ABSTRACT
More than ten years after the 11 September attacks in the United States, the terrorist threat continues to evolve. Strategies for protecting nuclear facilities and nuclear materials from sabotage and theft must be flexible enough to rapidly accommodate changes in the threat environment, yet also must be sufficiently detailed to provide assurance that they will be effective against a range of specific scenarios. Also, after the Fukushima accident, concerns have grown about the potential for “cliff-edge” effects, in which challenges such as flooding at a nuclear plant can lead to catastrophic consequences if the plant’s design basis is exceeded by only a small margin. Protective strategies for nuclear plants against terrorism should also be resistant to “cliff-edge” effects, yet there is insufficient attention to this issue in the security realm. Lessons can be drawn from the so-called “B.5.b” measures required by the U.S. Nuclear Regulatory Commission (NRC) after 11 September to provide backup means to prevent or mitigate core damage at nuclear plants in the event of an aircraft attack that disables ordinary mechanisms for core cooling. The B.5.b measures were specifically intended to cope with the aftermath of an aircraft attack, but might not have been usable following a different or more severe mode of attack. In addition, the B.5.b measures may not have been effective even for their intended purpose because the NRC did not require detailed procedures to govern how they would be implemented after an attack, or detailed inspections to ensure that B.5.b equipment would be operable. An approach that is both broader and deeper is required to provide an adequate level of security.

INTRODUCTION
One of the major goals of the Obama administration going into the 2010 Nuclear Security Summit was to “lock down” all vulnerable nuclear weapon-usable materials by the end of 2013. But what does this mean in operational terms? The gold standard for “locking down” nuclear facilities against terrorist attacks should be defined by a multi-step approach.

First, credible design basis threats (DBTs) must be formulated, with adequate conservatism to allow for uncertainties in the threat environment.

Second, facility operators should develop rigorous physical protection plans with the objective of providing high assurance of protection against the appropriate DBT for each class of facility. (The grading of security requirements for different threats should be applied, provided that there is rigorous technical assessment to support
the relevant threat levels.) An essential part of any security plan is a contingency response plan to document the strategy to protect against attacks of adversaries with characteristics defined by the DBT. The baseline strategy in today’s threat environment should include preparation to defend against well-trained, paramilitary armed attackers; an appropriate defensive strategy against such attacks would by necessity require the presence of on-site, tactically trained armed response forces on 24-hour alert.

The third component of the program is the development of a robust force-on-force exercise regimen with stringent government oversight, including enforcement mechanisms. Experience in the United States with physical protection implementation at civil nuclear facilities regulated by the Nuclear Regulatory Commission (NRC) has shown that significant security vulnerabilities can be present at a facility even if the security plan meets all regulatory requirements. These vulnerabilities are most easily revealed through the administration of performance tests. In order for performance tests to be useful, regulators must design them to measure as accurately as possible the actual day-to-day security posture of a facility, and regulators must have enforcement tools to ensure that operators address vulnerabilities revealed through such tests or risk revocation of their licenses.

Finally, security strategies must have well-defined contingency plans for coping with “beyond-design basis threat” attacks. The DBT is an artificial construct designed to define the legal responsibilities of facility operators for protecting their facilities against attack. However, the DBT approach as currently developed for use by the NRC, and as recommended in IAEA guidance, does not represent the largest credible threat against a nuclear facility as developed through intelligence information and other analysis. The DBT is a subset of adversary characteristics obtained by filtering the largest credible threat through a sieve of policy considerations, including (in the case of the U.S.) a subjective judgment as to the magnitude of the threat against which private industry should be responsible for providing protection. Consequently, the responsibility for protecting nuclear facilities against credible threats that exceed the DBT must be assigned to other entities. And such plans should be validated through performance testing to the extent feasible, for the same reasons that operator security plans need to be validated.

However, the question of how to respond to attacks exceeding the DBT remains a gray area. In the U.S., although it is assumed that government resources, such as local law enforcement and the National Guard, would be responsible for protecting nuclear facilities against such attacks, there is no well-defined plan for how that would actually take place in practice. IAEA guidance assumes that this security gap will be addressed by States. But an assault is capable of being successfully completed within a manner of minutes, so response times must be extremely short. Without the development of detailed contingency plans that can be verified, one cannot have a high degree of confidence that the “cavalry” will arrive in time to save the day.

These are essential components of a comprehensive security strategy for protecting nuclear facilities and materials. However, even the United States, which has incorporated many features of such a strategy into its regulations, falls short in some respects. U.S. experience in trying to impose stringent security requirements on an
industry that makes minimization of operating costs a priority demonstrates the practical difficulties of ensuring adequate security at commercial nuclear facilities. Even at Energy Department-owned facilities, the budget constraints under which the U.S. government is now operating have led to efforts to reduce the costs of security requirements that were upgraded after the 11 September attacks.

