

Threat Specific Mitigation

This section provides information that is relevant to mitigation of certain types of threat. It should be read in conjunction with the pages providing information on the current national security threats.

It provides guidance relating to:

- Threat planning assumptions/design basis threats
 - Protection standards
 - Chemical, Biological and Radiological/Nuclear threats, mitigations and responses
-

Threat Planning Assumptions & Design Basis Threat

When developing the requirements for protective security, it is necessary to develop what is known as 'threat planning assumptions (TPA)' or a 'design basis threat (DBT)'. For the purposes of this guidance, CPNI uses terms interchangeably. TPA should define the threats the facility is to be protected against over a specified time, usually several years or life of the facility.

When setting the TPA, it is important that:

- It is developed by competent individuals
- It is proportionate, representative of the threat and caters for an evolving threat picture over the specified period (they should not simply be based on a current assessment of the threat owing to the transient nature of threats and the long time it takes to develop and deliver protective security)
- Granular enough to be meaningful and useful
- It is linked to the security risk assessment and operational requirements process

Examples of TPA might include for example:

- An attack using a Vehicle Borne Improvised Explosive Device of a specified size
- An attack involving a specified number of adversaries, armed with specified number(s) of firearms, ammunition, improvised explosive devices etc.

Design/Protection Standards

Design and/or protection standards often define a level of 'protection' against defined 'threats'. They are essential tools that allow specifiers and suppliers to work to a common goal.

Examples such standards include for example:

- the CPNI Manual Forced Entry Attack Standard (MFES)
- BS EN 1063 – Bullet Resistance of Glass
- IWA 14 – International Workshop Agreement - Performance Requirement, Vehicle Impact Test Method and Performance Rating

When selecting design/protection standards, it is important that they are consistent with the Threat Planning Assumptions/Design Basis Threats. Further information on standards is contained on the linked pages and also in other relevant areas of the Physical Security pages.

Chemical, Biological, Radiological and Nuclear (CBRN)

The principles described above, including an understanding of organisational threats, risks and operational requirements, are equally applicable to CBRN. Furthermore, understanding what threats your protective security measures are effective against, or more importantly are not effective against, (in a similar way to TPA / DBT) is essential in order to appreciate the residual risk your organisation faces.

CBRN is a very broad area which can make processes such as TPA / DBT challenging to undertake. To support this, the linked pages provide information on the different types of materials, how they might be used and their effects and impact.

Guidance is also provided on measures that can lessen the consequence of an attack, including CBRN-specific mitigation methods, response planning and business continuity considerations.

Cyber Assurance of Physical Security Systems (CAPSS)

[MORE INFORMATION](#)

Chemical, Biological, Radiological and Nuclear (CBRN)...

[MORE INFORMATION](#)

Protection from Blast

[MORE INFORMATION](#)

Protection from Ballistic Attack

[MORE INFORMATION](#)

Protection from Forced Entry

[MORE INFORMATION](#)