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

By Alan J. Kuperman and Lara Kirkham[1]
Nuclear Proliferation Prevention Project (www.NPPP.org)
LBJ School of Public Affairs, University of Texas at Austin

Prepared for INMM 54th Annual Meeting, Palm Desert, CA, 17 July 2013

ABSTRACT

This paper 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.

INTRODUCTION

This paper 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.

The paper focuses principally on the threat assessment tools used by the NRC because more information is publically available about its methods. But we believe the analysis could help the DOD and DOE evaluate their own approaches 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 the current resources of potential adversaries. The paper starts with a critique of the DBT's theoretical underpinnings. It then explores proposed alternatives to the DBT approach, analyzing their theoretical and practical shortcomings as well. The paper closes with recommendations for revising the DBT and the U.S. government's approach to nuclear security.

We find 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 paper'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 paper argues that the U.S. government lacks reliable information that could 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 paper 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 among facilities that contain identical or functionally equivalent nuclear assets. The paper 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.

PREVIOUS CRITIQUES OF DBT'S POSITED ATTACK

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.[2] Since 2001, the U.S. nuclear industry has spent over $2 billion on security enhancements to their physical protection systems.[3] 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."[4] 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 revisions adopted in the wake of the terror attacks of 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 number of adversaries was kept relatively low because intelligence agencies assumed that they could detect conspiracies of more than a few members.[5] 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 only was increased to "less than double the old figure and a fraction of the size of the 9/11 group" of 19 hijackers.[6] Another source specifies it as "five or six well-armed terrorists, possibly working in conjunction with an insider or two."[7] This number reflects the NRC's assumption that only one terrorist cell would attack a plant.[8] 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.[9] Critics say this does not adequately represent the present threat, which should take into account the size of the entire 9/11 attack force, at least positing an attack from a "squad size" of adversaries (12-14 personnel).[10]

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.[11] 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.[12] (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 by regulation are not required to defend against the DBT.)[13] Thus, according to critics, the U.S. government both underestimates the insider threat and then fails to assure protection against even that underestimated threat. However, 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."[14] 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 fissile 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.[15]

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.[16] For example, according to the Project on Government Oversight (POGO), DOE timelines 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.[17] 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.[18]

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. These were originally on a list of weapons that intelligence staff proposed to require nuclear facilities to protect against.[19] But when the NRC finalized this revised DBT, it eliminated these two weapons, reflecting industry input.[20] POGO argues that this decision was based on pressure from the nuclear industry to keep down costs.[21] 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 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."[22] 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 attacks.[23] 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 after the industry complained.

Airborne & seaborne attacks

Existing US nuclear power plants were designed to withstand extreme environmental events such as hurricanes and earthquakes, but not deliberate attacks using fuel-laden airliners.[24] 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." According to the NRC, "the active protection against airborne threats is addressed by other federal organizations, including the military."[25]

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."[26] The doctrine further states that private nuclear facilities are not responsible for "defending against attacks that typically could only be carried out by foreign military organizations,"[27] which are the responsibility of the federal government. The industry thus relies on elements of the government, such as the FAA and North American Aerospace Defense Command, to detect, deter, and defend against airplane attacks.[28] The NRC argues that these agencies offer sufficient protection, obviating any need for plant operators to take additional protective measures.[29] 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."[30]

In another inconsistency, the NRC has required that all <u>future</u> power reactors be designed to mitigate attacks by commercial aircraft, but has not required <u>existing</u> reactors to make retrofits to address that threat.[31] 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 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."[32]

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.[33] The NRC counters that the Argonne study is old and flawed, and that new studies conducted with better computer models show the plants are safe.[34] However, 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. Instead, existing power plants are required only 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.[35] 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."[36] The NRC reportedly does not require a no-fly zone around nuclear plants, except during times of elevated threats, because it would impose costs on the aviation industry.[37] 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.[38]

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 – to cool 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, the Department of Defense responded to its DBT by requiring the placement of floating barriers around anchored ships and nuclear submarines, says UCS.[39] 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. Remarkably, 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.[40] According to statute, however, the NRC is not supposed to consider economic costs in ensuring the adequate protection of public health and safety.[41]

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.[42] 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.[43] Although this is unarguably true for the "potential" consequences, it is not necessarily true for the "expected" consequences, as elucidated below.

