THE AWARDS
AWARD WINNER
UNIVERSITY OF THE YEAR

University of HUDDERSFIELD
Applied Criminology
Centre

Glossary for Counter-Terrorism Toolkit

September 2015

PRE-EMPT

Process Review and Evaluation of

Multi-Modal Passenger Terminal Security

Paul Ekblom, Michelle Rogerson, Alex Hirschfield,

Kris Christmann and Andrew Newton

Applied Criminology Centre

University of Huddersfield

Orientation:

MS Word version: Use <Ctrl+F> to open Navigation Pane and click 'Headings' tab

PDF version: Open Bookmarks pane to reveal index

Introduction

Inevitably an area as complex, detailed and technical as security needs to define terms, not just for the end users of this report and for future applications, but to help synthesise the literature and to coordinate the teamwork during research and writing up. Two considerations have amplified this requirement – first, the deliberately conceptual approach taken in the project given the dearth of rigorous empirical studies; and second, the sheer diversity of terms, and of meaning assigned to each term, in the literature and in practice. For example, *Countermeasure* is defined by DHS lexicon as 'action, measure, or device that reduces an identified risk', whereas for BS 16000 (see below) it is 'Action taken to counter another action taken, or anticipated to be taken, by an opponent.'

Several well-developed glossaries exist. The most developed one is the Risk Lexicon of some 60 terms by the Department of Homeland Security (DHS)[1].The very recently published British Standard on Security Management (BS 16000)[2] contains a glossary drawing on/consistent with earlier British Standards and ISO 31000 – the more general international Risk Management Standard. Other glossaries/definitions consulted include the Securestations report[3], the Haddon Matrix for injury prevention[4] and UK CT strategy, CONTEST[5]

For the sake of knowledge management it is best to maintain a consistent 'controlled vocabulary', so drawing on prior art is preferable. Unfortunately these existing glossaries differ from one another in significant ways, e.g. over 'hazards' or 'risk assessment'; and neither extends to cover the concepts we have imported from crime science and which we consider vital to understanding what works in what context, and how to implement it. We have not (yet) incorporated any specialised terminology for land transport, though this is subject to review.

We have therefore developed our own glossary, which links as much as possible to these prior ones, but which endeavours to resolve differences and inconsistencies between them and also to connect security with crime science concepts, theory and research. The last connection – which we think is the first of its kind – is principally via two frameworks: the Conjunction of Terrorist Opportunity (CTO: Roach et al. 2005), which covers the immediate causes of terrorist incidents and principles of intervention in those causes in the service of protection and preparedness; and 5Is, a process model originating in crime prevention but extending to security. To resume an earlier illustration, from 5Is and CTO, and extended to cover preparedness as well as protection, we take *Intervention* to refer to reducing the risks of terrorist/criminal incidents via both elimination of possibility, reduction of likelihood and reduction of harm. This is closer to the definition of *Countermeasure* by DHS; we reserve the latter term for the narrower BS 16000 definition stated above. For reasons explained under the 'intervention' entry, we reject the use of the vague term 'measure'.

Our definitions have been developed in parallel with the Realist Review of the literature and the fieldwork for this project, and with the Conceptual Attack Framework (CAF). We have endeavoured to create 'definitions in depth', i.e. to ensure that when a particular definition refers to subsidiary concepts, those are defined too; and the whole suite of definitions is intended to be mutually consistent. The definitions have been incorporated as far as possible within the Indicative Toolkit.

---

[1] www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf
[2] http://shop.bsigroup.com/ProductDetail/?pid=000000000030285866
[3] www.securestation.eu/documents/securestation_d3_1.pdf
[4] http://injuryprevention.bmj.com/content/4/4/302.extract
[5] www.gov.uk/government/uploads/system/uploads/attachment_data/file/97994/contest-summary.pdf.

The current version of the Glossary will need revision as new concepts are encountered or feedback is received about intelligibility and utility. Further development may occur if the ongoing ISO 31000 revision has implications for security risk management (and indeed if the decision is taken to further embed the current indicative toolkit within ISO 31000). For development of the toolkit as a practical resource rather than an indicative one will require development of a set of simpler phrasing backed by the fuller technical definitions, and perhaps some examples, as the DHS lexicon does. Ideally any glossary would need testing for intelligibility, non-ambiguity etc, on an international set of users.

Following the Glossary is a narrative account, with diagram, of the relationships between key concepts.

Sources additional to those fully stated above are:

Cornish, D. (1994b) The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies*, 3, 151—96. Monsey, NY: Criminal Justice Press.

