5. Threat Definition

Abstract. In 2001, the International Atomic Energy Agency (IAEA) Board of Governors and General Conference endorsed ‘physical protection objectives and Fundamental Principles’ as a step to strengthen the international physical protection framework. Fundamental Principle G, contained in INFCIRC/225/Rev.5, states “the State’s physical protection system should be based on the State’s assessment of the threat.” Physical Protection System (PPS) stakeholders use a threat assessment process to evaluate the intentions and capabilities of perceived adversaries to a nuclear facility. The result is the Design Basis Threat (DBT), or threat definition. The international standard for the development of a DBT is discussed in this section. This approach consolidates the threats evaluated in a threat assessment, and modifies this consolidated threat based on policy decisions. The DBT must be considered when determining the objectives of or evaluating the effectiveness of an existing PPS.

5.1 Introduction

Threat Assessment
The possibility that terrorists, criminals, or protestors might attempt to seize or sabotage a nuclear facility, steal nuclear material, or perform other unauthorized activities within the nuclear industry must be considered in the protection of nuclear facilities. Physical Protection Systems (PPS) are developed to counter the defined threat to ensure adequate physical protection of nuclear facilities. PPS development involves balancing security needs with available resources. The threat influences both of these aspects. In most cases, the threat must be postulated, since it has not been demonstrated in frequent attacks on nuclear facilities. Where threat data are not available, assumptions must be made concerning the threat in order to develop a complete set of PPS requirements and prioritize budgetary and other resources. A structured analysis of the capabilities and intentions of potential threat capabilities and intentions provides a sound basis for making such assumptions.

The Threat Assessment is an independent effort that is not constrained by considerations of budget or policy. The threat assessment bounds the threat problem to support the subsequent DBT development effort.

IAEA International Standard for DBT Development
This section describes the international standard for the development of a State Design Basis Threat (DBT). An international team of experts in the development and use of a DBT developed this methodology over the past several years at the request of the International Atomic Energy Agency (IAEA). The team included representatives from the United Kingdom, France, Germany, the Russian Federation, Spain, and the United States. The team has presented several workshops on the development of a DBT to IAEA Member States and they have been working together to ensure this methodology represents best practices from each of the represented States.
This methodology supports the development of a State DBT to be used in design and evaluation of PPS for nuclear facilities.

The IAEA publishes Information Circular (INFCIRC)/225/Rev.5 to provide guidance for Member States. Fundamental Principle G states that PPS for all nuclear facilities and shipments should be based on the State's assessment of the threat. This recommendation was extracted into a paper: *The Physical Protection Objectives and Fundamental Principles*, which was approved by the IAEA Board of Governors in 2001, and was included in the *Amendment to the Convention on Physical Protection of Nuclear Materials* in 2005. The process for threat assessment and DBT development have been promulgated in the recent IAEA Nuclear Security Series publication number 14, Development, Use, and Maintenance of the Design Basis Threat (1999). The threat assessment defines the attributes and characteristics of all adversaries who might attempt to unlawfully remove material or sabotage the facility. From this threat assessment, the State’s Competent Authority then derives a DBT to be used in the design and evaluation of a PPS at a facility level.

**Definition of a DBT**

The IAEA defines a DBT as:

*The attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated.*

**What is a DBT**

A DBT is a document that outlines postulated adversary capabilities in terms useful for development of system requirements for a PPS. A DBT is used rather than a threat assessment for these reasons:

- A frequently changing threat assessment does not provide a sufficiently stable basis for PPS development programs which can span several years.

- A threat assessment is not constrained by resources or policy. It might not be feasible or desirable for the state to meet all possible threats. The DBT represents the State’s agreement as to what set of the threats are to be mitigated by the PPS. The DBT process incorporates additional considerations of policy, national priorities, risk tolerance, and available resources.