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."[44]

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."[45] 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.[46] 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 to further inefficiency.

ALTERNATIVES TO DBT FOR RISK ASSESSMENT

The DBT has become a standard risk assessment tool for many industries. But 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.

Historical Origins

NRC adopted its initial DBT in the 1970s, shortly after the Commission was created in 1974.[47] The DBT 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."[48] 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 the methodology of "probabilistic risk assessment" (PRA). 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.

Critiques of DBT Approach

The DBT approach assumes that terrorists act with some degree of predictability in the method and scope of their behavior.[49] 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 "incompletely characterize risk, ineffectively identify cost-effective risk management options, and lead to escalating physical protection costs."[50]

The DBT generally does not attempt to account for the strategic nature of terrorists, except 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 perceive 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."[51] 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.[52]

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.[53]

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 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."[54]

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 addressing, explicitly and rationally, the reality that many countries cannot afford to provide protection against the maximum credible threat. The best answer, they say, is to establish a three-tiered approach, based on a country's resources:[55]

- DBT level I – would require protection against the maximum, credible threat from a non-state adversary, as DOE and DOD reportedly do currently;
- DBT level II – would require an intermediate protection level that is the most the country can afford to provide.
- DBT level III – would require a minimum level of protection to be determined by an international body.[56]

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 would 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. Supplemental to the DBT, these steps can enhance 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."[57] 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 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 the 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.[58]

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.[59]

Indeed, a terrorist's expected payoff from an attack is actually a function of three factors: the probability that the specific attack will succeed, the consequences if that 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, but this is no easy task. The first two components of the calculus are more objective – the probability and consequences of a successful attack – although these too are 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 of 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 already fairly well protected should not be further hardened. That differs from the mainstream assumption that higher consequence targets should always be the priority, and it instead shifts the focus to lowering the vulnerability of other targets.[60]

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 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, which ostensibly is 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 would remain inefficient, according to the standards of game-theory advocates themselves.

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 does vary 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 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 (although 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."[61] Fourth, at private facilities, government forces often do not provide the necessary supplemental security that

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.[62] 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 Category I special nuclear material."[63]

CONCLUSIONS AND RECOMMENDATIONS

Each proposed alternative to the DBT has merit, but also has 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. First, the state cannot estimate accurately the expected payoffs to terrorists of various attacks. Second, terrorists lack perfect information about the state's defensive measures. Third, 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, which admittedly would complicate 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; rigid implementation that wastes resources by over-protecting some facilities that are less likely to be attacked; ignoring 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. 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; and that the government already provides supplementary security at NRC-licensed facilities to protect against this level of threat. Going forward, the combination of private and government security should be made 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.

NOTES

[1] This paper is based on a report prepared for the Office of the Secretary of Defense, which provided financial support for the research. The full report is available at www.NPPP.org. For helpful comments on an earlier draft, the authors thank Matthew Bunn of Harvard University and Alex Athey of the University of Texas at Austin.

[2] 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).

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

[4] 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.

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

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

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

[8] 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.

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

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

[16] 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).

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

[18] 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.

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

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

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

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

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

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

[25] 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.

[26] 10 C.F.R. § 50.13.

[27] 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.

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

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

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

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

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

[33] "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.

[34] 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).

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

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

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

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

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

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

[41] 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).

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

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

[44] 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).

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

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

[47] 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).

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

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

[50] 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.

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

[52] 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.

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

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

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

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

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

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

[59] 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.

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

[61] 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).

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

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