Ekblom. P. (2010) 'The Conjunction of Criminal Opportunity Theory'. *Sage Encyclopedia of Victimology and Crime Prevention,* Vol 1, 139-146. Available in modified form at https://5isframework.wordpress.com/conjunction-of-criminal-opportunity/

Ekblom, P. (2011) 'Deconstructing CPTED… and Reconstructing it for practice, knowledge management and research', thematic issue of *European Journal on Criminal Policy and Research* on *Updating Crime Prevention Through Environmental Design*, 17:7-28.

Ekblom, P. (2011) *Crime Prevention, Security and Community Safety Using the 5Is Framework.* Basingstoke: Palgrave Macmillan. See also https://5isframework.wordpress.com

Ekblom, P and Sidebottom, A. (2008) 'What do you mean, 'Is it secure?' Redesigning language to be fit for the task of assessing the security of domestic and personal electronic goods.' *European Journal on Criminal Policy and Research,* 14:61–87.

Roach, J, Ekblom, P and Flynn, R (2005) 'The Conjunction of Terrorist Opportunity: A Framework for Diagnosing and Preventing Acts of Terrorism.' *Security Journal* 18 (3):7-25.

Other definitions are as originally developed for this project.

The Glossary

Notes:

If you do not find a term you are seeking in the list of headings themselves, searching the entire text may reveal it.

Aka = also known as

5Is framework

A process model of undertaking **security** (**protective** and **preparatory** action) covering **Intelligence**, **Intervention**, **Implementation**, **Involvement** and **Impact**. Essentially an expanded and more detailed version of frameworks such as SARA in problem-oriented policing. (5Is modified)

Affordance

Affordance – how **perpetrators** view MMPT as a means of realising their **goals** of harming **target vectors** and influencing the **target audience**, given their **capabilities** including **tactical atttack methods** at their disposal and the **attack procedural** knowledge and **resources** to carry them out, which, through problem-solving, convert a potential **opportunity** to a **feasible** one.

Asset

Person, structure, facility, information, material, or process that has value. Humans can be considered assets in respect of performing key functions or having key skills; otherwise they are considered and valued separately. See also **critical asset.** (DHS modified)

Attack

Subset of **incidents** in which the main operational attack is undertaken by the terrorist/criminal **perpetrators**.

Attack procedure aka attack script

Steps that a **perpetrator** takes or may take to plan, prepare for, execute and immediately follow through an **attack**. (DHS modified and drawing on crime scripts concept of Cornish)

An **attack script track** is a particular sequence of steps selected/taken at each of the choice points, i.e. a single path from the trunk of the tree to the tip of one branch. (Modified from Cornish)

Attack script permutation

A single procedural thread through the alternative tracks available to **perpetrators** to execute.

Attack tree

A tool to provide a visual representation of the anticipated and potential **procedures/paths** a **perpetrator** can take to execute an attack. (Securestation modified)

Baseline security

Level of **security** that exists currently – a reference point against which to consider the necessity for/nature of additional security in light of new **risk** information

Best practice

See practice

Capability aka resources for offending

The means to accomplish a mission, function, **objective** or **goal**. (DHS modified)

Climate setting

A task of **involvement** that supports **mobilisation** and **partnership** by influencing understanding, expectation and acceptance, among the relevant stakeholders, of particular **protective** and **preparatory** action whether at **tactical**, **operational** or **strategic** level.

Conceptual attack framework (CAF)

Integrating framework developed for this project which maps out the known combinations of **tactical attack methods**, the possible permutations of **attack procedures**, the **protective** and **preparatory** interventions to thwart or mitigate them, and the wider process of doing security at MMPT sites.

Consequences

The direct and indirect effects, typically adverse, of terrorist/criminal incidents whether successful or merely attempts.

Countermeasure

Action taken to counter another action taken, or anticipated to be taken, by an opponent. This could cover action taken by a **perpetrator** to counter a **security intervention**, or by the **security** side to counter an action by a **perpetrator**. (BS16000 modified)

Critical asset

Any person, facility, equipment, service or resource considered essential to operations in peace, crisis and war and warranting action to ensure its continued efficient operation, protection from disruption, degradation or destruction, and timely restoration. (Securestation modified)

Damage assessment

Process to determine the magnitude of damage and the unmet needs of individuals, businesses, the public sector, and the community caused by an **incident**. (Securestation modified)

Enclosure aka target enclosure

Space bounded by a barrier, with an interior, designed entrance/exit points and a periphery. The interior usually contains **target vectors**, although additionally or instead the enclosure as a whole can be a **target vector**. The potential **target vectors** may be subject to attack within the enclosure, at the entrance/exit points (e.g. queueing) or at the periphery. One enclosure may contain others (e.g. private, staff-only zones within the otherwise public space in the MMPT); the main enclosure is located in a **wider environment** which may include space under the control of the MMPT such as car parks, of other organisations (e.g. neighbouring businesses) or public (e.g. the adjacent streets). (CTO modified)

Event

A pre-planned short-term activity of some significance, e.g. a major football match. Distinguished from an **incident** which is specifically a harmful, or potentially harmful, and unforeseen event.

