC-licensed facilities is inadequate to defend against a maximum, credible, non-state adversary. This leaves private-sector facilities less protected than government facilities that face similar risks of theft of fissile material or radiological sabotage, which makes no sense. Fifth, the fact that certain acts of nuclear terrorism are easier to perpetrate, or are believed to have lesser value for terrorists, does not necessarily mean that the attacking force would be less robust. It is non-conservative and imprudent to reduce security requirements based on the assumption that terrorists would deploy a smaller attacking force than they are capable of doing.

Discarding these unrealistic assumptions leads to the conclusion that, so long as the U.S. government employs a DBT, it should be the same for all U.S. nuclear facilities – whether public or private – that pose catastrophic risks, whether from theft of nuclear weapons or fissile materials, or from radiological sabotage of a nuclear power reactor.[135] (The GAO similarly has criticized the variation of the DBT between public and private facilities, in a 2007 letter to Congress, recommending that "DOE and NRC should develop a common DBT for DOE sites and NRC licensees that store and process

---

[134] Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford University Press, 1962). Richard K. Betts, *Surprise Attack Lessons for Defense Planning* (Brookings Institution Press, 1982). Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (Columbia University Press, 2007).

[135] The far smaller potential consequences of radiological sabotage at a research reactor do justify a less robust DBT for this particular vulnerability.

Category I special nuclear material."[136]) If the U.S. government adopted such a common DBT, the NRC could still accommodate the legal and financial limits on private security measures by subdividing the DBT into a smaller threat, which licensees would be required to defend against, and a larger threat that government forces would be required to defend against. This would have the virtue of eliminating two widespread, but erroneous and dangerous, assumptions about the NRC's current approach: that its existing DBT already represents the maximum, credible, threat from non-state adversaries; or that the government already provides supplementary security at NRC-licensed facilities to protect against this level of threat.

## VII. CONCLUSIONS AND RECOMMENDATIONS

Each proposed alternative to the DBT has merit, but also shortcomings that its advocates tend to ignore or downplay.

Game Theory undoubtedly would enable more efficient allocation of security resources if its assumptions held true in practice, but they do not. The state cannot estimate accurately the expected payoffs to terrorists of various attacks. Terrorists lack perfect information about the state's defensive measures. Even if they should, states are unlikely to centrally coordinate all of their security spending, and state officials are unlikely to abandon protections against a known adversary based merely on intelligence estimates that the adversary will not attack a certain facility even though it could. In light of the fact that game theory is based on so many unrealistic assumptions about the attributes and actions of its two "players" – terrorists and states – its resulting recommendations for allocating security resources will not necessarily be more efficient than those arising from the DBT. Better insight on this question could be gained by employing more realistic assumptions in game-theory models, at the expense of complicating the calculations.

Tiered security has the attraction of being a structured, rather than ad hoc, response to the reality that some facilities or states lack the resources to defend against a maximum, credible threat from non-state adversaries. But since nuclear terrorism at any facility could have global consequences, it is not clear why the international community should be willing to accept lower security levels for some states or facilities. Moreover, an explicitly tiered system could effectively advertise to potential adversaries which facilities in the world are most vulnerable to attack, which would be counter-productive.

Creating or enhancing a "nuclear security culture" would be beneficial. But even advocates of this "paradigm shift" acknowledge that it could only be a supplement to, not a replacement for, allocating resources for physical security.

The DBT approach is also criticized on many grounds: the difficulty of specifying the attributes of a maximum, credible adversary; prescriptive implementation that wastes resources by over-protecting some facilities that are less likely to be attacked; ignoring

[136] GAO, "Nuclear Security," correspondence to The Honorable Christopher Shays, GAO-07-1197R, September 11, 2007.

the reality that terrorists will respond strategically to defenses that they know about; and requiring a level of security that is unaffordable and therefore not implemented in many cases. Each of these criticisms has some merit. But it is not obvious, based on current information, that the DBT approach is less efficient than the alternatives.

So long as the U.S. government relies on the DBT, this approach should be made more rational. Most importantly, the DBT should be the same for all U.S. nuclear facilities – whether public or private – that pose catastrophic risks, whether from theft of nuclear weapons or fissile materials, or from radiological sabotage of a nuclear power reactor. The NRC could still accommodate the legal and financial limits on private security measures by subdividing the DBT into a smaller threat, which its licensees would be required to defend against, and a larger threat that government forces would be required to defend against. However, it is essential to ensure that the combination of private and government security be sufficient to defend against the maximum credible threat from a non-state adversary, which unfortunately does not appear to be the case currently at many NRC-licensed facilities.