To effectively guide PPS development, the DBT addresses four themes:

- Who an adversary can be – an external adversary (outsider) and/or
5. Threat Definition

<table>
<thead>
<tr>
<th>Value of the DBT</th>
</tr>
</thead>
<tbody>
<tr>
<td>The DBT is an essential part of the State’s system of physical protection. INFCIRC/225/Rev.5 states that the DBT aids the licensing process by:</td>
</tr>
<tr>
<td>• Providing a common basis for all facilities in one country,</td>
</tr>
<tr>
<td>• Providing a standard against which to design and evaluate a PPS, and</td>
</tr>
<tr>
<td>• Setting a baseline against which to evaluate future changes in the threat.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application of a DBT</th>
</tr>
</thead>
<tbody>
<tr>
<td>A DBT establishes boundaries for the development of adversary scenarios, and permits definition of the most severe (successful) credible adversary scenario. A DBT can assess the effectiveness of a facility or transport protection system against theft and sabotage.</td>
</tr>
</tbody>
</table>

adversaries within certain internal organizations or facilities (insider

- What the adversary can do – this DBT content connects adversary capabilities with potential consequence to the facility and its protected assets.

- What the adversary is like – adversary general attributes and characteristics, such as motivation, intent, level of expertise, are important to assist PPS designers in making certain detailed inferences to support PPS design.

- How PPS performance can be measured – The DBT should contain information in sufficient detail to support evaluation of the PPS to ensure it meets requirements.
5.2 Regulatory Basis for DBT in the US

U.S. DOE and NRC Use a DBT

Two agencies in the US regulate the use, storage, and processing of nuclear material:

- Department of Energy (DOE)
- Nuclear Regulatory Commission (NRC)

Both of these agencies use a DBT in their regulatory process; however, the process is slightly different in each case.

5.2.1 Department of Energy

DOE Orders Instruct Facilities

The DOE issues instructions to facilities through written “orders” that originate from headquarters in Washington, D.C. The primary order is DOE Order 470.1, entitled “Safeguards\(^1\) and Security Program.” The order defines how to establish a PPS and how to use a DBT in the analysis of a PPS. The DOE order requires each facility to analyze the threat in its local area and compare it to the national threat. If the local threat is greater (such as a local military militia movement or active environmentalists), the local facility must provide additional physical protection. The local facility can never define a lower standard than the national DBT.

Evaluating Safeguards and Security Programs

DOE Order 470.2 is the "Safeguards and Security Independent Oversight Program." This order controls how the security programs are evaluated. The DOE licenses the weapons programs facilities and most government-owned nuclear material. The DOE issues orders and directives on how a facility should implement a PPS and each facility is required to comply with those directives because the DOE owns the material.

Site Safeguards and Security Plan (SSSP)

Every year, each facility must submit a Site Safeguards and Security Plan (SSSP) to the DOE. This plan contains:

- Details of how the facility meets the requirements in the directives and orders
- The facility’s assessment of the effectiveness of its physical protection and MC&A systems.

The DOE specifies the level of system effectiveness required by the facility. The Plan defines how the PPS achieves the required level of system

---

\(^1\) Safeguards in DOE terminology refers to domestic material control and accounting.
5. Threat Definition

The Twenty-Sixth International Training Course

5.2.2 Nuclear Regulatory Commission

**Enabling Legislation**

The Atomic Energy Act of 1954 and the Energy Reorganization Act of 1974 are the major legislation that defines regulation of civilian nuclear facilities. The 1974 act established standards and regulations and allowed for issuing licenses and inspecting facilities and transporters. The legislation also established the Office of Threat Assessment within the NRC.

**NRC Issues and Enforces Regulations**

The NRC issues regulations that control licensing, inspections, and the ability to levy fines. Since these directives are federal law, each facility must ensure that they comply with them or face monetary fines or criminal sanctions. The NRC has the legal authority to issue fines and approve, deny, or revoke licenses based on the facility evaluation against the DBT.

**Each Facility Submits a Security Plan**

Each nuclear facility regulated by the NRC must also submit a security plan to the NRC for review and approval to ensure all federal laws are being met. The NRC also conducts site inspections to ensure that all federal laws are being followed and that the facility demonstrates an effective PPS. In the event a facility can demonstrate that non-compliance with a specific requirement will not adversely affect the effectiveness of the PPS, they may receive a waiver that allows them to not comply with that specific requirement.

5.2.3 Design Basis Threat

**Office of Threat Assessment**

Both the NRC and DOE maintain an Office of Threat Assessment. Both offices employ professional analysts with experience in counterintelligence, the military, or law enforcement. Their mission is to conduct ongoing investigations into current terrorist, protestor, and criminal information to ensure that the formal DBT remains credible. If current intelligence indicates the need to revise the DBT, each agency has a process to revise and re-issue the DBT to their facilities.