Goal aka objective, aim, purpose, intent

Intended end state to be achieved by some action/procedure. The goals in question are those of **perpetrators**. Hygiene goals are those the **perpetrator** wants to avoid, e.g. of being detected or arrested. For clarity, the term **objective** is used for the security side.

Good practice

See practice

Governance

Processes and systems for regulation, consultation and decision-making; responsibility, authority and accountability. Covers a wide range of strategic-level domains including legislation, policymaking and **partnership**; and **operational** domains including information-sharing. (5Is modified)

Harm

Undesired **consequences** of some incident including death, injury, operational interruption, disruption, loss, emergency or crisis. The consequences can be suffered by persons, places, systems, networks or other **assets**; they can be direct, or mediated via a subsequent chain of cause and effect. (Securestation and DHS modified)

Hazard aka risk source

A natural or man-made cause of **harm**, duress [DHS] or difficulty – some object, environmental configuration or behaviour that, usually in conjunction with other necessary or sufficient conditions, brings into existence, or increases, the **risk** of harmful incidents. A *potential* hazard is one where other events must occur or conditions must be met (perhaps as a result of intentional or incidental human action) for it to become an actual hazard.

- A hazard is not inherently targeted, but a **perpetrator** can:
  - intentionally *create* and *target* a hazard – e.g. a booby-trap bomb (whole thing becomes a threat with a hazard embedded in it)
  - intentionally *exploit* and *target* a pre-existing hazard – e.g. creating a panic/crush down some hazardous stairs, or triggering a landslip
  - unintentionally cause a hazard as a *side-effect* of intentional terrorist/criminal action – e.g. children caught in crossfire of attack on police
- A hazard may constitute a key part of a terrorist/ criminal **opportunity**; other aspects of **opportunity** include the **target vector** of **perpetrator's** malevolent **goal** that is **vulnerable** to the hazard, the capability/resources and presence of perpetrator to manipulate the hazard or its context, **enclosure** and **wider environment** in which the hazard is situated or which it can affect; absent/incapable **preventers**; present **promoters.** (CTO modified)

Impact aka outcome

Impact is the extent to which planned and implemented **security** action meets its **objectives**, principally in reducing the targeted **risks** of terrorism and crime.

Impact evaluation aka outcome evaluation

Impact evaluation seeks to determine, in an appropriately rigorous way, the extent to which **security** action has met its **objectives**, a causal link can be reliably attributed, and (Realist Evaluation) ideally the underlying mechanisms and necessary contextual conditions identified.

Implementation

Set of practical and managerial tasks required to realise the methods of **Intervention**. The people-oriented dimension is **involvement**. (5Is modified)

Incident aka harmful event

An event, caused (in a **security** context) by malevolent human action, unforeseen by the legitimate authorities, that may constitute, cause or enable, **harm** and that may require **protective** and/or **preparatory** action to reduce its **risk**. Includes the occurrence of potential terrorist or criminal actions at earlier stages of the **attack procedure**, e.g. hostile reconnaissance, which could be termed preparatory **incidents**. Note that **event** in general is used to refer to pre-planned short-term activities of some significance. (DHS modified)

Instantiation

Converting a generic concept into a specific instance, for example by populating the generic **attack procedure** by the parameters of a particular **tactical attack method** combination.

Intelligence (process and product)

1) The process of gathering and analysing information and knowledge on terrorism and crime, their nature, **likelihood**, causes and **harmful consequences**, in order to inform the setting of **security objectives** and priorities; the planning and design of the **security Intervention**/s and the other tasks

that follow. 2) The product of the intelligence process – information to guide decisions and action (5Is modified)

Intervention

The theoretical principles and practical methods of achieving **protective** and **preparatory objectives** and thwarting the goals of **perpetrators**: respectively, blocking, diverting or weakening the causes of terrorist or criminal **incidents** or of wider community safety problems, so the **likelihood** of their occurrence, and the **harm** they cause, is reduced; and stopping ongoing **harmful incidents** and **mitigating** the **harm** already done. The looser term 'measures' is often used in the literature but we believe this does not give the focus of intervention, **implementation** and **involvement** as the main tasks of the **security** response; moreover, it can be confused with 'measurement' .(5Is modified)

