Pre-EMPT

Process Review and Evaluation of Multi-Modal Passenger Terminal Security

University of HUDDERSFIELD

Dr Andrew Newton
& Professor Paul Ekblom

Applied Criminology Centre,
University of Huddersfield, UK
a.d.newton@hud.ac.uk; p.ekblom2@hud.ac.uk

Inspiring tomorrow's professionals

THE AWARDS AWARD WINNER UNIVERSITY OF THE YEAR

theguardian UNIVERSITY AWARDS Winner 2013

2012 THE AWARDS WINNER Entrepreneurial University of the Year

THE QUEEN'S AWARDS FOR ENTERPRISE

Overview

University of HUDDERSFIELD

- Project Aims
- Methodology:
  - Conceptual Attack Framework (CAF)
  - Realist Literature Review
  - Fieldwork/ Site Visits
- Complexity of Multi-Modal Passenger Terminals (MMPTs)
- Findings
  - 8 General Principles for Securing MMPTs
- Future Steps

- CAF Demo
- Indicative Toolkit
- Future Steps

Project Aims

- **to understand** how MMPTs operate and tactical security challenges they face
- **to identify** ‘best practice’ solutions to securing MMPTs from terrorist attack and serious crime
- **to produce** an indicative toolkit
- **to inform** the development of a pan EU Land Transportation Security Strategy

Multiple Methods Approach

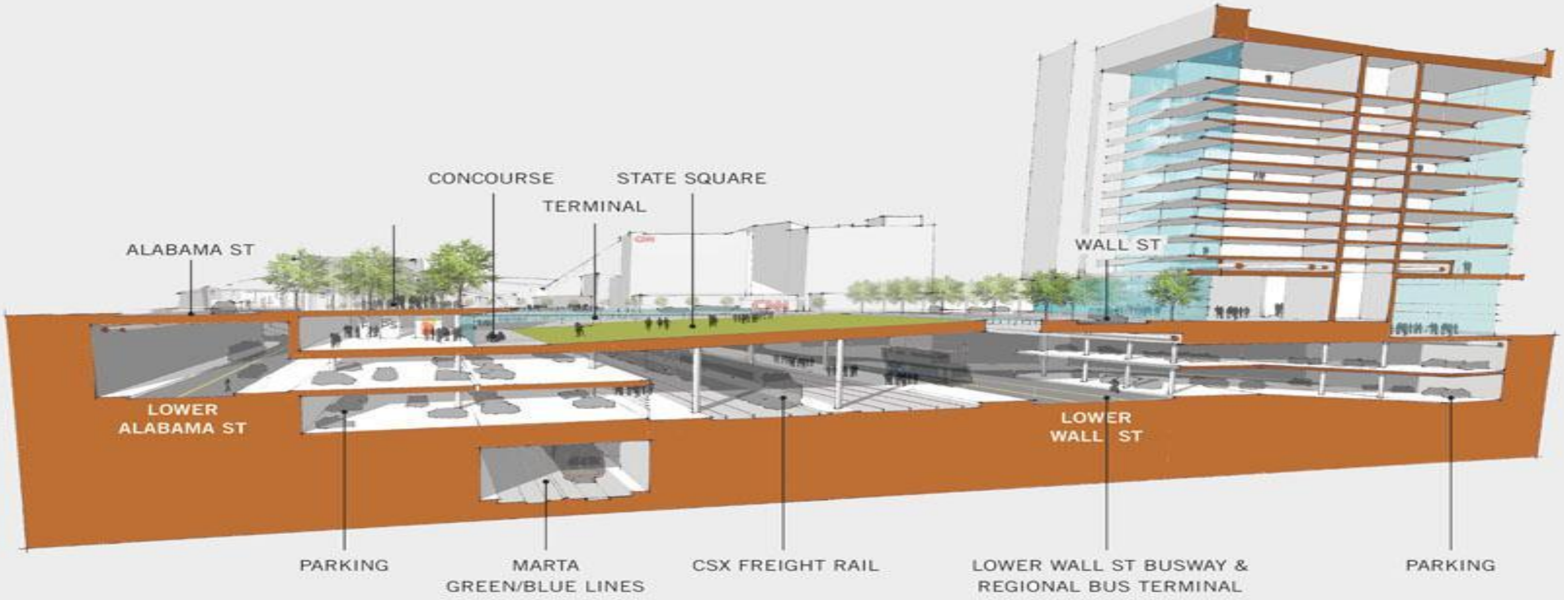
1. Creation of a Conceptual Attack Framework

2. Realist Review of Literature

3. Fieldwork

4. Development of an ‘indicative’ toolkit

Complexity of MMTP



Transport, Infrastructure & Land Use	Integral/ Adjoining Retail/Leisure Facilities	What varies between MMPTs
Transport Mode Over-ground Rail Metro System Tram System Bus Station Taxi Rank **Infrastructure** Waiting areas Concourses and platforms Walkways Escalators Elevators Ticket & other barriers	Retail outlets Supermarkets Pubs and Bars Fast food establishments Restaurants	Environmental Design Opening/ Closing times Responsibility for security Training of security staff Surveillance & communications (equipment & practices) Land & property ownership Jurisdictions for security staff (patrols) Governance Structures Vetting of staff Site maintenance requirements /practices Partnership working Passenger flows by time Flows of other site users (employees, visitors, customers) Vehicles (passenger vs. freight trains) Open and restricted areas for site users Entry and exit points Environmental Quality