**“Credible” Threat**

The most difficult part of this threat assessment process is to ensure the DBT remains “credible,” e.g., that it does not understate or overstate the threat. If the DBT is not credible, then the PPS may be over- or under-designed, thus presenting more risk than expected or greater cost in counter
Inter-Agency Cooperation Is Vital

The NRC and DOE have both emphasized that cooperation and the exchange of information among many agencies is vital to the process. There is daily interaction among the NRC, DOE, and several other intelligence agencies to share information and intelligence to ensure the DBT is as credible and reasonable as possible.

5.3 Definitions

Terminology

The following terms are used to discuss the development, maintenance, and implementation of a DBT. These definitions are from INFCIRC 225/Rev.5.

Threat

A person or group of persons with the potential (motivation, intention, or capability) to commit a malicious act.

Threat Assessment

An analysis of the threats – based on available intelligence, law enforcement, and open source information – that describes the motivations, intentions and capabilities of these threats.

Design Basis Threat

The attributes and characteristics of potential insider and/or external adversaries who might attempt unauthorized removal or sabotage, against which a PPS is designed and evaluated.

5.4 The Threat Assessment Process

Steps to Threat Assessment

A threat assessment is a formal process of gathering, organizing and assessing information about existing, or potential threats that could result in, or lead to a malicious act. It is conducted by trained specialists who gather and analyze threat data to provide an information product to a customer. This process precedes the development of the DBT. The threat assessment process will be tailored to support the subsequent objective of DBT development. Threat assessors need an understanding of the protected nuclear materials, and the nuclear security environment in order to derive data relevant to the DBT.

Requirements for the Threat Assessment

To focus the threat assessment effort on the needs of the PPS developers, the assessment team is provided the following information:

- What are the likely targets?
- What is the objective of the threat (e.g., theft or sabotage)?
- What types of information should be included in the assessment (e.g.,
need capabilities, motivations, and intentions)?

The assessors need to understand the customer concerns. These include the materials, processes, locations, potential consequences, and timescales. The assessor does not need to know specific vulnerabilities or details of the existing PPS.

In return, the customer needs to understand the limitations of a threat assessment—what it can do, and what it cannot do, how to interpret the threat assessment, and what protection is required for the threat assessment information. The customer does not need to know the sources of intelligence and the detailed data behind the analysis.

The threat assessment should consider threats of terrorism, espionage, proliferation, subversion, and crime. The sources of these threats could be domestic, transnational, or global in nature. The assessment should consider all credible capabilities of a threat entity, even if not yet demonstrated.

While the regulatory agency maintains overall responsibility for the development, maintenance, and implementation of a DBT, the support of other organizations is needed for success. These organizations include, but are not limited to:

- The intelligence community;
- Federal, state, and local law enforcement agencies; and
- Customs and Ministries of Defense.

In the U.S., a Presidential Directive authorizes the regulatory authority to gain support from the various organizations needed to ensure the DBT remains credible and is based on actual intelligence data. This authority for the agencies to interact also provides the mechanism needed for sharing sensitive and classified information between the appropriate agencies and organizations.

A wide and diverse threat exists in the world today. This threat is unprecedented; i.e., it has not yet happened, at least not with enough frequency to provide the data normally available to intelligence agencies. To fill in the information gaps that are inevitable with this type of threat, assumptions are made. Assumptions are things we do not know to be facts. Only those assumptions that are necessary to support a complete and relevant assessment are included. The inferences and considerations that support assumptions should be reasonable. Some examples of assumptions...
that should be considered include the following:

- The attack will occur without warning. Unless there are obvious precursor activities and events indicating an impending attack, the State should not assume prior warning of an attack.

- The attack will not be a foreign state-level act of war. Planning for defense against attacks by foreign states is normally conducted within the State’s Defense Ministry and is beyond the scope of what a facility-level PPS is designed to handle.

- The attacking threat force may have a strong infrastructure. They may be supported by a network of safe houses, good transportation, and sufficient financing.