Involvement

The action whereby professional security practitioners seek, through **mobilisation** or **partnership**, to get other people, departments and agencies to understand, accept, and undertake the tasks, roles and responsibilities of implementing **protective** or **preparatory** interventions; or otherwise to share or support them by alleviating constraints, boosting enablers and establishing a receptive **climate**. Involvement is the people-oriented side of **implementation**. (5Is modified)

Likelihood

The chance of some **incident** happening, usually on a ranked scale with a greater or lesser degree of formalisation (see **probability** for formal mathematical equivalent). (BS 16000 modified)

Mechanism aka causal mechanism

The detailed cause-effect process of how some **intervention method** works, typically by interactions between the deployment of the method and a number of factors in the **perpetrator** and in the **situation** of the terrorist/criminal **incident** or events preceding it. Many of these are considered as context or background factors whose presence is necessary for the mechanism to be successfully triggered. **Principles**, **methods** and mechanisms are primarily used to describe **interventions** (and other action) at the **tactical** level. (5Is modified)

Method (of protection/preparedness) aka technique

Practical realisation of one or more **intervention principles**; methods work via causal **mechanisms**. (5Is modified)

Mitigation

Action to reduce or immediately make good **harm**, undertaken either during (secondary **security**) or immediately after (tertiary **security**) undesired **incident** or its knock-on consequences. (Haddon matrix, 5Is modified)

Mobilisation

Action by **security** professionals to invite, persuade or sometimes order other individuals, groups or organisations to take positive **security** action or to desist from activities which **promote** terrorism or crime. (5Is modified)

Objective aka aim, goal or purpose

Intended end state to be achieved by some action/procedure. The objectives in question are those of the **security** side. For clarity, the term **goal** is used for the **perpetrator** side.

Operational level, operations

Level of **security** action that coordinates the minute details of **tactics** with the overarching objectives of **strategy**. We take this to refer to actions designed to achieve or support the achievement of immediate local **objectives**, especially **security objectives**, through the deployment on-site of **security tactics**. Note – this is based on military literature; in much business literature and in some emergency planning literature, the operational level is placed *below* that of **tactics** and the meaning is essentially reversed.

Opportunity

An ecological concept, relating to how agents encounter, seek or create a set of circumstances in which their resources enable them to cope with the **hazards** and exploit the possibilities in order to achieve their multiple **goals**/**objectives**. The agents and their **goals/objectives** can be malevolent or benevolent, hence a terrorism opportunity or a **security** opportunity. The **goals** can be positive (getting the money…) or 'hygiene' related (…whilst avoiding arrest or injury). Opportunity comprises some **goal/objective**, **capability/resources** to carry it out, a **vulnerable**, rewarding and/or provocative **target vector**, and a broader set of conducive immediate contextual conditions. The *Conjunction of Terrorist/Criminal Opportunity* (CTO/CCO) integrates all the above factors into a single framework which covers both understanding the immediate causation of terrorist/criminal **incidents**, and the theoretical **principles** by which these causes are blocked, weakened or diverted in order to reduce the **risk** of those **incidents** occurring/causing **harm**.

A **feasible** opportunity is one which **perpetrators** are **capable** of exploiting, either as it currently is or with modifications they are capable of making. The alternative is a **blocked** one.

An **opportunity path** is where every stage of an **attack procedure** encounters feasible opportunities.

Partnership aka interagency, multiagency working

A way of enhancing performance in the delivery of a common **objective**, and perhaps of extending the scope of action, by the taking of joint responsibility, the sharing of risk and the pooling of resources by different public and/or private agencies. (5Is modified)

Perpetrator aka offender, terrorist, criminal, adversary

Individual, group, organization, or government that conducts or has the **intent** to conduct terrorist/criminal activities. (DHS modified)

Practice (best, good, recognised…)

In the Realist Review – based on research evidence and published expertise

- **Best Practice** – *strong* research evidence that the practice was effective in its implementation and impact *and* outperformed alternatives
- **Good Practice** – *strong* research evidence of effectiveness in implementation and impact, *without* a comparative element; or *moderate* research evidence *with or without* comparison
- **Potentially Good Practice** – assessments of implementation and impact are *moderate to strong* and *with or without* comparison but based on a *consensus of opinions* from experts and respected authorities/ organisations rather than empirical research
- **Highlighted Practices** – claimed as effective or ineffective in the literature but without any supporting evidence
- **Practices to avoid** – the literature suggests these would *not* be beneficial; and where there is *strong-moderate* research evidence and/or a *consensus of expert opinion* to support the claim

In the Fieldwork – based on professional judgement of experienced research team

- **Recognised good practice**
- **Practice to avoid**
- **Practice which may be good or that should be avoided depending on context**
- **Neutral or uncertain evidence**
- **Identification of a contradiction requiring resolution e.g. through design**

Practices (other practices)

Practices are any kind of replicable **security**-related action, including but not exclusively, **interventions**. Other practices are **security** actions which do not amount to a complete **intervention**, i.e. deploy no **methods/mechanisms** sufficient in themselves to reduce the risk of terrorist/crime **incidents** whether through **protection** or **preparedness**. An example is training.