In any event, adherence to a comprehensive strategy like the one outlined above is not being used as a standard to assess whether any country has demonstrated its ability to “lock down” nuclear material. The physical protection standards available to the international community include INFCIRC/225/Rev. 5 and the guidance contained in the IAEA Security Series documents. In the multinational context, INFCIRC/225 serves only as a non-binding set of recommendations, although it is a legally binding instrument within some bilateral nuclear cooperation agreements. INFCIRC/225/Rev. 4 dated from 1998, and remained in effect for about a decade after the 11 September attacks even though those attacks effectively rendered obsolete any guidance based on previous perceptions of the magnitude of the terrorist threat. Rev. 5 is an improvement over Rev. 4 in some respects, but still has too many loopholes to allow it to serve as a comprehensive and effective standard.

For instance, Rev. 5 recognizes for the first time the importance of performance testing, but does not stipulate the mandatory use of force-on-force exercises, which represent the most rigorous and effective means of such testing. Moreover, although Rev. 4 was the first revision of INFCIRC/225 to describe the use of the DBT in developing security plans, Rev. 5 actually allows use of a “threat assessment” instead of a DBT approach for lower risk materials and facilities. And as in all previous versions of INFCIRC/225, Rev. 5 does not require on-site armed response forces, even for protection of Category I materials. It continues to sanction the intolerable situation in which bomb quantities of weapon-usable materials could be protected only by unarmed guards, provided that they have an agreement with off-site armed responders, but without requiring any mechanism for validating whether the off-site forces would be capable of responding to attacks in a timely and effective manner.

DEFENSE-IN-DEPTH

Another element of a robust security program for nuclear facilities is defense-in-depth. In nuclear power safety parlance, defense-in-depth refers to the provision of separate safety features for preventing accidents, for mitigating their consequences should they occur, and for protecting the public and the environment from any radiological releases should they occur. Within each of those categories, defense-in-depth would generally require that multiple diverse and redundant means exist for achieving each objective.

With regard to security at nuclear power plants, defense-in-depth principles have not traditionally been as well established. Protection against radiological sabotage generally relies on preventing core damage by ensuring that an adversary team is unable to successfully damage enough critical safety equipment to cause an uncontrolled loss of heat removal. This focus is to a large extent appropriate, because the success path to halting a large radiological release becomes much more uncertain once core damage has begun. This is clear from the experience of the Fukushima Daiichi accident. In the event of a terrorist attack, the situation could
be even more dire, in that operators would not only need to be protected from high radiation levels and other potential obstacles to carrying out emergency actions, but would also need to be protected from adversaries who would seek to stop them. In the U.S., the NRC requires that operators possess a capability to mitigate sabotage attacks only in the event of aircraft attack, which is an event that the NRC does not include in the DBT and thus does not require operators to address in their security plans by providing means for prevention. (Prevention would entail active defensive means like anti-aircraft weapons or passive means like artificial fog or additional structural barriers.)

Finally, emergency preparedness (EP) plans designed to protect the public from accidents may not be sufficient to cope with certain unique aspects of hostile-action events. These differences need to be thoroughly evaluated and EP plans modified accordingly.

**PREVENTION**

In the U.S., the NRC requires that certain types of commercial nuclear facilities develop a security program that protects against the DBT. To protect against the DBT of radiological sabotage at power reactors, the requirement is to “prevent significant core damage and spent fuel sabotage.”

The process by which this requirement is implemented is through the identification and protection of “target sets.” A “target set” consists of critical equipment needed to provide cooling to reactor cores or spent fuel pools, or protection of spent fuel in dry cask storage. Destruction of a complete target set would lead to (significant) core or spent fuel damage without operator intervention. Therefore, strategies for defending against radiological sabotage are based on preventing destruction of an entire target set.

Although there are similarities between prevention of sabotage and accident prevention, they are conceptually quite different. While a nuclear plant probabilistic risk assessment can be used to identify the groups of equipment that comprise various target sets, one cannot use a probabilistic risk assessment to calculate the risk of sabotage. This is because the events that occur during an accident sequence are primarily random events, whereas the events that occur during a sabotage attack can be deliberately caused, and can be modified by human actions depending on the situation. This introduces elements into the analysis that cannot be modeled. (This is also unlike the situation with operator actions that are sometimes modeled in a PRA. In that case, whether an operator succeeds or fails is derived from performance data – data that is not available for terrorist attack scenarios.)