Once the objectives are established, the assessment can be initiated. The threat assessment is a three-step process:

1. Gathering data for input into the process
2. Analyzing data for credible motivation, intention, and capabilities for each adversary entity
3. Documenting the results of analysis along with some measure of confidence in the data.

Analysts may use any reliable information source to help define the threat assessment. Data can be gathered from a variety of open and classified sources, including human and electronic intelligence sources, law enforcement informants, criminal data, news reports, and other sources. The reliability and credibility of information is important. For example, the Internet provides a great deal of information, but is not always a reliable source. Intelligence analysts provide the expertise to judge the reliability of potential threat data.

The nuclear industry has had very few attacks worldwide, and so analysts have had to draw inferences about the threat from analogous industries. For example, the attacks on embassies, government buildings, and private industries have been analyzed for appropriate information. In the United States, the RAND Corporation completed an extensive study of nuclear crime. Lacking an adequate sample of nuclear incidents from which they might build a profile of the adversaries, RAND analysts expanded their study to include actual crimes outside the nuclear domain that could be related. Several hundred cases of conventional crimes were analyzed, including:
5. Threat Definition

- sophisticated burglaries
- major armed robberies
- industrial sabotage
- crimes committed by well-educated, professional people
- incidents involving political extremists, such as terrorist assaults and “symbolic” bombings, where a political statement—and not the destruction of the target—was the primary aim.

They also examined the criminals (arsonists, psychotic bombers, and mass murderers) as well as the crimes for clues about the criminals’ capabilities and motivations. Just as intelligence experts must evaluate the reliability of data, so also must they evaluate the relevance of attacks in other industries, to ensure that proper inferences are drawn.

Other Information Sources

A review of past and current crimes committed locally, nationally, and internationally may provide useful information in characterizing the potential threat. Other sources that can be considered include:

- the annual State Department report on Global Terrorism (www.state.gov);
- information services such as LEXUS, NEXUS, and FIBIS
- *Jane's International Defense Review*, which includes books on weapons and their capabilities;
- the NRC Safeguards Summary Event List, which lists all events and incidents at nuclear power plants; and annual FBI bomb data.

Data Analysis

The data is analyzed to assess, for each threat entity, their motivation, intentions, and capabilities. Motivations can be ideological, personal, economic, or irrational (psychotic). Intentions by which their motivations are achieved include theft, sabotage, hostage-taking (such as a facility). Understanding, or postulating adversary intentions also helps to judge the relevance of nuclear security-related information from other nations.

Postulated threat intentions might not be the same for all States. Capabilities can refer to the characteristics of how an adversary could undertake its intention. These include group size, weapons, knowledge and skills, equipment, funding, and collusion with insiders. Further, in parallel, the credibility of the data is assessed to measure the confidence that can be placed in the results. Credibility of data includes whether the source of information was direct or indirect, whether the data source has a history of
reliability, and whether the data was independently corroborated.

The results of the analysis of the intelligence data is prepared for the customer in a written report that includes a measure of the confidence in the raw data from which the analysis is drawn. This measure of confidence provides some insight into the weight that should be paid to data concerning different threat entities when consolidating the threat assessment into a DBT.

It might be useful to look at the results in a matrix format, where each column represents a different threat entity, and each row represents a threat characteristic (see Table 5-1). This table format provides a good means of comparing the different threats identified in the Threat Assessment.

<table>
<thead>
<tr>
<th>External Threat</th>
<th>Threat Entity 1</th>
<th>Threat Entity 2</th>
<th>Threat Entity 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motivations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intentions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capabilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Size of Group</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weapons</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Explosives</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transportation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power and hand tools</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical skills</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level of funding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.5 Develop a Design Basis Threat from the Threat Assessment

DBT development takes the threat assessment as an input, and screens it through additional considerations to arrive at an agreed level of PPS required performance and accepted residual risk.

Input for the DBT

The primary input for the DBT is the Threat Assessment document.

Further, the consequences deemed unacceptable by the State should be understood.
### Process for Developing a DBT

The process for developing the DBT involves further analysis and, most importantly, decision-making. There are three important phases of the process:

- screening the threat assessment output for those threats with motivation, intention, and/or capability to commit a malicious act involving nuclear materials and nuclear facilities;
- translating the screened list into a composite adversary with postulated adversary capabilities; and
- modifying the composite adversary postulated capabilities on the basis of relevant policy considerations.