Preparedness aka emergency preparedness

Advance action to make procedures and **assets** ready to resist/respond should a terrorist/criminal **incident** occur. Comprises secondary **security** which is stopping an ongoing **incident**; and tertiary security which is **mitigating** immediate and subsequent **harms** from that **incident**. (CONTEST and 5Is modified)

Preventers

Individuals, groups, departments or organisations who reduce the **risk** of terrorist/criminal **incidents** by delivering **protection** and **preparedness**, whether acting professionally, in line with job responsibilities, as **mobilised** by professionals or spontaneously. Includes roles of guardian of target and manager of place. (5Is modified)

Principles (of protection/preparedness) especially Intervention principles

Intervention principles are theoretical abstractions/generalisations of how **interventions** work (i.e. of causal **mechanisms**) e.g. by increasing the effort to perpetrators (Rational Choice perspective), increasing deterrence (e.g. 11Ds), hardening the **target** (situational prevention/CPTED) or restricting resources for **perpetrators** (CTO). Other principles relate to **implementation** (e.g. covering project management) or **involvement** (e.g. principles of **mobilisation**).Principles are realised through practical **methods** with which they have a many-to-many relationship (i.e. one **method** can work via several principles as alternative possibilities, or operating in conjunction; one principle can be realised in practice by several **methods**). Principles, **methods** and **mechanisms** are primarily used to describe **interventions** (and other action) at the **tactical** level. (5Is modified)

Probability

Formal mathematical representation of **likelihood**.

Problem

A set of environmental circumstances that hinders an agent (or agents), equipped with a certain set of resources, from immediately achieving a particular **goal** or **goals/objectives**. The agents and their **goals/objectives** can be malevolent or benevolent.

Process evaluation

Process evaluation covers the sequence of actions undertaken to deliver the desired **impact**. It assesses performance and identifies obstacles, constraints, enablers, tradeoffs, design contradictions and wider issues concerning all the detailed tasks described under **Intelligence, Intervention, Implementation** and **Involvement**.

Promoters

Individuals, groups, departments or organisations who increase the **risk** of terrorist/criminal **incidents** whether deliberately, recklessly or inadvertently. Note that for the purpose of the present project this relates to increasing the **opportunity** for terrorist/criminal action, not, say, to radicalisation. (CTO modified)

Protection aka primary security

Advance action, on-site, to eliminate the **risk** of **harmful** terrorist/criminal **incident** as a *possibility,* or failing that to reduce its **likelihood** and potential **harm**. Will usually centre on **opportunity** reduction via ***situational*** *prevention*. (CONTEST, 5Is, Haddon Matrix modified)

Protector aka preventer

Role of person (or intelligent software) who undertakes **protection**, i.e. **primary security**, before an **incident** (might) occur, whether as formal **security** professional, designated employee, general employee or third party e.g. a passenger.

Redundancy

Additional or alternative systems, sub-systems, **assets**, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, **asset**, or process. (DHS)

Residual risk

Risk that remains after **interventions** are **implemented**. (BS 16000 modified)

Resilience

Ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions. (DHS)

Responder

Role of person (or intelligent software) who undertakes **secondary or tertiary security** during or immediately after an **incident**, whether as formal **security** professional, designated employee, general employee or third party e.g. a passenger

Response

Closely-defined and usually pre-planned **security** action taken on detection of an **incident**, receipt of a **threat message** or detection of a **vulnerability**. Differs from the more open-ended **security** action under **intervention**

Risk (general)

Effect of uncertainty on **objectives** or **goals**; in the case of terrorism/crime, the uncertainty is about malintended harmful outcomes. (BS 16000 modified)

Risk (terrorist or crime) (see also Scenario)

Potential for a harmful outcome from a particular terrorist or crime **incident** or set of similar **incidents**. *A* risk can be described as a possibility i.e. the set of **harmful incidents**, which can occur with a certain **likelihood**, and be **harmful** either in themselves or via increasing the risk of subsequent **harmful** events. A risk is caused by a combination of **perpetrator threats**, **target vector vulnerabilities**, and **harmful consequences** associated with the **incident**. (DHS modified)

Risk analysis

Product or process to comprehend the nature of risk and to determine the level of risk; an aspect of **Intelligence** (BS 16000, 5Is modified)

Risk assessment

Product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making. Draws on **risk analysis**. (DHS modified) OR: = identifying internal and external **threats** and **vulnerabilities**, identifying the **likelihood** of an **incident** arising from such **threats** or **vulnerabilities**, defining **critical** functions necessary to reduce exposure, and evaluating the cost of such controls (Securestations).