As stated earlier, a physical protection plan that looks good on paper may not be effective in practice. This was a clear lesson from the NRC’s Operational Safeguards Response Evaluation (OSRE), a program in the late 1990s that utilized force-on-force performance tests to assess the readiness of nuclear plants to protect against the DBT. Approximately 50 percent of the nuclear plants tested failed to protect an entire target set in at least one exercise scenario, even though all plants had NRC-approved security plans.
As recognition of the importance of performance testing, force-on-force exercises were formally incorporated into NRC regulations as part of the reforms that took place after the 11 September attacks and are part of the NRC inspection program. Every plant must undergo an NRC-run force-on-force inspection every three years. Although NRC does not release the individual results of these tests for security reasons, it does provide the results in aggregate form every year to Congress. The results from report to Congress for 2010 are presented in Table 1.

<table>
<thead>
<tr>
<th>24</th>
<th>Total Number of Inspections Conducted</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Total Number of Times a Complete Target Set Damaged or Destroyed</td>
</tr>
<tr>
<td>23</td>
<td>Total Number of Inspection Findings</td>
</tr>
<tr>
<td>12</td>
<td>Total Number of Inspections with No Finding</td>
</tr>
<tr>
<td>18</td>
<td>Total Number of Green Findings</td>
</tr>
<tr>
<td>5</td>
<td>Total Number of Greater-than-Green Findings</td>
</tr>
</tbody>
</table>

The NRC also conducts force-on-force inspections for Category I fuel cycle facilities with respect to the DBT for theft and diversion of Category I quantities of special nuclear material, and also the DBT of radiological sabotage if appropriate. However, it does not report the findings publicly. At present there are only two commercial Category I facilities licensed to operate by the NRC.

It can be seen from Table 1 that the force-on-force inspections have an approximately 10 percent failure rate, in that a complete target set was damaged or destroyed in 2 out of 24 inspections conducted. Figure 1 shows that this failure rate has been fairly constant since the post-11 September program was introduced (the 2006 data point is probably an artifact of issues associated with startup of the program). This appears to be a significant improvement in comparison to the 50 percent failure rate observed during the OSRE program. However, one cannot make a direct comparison because there is little public information about how the guidelines for the current force-on-force inspection regime compare to those for the OSRE program.
The effectiveness of force-on-force exercises depends critically on how they are conducted. For confidence that the results of force-on-force testing are meaningful, assurances are needed that the tests are challenging (and that the maximum DBT capabilities are utilized in at least some of the tests). Safeguards need to be in place to ensure that there is no cheating. In particular, the mock adversary force should be fully independent of plant management and ideally should be under the control of the regulator. And the tests should also strive to ensure that they measure accurate representations of the everyday security posture at a facility. This is difficult to achieve because the tests cannot fully simulate the one advantage that an attacking force must be assumed to have: the element of surprise. One cannot assume that intelligence agencies will be able to provide timely advance warning of an attack. However, there must necessarily be significant advance warning of a force-on-force test in order to ensure that the site makes the necessary preparations. The length of advance notice that U.S. plants are provided has decreased significantly since the days of OSRE but it is still significant. This contributes to the concern that the response force may undergo an unusual level of training to be ready for the test.

Issues of concern that have arisen in the context of force-on-force tests include the adequacy of the exercise “controllers” that act as referees during the test, the assumptions regarding insider assistance and the amount of facility information that the adversary team is assumed to possess, and the extent to which armed security officers with contingency response duties are assigned other duties.

Another concern is that pass-fail testing measured against the DBT does not provide important information about the “security margin” built into the protective strategy and the ability of a security force to protect against beyond-DBT attacks. For plants that have successfully protected at least one target in a target set, it is important to know how close they actually came to losing the last target. For example, if they passed the test by a hair’s breadth due to sheer luck, their performance should not be assessed as fully successful. Thus the evaluations should also test for the presence of “cliff-edge” effects: that is, they should assess how robust the protective
strategy is with respect to a slight increase in adversary capabilities, such as use of a new weapon or new tactic. Perhaps the ultimate cliff-edge effect would be the conversion of a passive insider to an active, violent insider.

The amount of margin available in a plant’s security posture can be tested in two ways. First, force-on-force tests could be conducted using beyond-DBT adversary characteristics. Second, successful DBT force-on-force tests could be evaluated using “margin assessment” – that is, how close did the DBT adversary come to destroying a target set? In the U.S., there have only been minimal steps in this direction. NRC has reportedly conducted some beyond-DBT force-on-force exercises, but only on a voluntary basis, and it is not clear how the results of those exercises were utilized. Also, the NRC staff proposed a margin assessment method in 2010, which would have replaced the pass-fail evaluation currently used in security inspections with a numerical score that would take into account (Figure 2). However, it is not publicly known whether this new procedure was ever implemented.