### Screen Output of Threat Assessment

In this phase, the potential targets of malicious action that could lead to unacceptable consequences are compared to the characteristics of each potential adversary.

- If the capabilities are insufficient to cause the consequence at the target (ignoring the physical protection), then this threat entity can be flagged for possible screening.
- If the motivations and intentions of the threat entity are completely incompatible with the malicious act, resulting in unacceptable consequences, then the threat entity can be flagged for possible screening; however, care should be taken in screening a highly capable adversary due solely to lack of motivation. The motivations should be clearly incompatible with the target, act, and consequence.

The rationale for all screened threat entities should be carefully documented. Those threats removed as a result of screening should still be considered if new information becomes available.

### Composite Adversary with Postulated Capabilities

Screened threat entities should be translated into a composite adversary description. This process might be facilitated by reviewing the threat entity characteristics matrix as proposed in Table 5.1. When developing a composite adversary with capabilities assembled from the suite of threat entities outlined in the screened threat assessment, care should be taken to develop a ‘credible’ composite adversary and not simply assemble the worst capabilities from the suite of threat entities.

### Modify Composite Adversary for

The DBT will implicitly define the risk that a State accepts, and is therefore a policy document. As such, the DBT needs to consider policy considerations.
Policy Considerations

- Degree of conservatism of DBT—The DBT needs to compensate for uncertainty in threat assessment data, for possible future evolution of the threat, and address any threats not raised in the threat assessment because it is prudent to do so.

- Cost-Benefit-Consequence Tradeoffs—Managing the risk and benefit of nuclear resources is a policy consideration that must be addressed. Consideration should be given to the risks and costs of protection completed for other non-nuclear resources of similar consequence.

- Political factors—Consideration of public confidence in the State’s responsibility and that of neighboring States needs to be factored into the DBT.

Output of the DBT Process

The output of the DBT process is a description of threat capabilities that a State has committed to mitigate. Not all threats identified in the prior threat assessment process are necessarily included in the DBT.

As mentioned earlier, the DBT is a regulatory tool intended to assist the regulation of licensed facilities. It is possible and even likely that the threat capabilities output from the DBT process are not all applicable to this purpose of regulating licensees. Several threats may exceed the resources and authority that the licensee could be reasonably expected to possess. Therefore the output of the DBT process is reviewed and those threat capabilities that are not appropriate for use to regulate physical protection are set aside. The remainder is the DBT.

Other Threat Capabilities requiring protection

Those threat capabilities not included in the DBT are addressed by the State. These capabilities, sometimes referred to as Beyond the DBT, should be the responsibility of State security organizations and might include Police, Border Control, Aviation Control, or others.

5.6 Using a Design Basis Threat

Introduce the DBT into the Regulatory Framework

The implementation of a DBT in a State will vary based on legal and regulatory constraints established by constitution or laws, on responsibilities...
5. Threat Definition

and competencies of government entities, and on operator competencies and resources in physical protection.

Considering this, the competent authority needs to determine the most effective means to use the DBT to influence effective physical protection. There are basically three options that could be pursued:

- Competent authority provides the DBT to the operator along with guidance on effectiveness of PPS to protect against it
- Regulator establishes performance requirements based on the DBT, and provides performance requirements to the operator
- Regulator defines prescriptive requirements based on the DBT, and provides these to the operator.

In deciding which approach is the most appropriate, a State needs to consider several State-specific factors:

- The competence of the operator to interpret performance requirements
- The number of facilities in a State, and the impact of limiting flexibility of a facility to develop the optimum solution
- The severity of the potential consequences

A State should possess the expertise to evaluate the effectiveness of the protection system against the DBT. To do this evaluation, the DBT may be used as a basis to:

- develop potential adversary scenarios
- conduct analysis of the effectiveness of the protection system
- identify PPS vulnerabilities
- analyze and prioritize potential upgrades

The use of the DBT encourages a strategic approach to physical protection.
## 5.7 Maintaining the DBT

**Review DBT Regularly, or When a Significant Change Occurs**

Although the DBT document relatively static, it can be updated at appropriate intervals. The State’s DBT may be reviewed and revised for the following reasons:

- Routine and periodic review done on a regular basis. The US NRC conducts a periodic review every six months and the US DOE conducts a review every two years.
- A significant event occurs (such as 9/11)
- A significant change in domestic or international regulation, policy, or guidance is made relevant to the DBT
- Changes in nuclear activities are made that might introduce new consequences
- A proposal for review is submitted by any of the interested parties

**Relevant Issues**

The regulatory authority considers updates based on changes in the following:

- Threat conditions and capabilities
- Facility Operators
- Applicable regulations
- State or ministry oversight responsibilities
- DBT or threat assumptions
- The international situation
- Government policy, technical resources, or State resources
- Changes in the physical environment; e.g., new population densities near facilities
- The level of risk
- Facilities or transport conditions
- Targets
5. Threat Definition

After the State has reviewed these questions and has a sound understanding of the issues, it should begin the process of reviewing and revising the DBT. Performing the process described in this document and conducting a comprehensive review of the threat assessment and DBT can complete this effort.

The NRC has a full-time staff in the Office of Threat Assessment that reviews the DBT every six months and reports on whether the DBT is still current. For example, a major change to the DBT occurred in 1993 after two incidents took place:

- At the Three Mile Island reactor, a deranged person drove a vehicle through the gate and crashed it into the roll-up door of the turbine bay. He abandoned the car and was at large in the turbine bay for more than an hour before security forces were able to apprehend him.
- In 1993, militants attacked the World Trade Center. A vehicle bomb blew up in the parking lot underneath the building.

Based on these two incidents, the Office of Threat Assessment added vehicle bombs to the sabotage threat in 1993. The facilities had one year to comment on the proposed addition to the DBT. In 1994, the change was accepted and incorporated into federal law. The facilities then had one year to either:

- Design and install vehicle barriers to prevent this threat from being successful, or
- Prove that a DBT vehicle bomb could not damage vital equipment without vehicle barriers.

Once this phase was complete, NRC personnel reviewed the upgrades and assessments to verify that the PPS would be effective against this type of threat scenario.

5.8 Example Threat Statement

The following is the unclassified portion of the NRC DBT, which is published in the Code of Federal Register that all NRC facilities must comply with to obtain an operating license.

The threat consists of an external assault that is determined and violent, and an attack by stealth or deceptive actions, by several persons with the following attributes, assistance, and equipment:

- Well-trained (including military training and skills) and dedicated indi-
Define Physical Protection System Requirements

- Insider assistance, which may include a knowledgeable employee in any position who attempts to participate in a passive role (e.g., provide information), or an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in a violent attack), or both
- Suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long-range accuracy
- Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system
- Land vehicles used for transporting personnel and their hand-carried equipment
- The ability to operate as two or more teams

Finally, the threat considers the potential for a conspiracy between individuals in any position who have:

- Access to and detailed knowledge of nuclear power plants or facilities, and/or
- Items that could facilitate theft of special nuclear material, e.g., small tools, substitute material, or false documents.

5.9 Summary

DBT Provides Foundation for PPS

Agencies use the DBT process to determine the threats facing their nuclear facilities. The DBT provides the basis for measuring the adequacy of PPS, provides a baseline standard for future changes, and ensures a standardized level of protection for all facilities.

The DBT Process

The international standard for the development of a DBT involves the following process:

1. Conduct a Threat Assessment
2. Understand the Unacceptable Consequences to the State
3. Develop a DBT from the Threat Assessment

The DBT development is a three-step process:

1. Review threat entities from Threat Assessment for relevance to the
5. Threat Definition

**DBT Is a Continuing Effort**

A DBT is continuously evaluated as new information becomes available to ensure it remains credible and provides a sound basis for the design and evaluation of a PPS. As the adversaries develop new capabilities, the DBT must change with the threat.

**DBT Details Are Classified**

To keep information out of the hands of adversaries, some parts of the DBT should be classified. Information, such as specific numbers of attackers and weapons or tactics, should not be shared.

---

5. Threat Definition

targets

a. Screen out threats with insufficient capability
b. Screen out threats with incompatible motivation

2. Develop a Composite DBT to represent the suite of threat entities remaining after Step 1.

3. Modify composite adversary for policy considerations
   a. Modify for degree of conservatism
   b. Modify for cost-benefit considerations
   c. Modify for political factors