Risk control

Deliberate action taken to reduce risk or maintain it at an acceptable level. (DHS modified)

Risk management

Coordinated activities to direct and control an organization with regard to risk (BS 16000); in detail, process of identifying, analyzing, assessing, and communicating risk and **treating** it by accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost. (DHS modified)

Scenario (threat or risk)

Hypothetical permutation, of greater or lesser specificity depending on available information, comprising a particular terrorist/criminal **intent** and **capability** (including particular **tactical attack methods** and weapons), supplying and/or exploiting a particular **hazard** to which the **target vector** is **vulnerable**), through a particular **attack procedure**, with particular **harmful consequences**. (DHS modified)

A given Attack Threat Scenario, matched up with particular Situational Opportunity factors at the MMPT which Perpetrators must exploit and/or cope with at every step of the relevant Attack Procedure, generates a **Feasible Risk Scenario**.

Secured by Design (SBD)

UK national-level expert police body focusing on the design and security for new and refurbished homes, commercial premises and car parks as well as the acknowledgement of quality security products and crime prevention projects. www.securedbydesign.com

Security

Deliberate action to reduce the **risk** of terrorist/criminal incidents, taken before, during or after a given **incident**; and intended to eliminate the possibility of the **incidents**, reduce the **likelihood** and reduce the immediate or subsequent **harm**. Comprises primary security (**protection** to prevent the occurrence of **incidents**) secondary security (**preparatory** action for stopping ongoing **incidents**) and tertiary security (**preparatory** action for **mitigating harm** from **incidents**). (5Is modified)

Screening

Security screening is a procedure, intended to check whether individuals are carrying weapons, reconnaissance devices (e.g. cameras or other unauthorised items), undertaken at specific places where the screening authority has jurisdiction (normally the entrance to an **enclosure**, at internal checkpoints, or occasionally at random). The procedure is often facilitated by built-environment and technological arrangements, e.g. a barrier/desk and some kind of detector device, but it may be purely behavioural. Security screening may be combined procedurally, and/or in physical arrangements, with *right-to-travel* screening; the particular arrangements and the wider context may also have positive or negative implications for crimes ranging from fare evasion to assault of staff; and for terrorist risk eg if queues form or are dispersed.

Situation aka terrorist/crime situation

Those aspects of the conjunction of **opportunity** during and/or immediately preceding a terrorist/criminal **incident**, which the **perpetrator** exploits, and has to cope with in undertaking an attack or preparatory action. Includes both the **target (vector)**, **enclosure**, wider **environment**, **preventers** and **promoters**. (CTO)

Solution

A set of actions that overcomes **problem**/s to enable the realisation of an **opportunity** and hence the achievement of **goals/objectives**. This applies to both **Perpetrator** and **Protector** perspectives.

Strategic level, strategy

Top level **objectives** which can relate to **security** alone, or wider considerations e.g. provision of efficient, economical and open transport services. Served by **operations** and then at most detailed level, **tactics**.

Surveillance

An **operational security** task which can be subdivided into a generic script of watching, patrolling or remotely monitoring some building, interior or landscape, for the presence of some suspicious person or object, or occurrence of suspicious behaviour; detecting a possible hazard or suspicious behaviour; provisionally attributing innocent or terrorist/criminal intent; investigating further; and/or making some escalatory **response**, whether to confront or arrest the person directly, take protective action such as evacuating the vicinity, report or summon assistance. (Deconstructing CPTED)

Tactical level, tactics

Principles and **methods** of **protective** and **preparatory interventions** available to deploy and customise to particular MMPT sites. The lowest level of abstraction of **security** action.