![Diagram: Force on Force Margin Assessment](image)

**Figure 2.** NRC staff’s proposed “margin assessment” procedure.
MITIGATION
If radiological sabotage is not prevented and a complete target set is destroyed, then one should consider if the consequences of such an event could be mitigated. For example, in the U.S., it is assumed that aircraft attacks cannot be prevented by reactor operators, but the consequences of the ensuing explosions and fires could be mitigated. This led to the introduction of the so-called “B.5.b” strategies: emergency equipment and operator actions designed to restore core and spent fuel pool cooling.

B.5.b strategies were designed only for an aircraft attack scenario, and they therefore assume that equipment will be available and can be used provided it survives the aircraft attack. B.5.b strategies were not intended for use in any other attack scenario, such as a ground assault. In such scenarios, operators and equipment would have to be protected from any remaining adversaries by security forces, and therefore security plans would have to address such requirements. However, B.5.b. strategies were not incorporated into site security or contingency plans.

If the potential need for mitigation of successful attacks were considered an important part of a defense-in-depth strategy, this would result in the need for significant additional security resources to ensure protection of the necessary equipment and operator actions. This would raise questions about whether this equipment --- and in fact even the operators themselves --- would have to be become parts of target sets. If that were to happen, plant security plans would need to be modified, and plant security margins would be increased, but so would security costs. Such cost increases may well be justified by the increased benefit.

EMERGENCY PREPAREDNESS
The NRC has recognized that emergency preparedness measures designed to protect the public need to be modified to deal with hostile action-based events, and has made some changes to its EP requirements. In particular, it now requires that periodic emergency planning exercises must now include hostile-action based scenarios. However, it is not clear if these scenarios will address all the issues that may pose challenges to EP implementation during a terrorist attack. First of all, a terrorist attack has the potential to cause large releases before evacuation can be carried out. Moreover, the potential for deliberate interference with emergency response and evacuation by adversaries could require expanded responsibilities for site security forces and local law enforcement.

A DECREASE IN THE SECURITY MARGIN FOR WEAPON-USABLE MATERIALS
For the past several years, the U.S. has led the charge internationally for increasing the security of weapon-usable materials. However, over the same period, the U.S. has taken measures that have weakened, rather than strengthened, domestic protection of such materials.

First of all, the NRC has downgraded the security requirements for MOX fuel, a mixture of plutonium and uranium. The Category I requirements for storage of MOX fuel at reactor sites have been weakened. And an NRC proposal currently under consideration to “risk inform” the security requirements of plutonium and other actinides based on material form could lead to further security reductions, including
the transport of MOX fuel in ordinary trucks instead of specially secured transport vehicles.

The NRC has also granted permission for the use of “alternate” security methods at the MOX fuel fabrication plant under construction at the Savannah River Site in South Carolina. Although the NRC staff judged these alternate methods to be equivalent to or even superior to the existing regulations, the public is unable to analyze the NRC’s reasoning because the relevant details are classified. In addition, the NRC has approved the MOX plant’s proposed approach for complying with material control and accounting requirements that are complementary to physical protection (alarm resolution, assessment of validity of alleged thefts). However, the adequacy of these proposals is currently being challenged by intervenors.

In addition to plutonium, some isotopes of other actinides, such as neptunium, americium and curium, are weapon-usable and should be protected accordingly. However, the NRC has voted repeatedly not to require such protection for neptunium, americium and curium. This inaction on the NRC’s part continues to give support to those who argue that fuel cycles which separate plutonium in a mixture with these other actinides pose reduced security threats compared to those that produce separated plutonium. But this has been decisively refuted by a multi-year study conducted by the U.S. nuclear weapons laboratories. According to this study,

“The primary conclusion … is that all fissile material must be rigorously safeguarded to detect diversion by a state and provided the highest levels of physical protection to prevent theft by subnational groups; no “silver bullet” fuel cycle has been found that will permit the relaxation of current international safeguards or national physical security protection levels.”[1]

There is no justification for the U.S. to reduce the security requirements for weapon-usable materials at home when it is urging other countries to strengthen them.

CONCLUSION

Terrorist attacks have the potential to challenge all the barriers to radiological exposure of the public that constitute a defense-in-depth approach to safety at nuclear facilities: accident prevention, consequence mitigation, and emergency preparedness. Consequently, a comprehensive approach to protecting the public from radiological sabotage must address all of these barriers as well. Moreover, defense-in-depth also requires the provision of robust security margins within each of these areas.

The standard of merit for assessing the adequacy of security at nuclear facilities is rooted in force-on-force performance testing. In an ideal world, an international body should have the authority to be able to utilize a mock adversary force to assess, at short notice, the security posture of any facility in the world that poses a major radiological hazard or is a tempting target for terrorists seeking nuclear weapon-usable materials. National sovereignty concerns pale in comparison to the global safety and security implications of poorly secured nuclear facilities.