Tactical attack method

Manner and means, including the weapon and delivery method, which a **perpetrator** may use to cause **harm** to a **target vector**. (DHS modified)

Target audience

Persons, organisations, governments, communities or societies intended to be influenced, perhaps as part of a wider campaign, via the effects of the terrorist/criminal **incident** upon **target vectors**. (CTO)

Target vector/target

Persons, organisations, assets, network, system or geographic area chosen by a perpetrator to be adversely affected by an incident in order to influence the target audience. In many non-terrorist crimes, the term target is sufficient; this can also be used in the case of terrorism, for brevity (CTO, modified by DHS)

Terrorism/crime situation

Immediate physical/social context in which **perpetrator** may undertake some action of interest including the **attack** itself; comprises the **target vector/s, enclosure, wider environment,** actual/potential **hazards** in situ which could serve as **resources** for offending, and people, groups, organisations or departments undertaking **preventer** and **promoter** roles. (CTO modified)

Threat (see also Scenario)

A combination of terrorist/criminal **capability** and **intent**, generating a malevolent action potential to cause one or more **incidents** whose immediate purpose is to **harm** some **target vector**. This can be done by creating, exploiting and directing a **hazard** to which the **target vector** is **vulnerable**. (DHS modified)

Track aka attack procedure track

In an **attack procedure** or **script**, where there are alternative actions available to complete a given step, or several such steps, a track is one permutation of the sequence of steps from start to finish. (Cornish modified)

Vulnerability

Intrinsic properties of some **asset** or person, resulting in susceptibility to a **hazard** that can enable the occurrence of an **incident** which is inherently **harmful** or engenders **harmful consequences**. A vulnerability is always relative to a **hazard**, and by implication relative to the **threat** that may create or exploit that **hazard**. (BS 16000 modified, see also IIS)

Wider environment

The environment within which the **enclosure** is embedded. The **enclosure** could be the MMPT; but if there is an **enclosure** *within* the MMPT, e.g. control room, the rest of the MMPT constitutes the first layer of the wider environment relative to that. (CTO modified)

Key relationships

The diagram below (Figure 1) and this accompanying narrative are an attempt to outline the relationships between key terms in the glossary.

The numbers and letters are assigned purely for narrative purposes, there is no particular significance in the number sequence or hierarchy apart from some elementary groupings (e.g. 1a-c).

In generating the narrative we can adopt, in turn, the different perspectives of **Threat** in general (pink boxes); the Perpetrators' **Capability** to realise the threat (pink); the **Situation** which motivates and/or enables the attack (green); the **Risk** of the attack (blue); and its **Consequences** (purple). Lines representing influences **on** the Perpetrators are red; those emanating **from** the Perpetrators are **black**; general influences on Risk are blue; and the pale green line between Target vector and Target enclosure indicates that these may sometimes be one and the same thing.

Starting from the left, the **Threat** from the Perpetrator [1] comprises their Capability [1a] and their Intent (goals) [1b]. Intent is motivated and directed [A] by factors of the Target vector (Utility and Provocativeness to perpetrator) and perhaps by similar factors [B] of the wider MMPT site or its environs. Threat is focused by the [1c] presence of the Perpetrator in, or remote influence (e.g. by internet or drones) on the Situation [3]. This presence is enabled [C] by the approachability of the Enclosure [4f] within its Wider Environment [4]. (Physical or remote accessibility of the MMPT to the Perpetrators renders the Threat a potentially Present Threat.)

The above Threat factors and Perpetrator Presence empower [D] the Perpetrators to [E] create or bring in [5] External hazards (e.g. a potential landslip or a bomb) or misuse [F] Internal hazards [4a] already on-site (e.g. a fuel store, steep escalator). These are activated, ie from potential to actual hazards, [G,H] in order to exploit the Vulnerability [2a] of the Target vector to injury, damage or destruction from them, in attacking it [I]. The Vulnerability of the MMPT Enclosure [4b] can be exploited [J] to enable access [K] to Target vectors [2] in the interior; alternatively, the Enclosure [4] can be all or part of the Target vector in itself (e.g. blow up the station building, versus get inside building to attack passengers within it). (Hence the green line linking them.)

Perpetrators' **Capability** [1a] (including Tactical Attack Methods and Attack Procedural knowledge) enables them [D] to

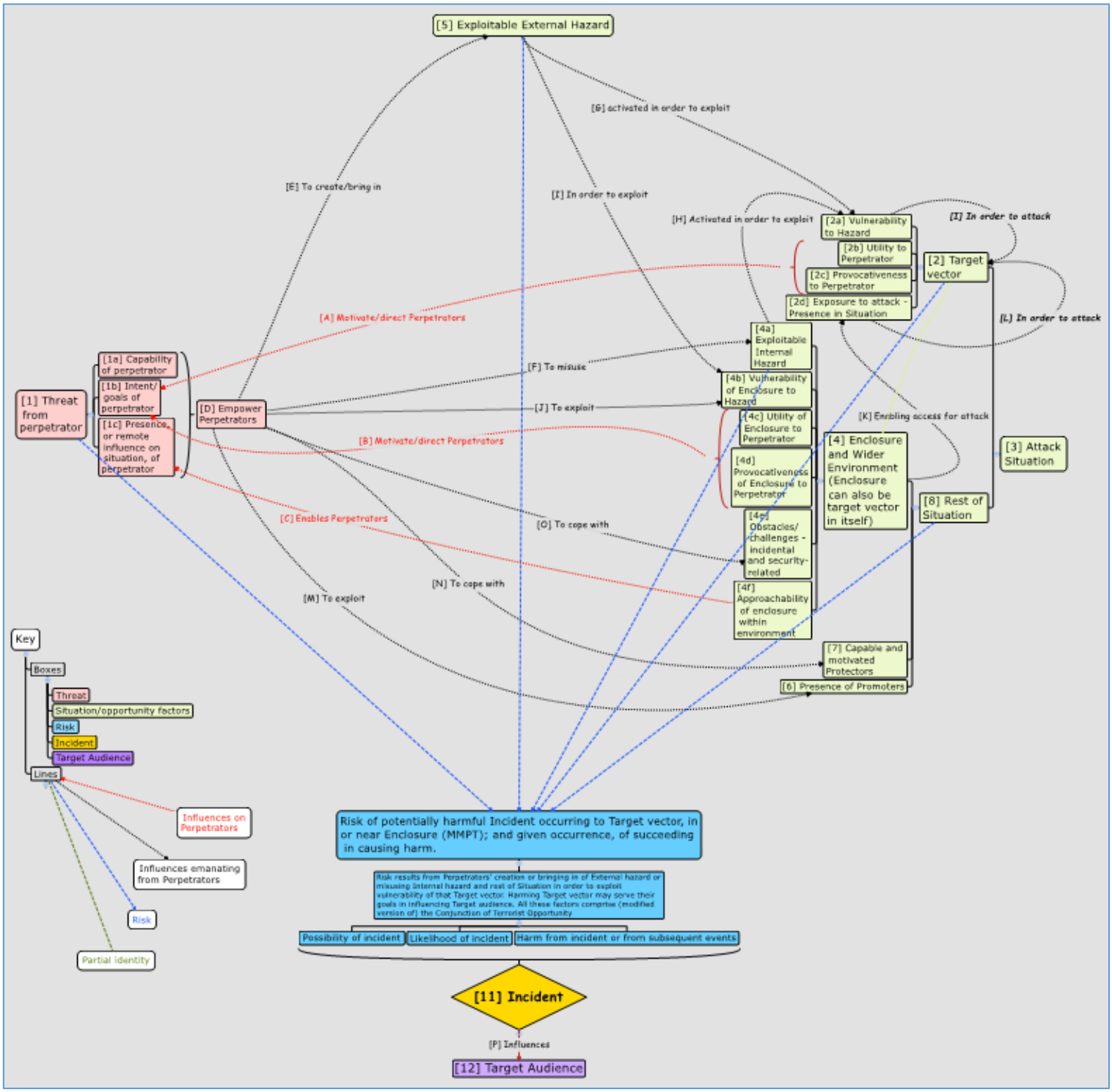
- Generate, activate and misuse [E,F,G,H] the Hazards [4a,5] to exploit [I] the Vulnerability [2a] of the chosen Target vectors [2];
- Do likewise to exploit [J] the Vulnerability of and Enclosures [4b] enabling access [K] to attack [L] the Target vector [2] where the latter is people or assets within it;
- Exploit [M] the presence of Promoters [6] (e.g. people who leave the control room door carelessly unlocked, or a deliberate insider supporter);
- Cope [N] with the actions of Protectors [7] (e.g. security guards), and [O] deliberate security-related obstacles and challenges [4e] (e.g. barriers, CCTV), and incidental counterparts (e.g. high-voltage cables, train movements).

The immediate **Situation** [3] in which the Incident may occur thus comprises the Target vector [2], the (presence or absence of) Protectors [7] and Promoters [6], and the Enclosure(s) [4] and Wider environment, which in turn contain both exploitable Hazards [5, 4a] and obstacles/challenges to the Perpetrators' pursuit of their goals [4e]. To be effective, the Hazards (whether Internal [4a] or External [5] in origin) may require various contextual conditions elsewhere in the Situation [8] to be met (e.g. an incendiary may only work if the weather is dry and still).

All the above interacting factors come together (blue lines) in the Conjunction of Terrorist (or Criminal) Opportunity which produces a heightened **Risk** [9] of an Incident being initiated, and once initiated, of succeeding in causing harm.

In terms of **Consequences** [10] the Incident [11] then influences [P] the Target audience [12], the nature and magnitude of the influence depending on whether/to what extent the harm was successfully caused.

Figure 1 – Key relationships in the Glossary



Note – a higher quality graphic (svg format for web browsers) is available from the Pre-Empt website.