Realist Review

- Searched 15 Bibliographic Data Bases
- Approached relevant organisations and experts
- 409 relevant items identified (abstract/title)
- 139 documents reviewed in depth (34%)

Fieldwork

University of HUDDERSFIELD

- to experience contrasting MMPT environments

- to gain insights/capture experience based knowledge
  - management of security incidents
  - different agencies involved
  - partnership working
  - available resources
  - existing security interventions
  - recognised good practice
  - areas of concern

Conceptual Attack Framework

- Map out theoretically plausible attacks

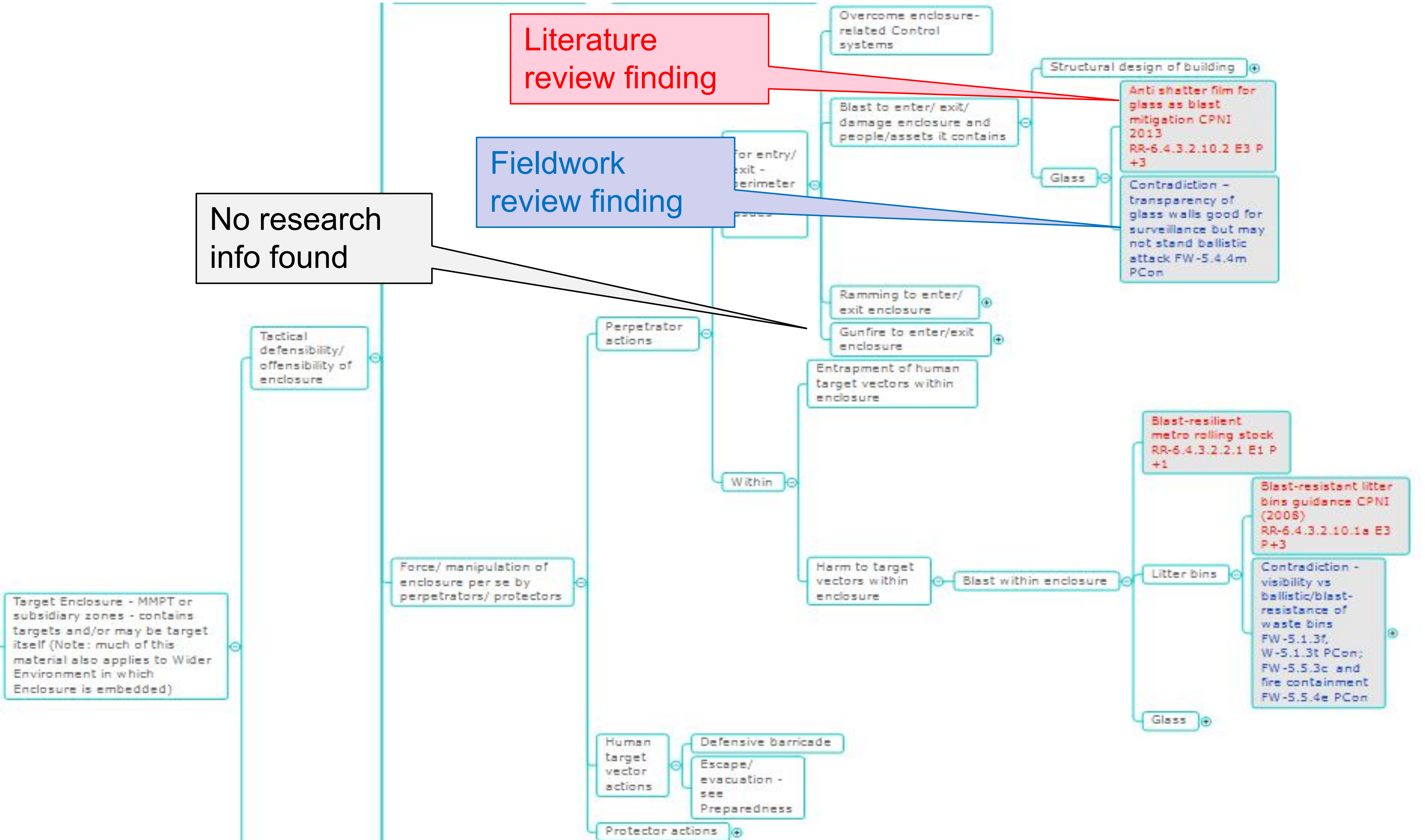
- Map out theoretically plausible responses

- Compare recorded attacks and responses
  - Literature and fieldwork,
  - Organised them on ‘knowledge trees’

- Flagged plausible attacks & responses:
  - absent from the literature
  - not on the ‘radar’ of practitioners

CAF: Consolidating Findings

University of HUDDERSFIELD



Literature review finding

Fieldwork review finding

No research info found

Target Enclosure - MMPT or subsidiary zones - contains targets and/or may be target itself (Note: much of this material also applies to Wider Environment in which Enclosure is embedded)

Tactical defensibility/ offensibility of enclosure

Force/ manipulation of enclosure per se by perpetrators/ protectors

Perpetrator actions

for entry/ exit - perimeter

Overcome enclosure-related Control systems

Blast to enter/ exit/ damage enclosure and people/assets it contains

Structural design of building

Glass

Anti shatter film for glass as blast mitigation CPNI 2013 RR-6.4.3.2.10.2 E3 P +3

Contradiction – transparency of glass walls good for surveillance but may not stand ballistic attack FW-5.4.4m PCon

Ramming to enter/ exit enclosure

Gunfire to enter/exit enclosure

Within

Entrapment of human target vectors within enclosure

Harm to target vectors within enclosure

Blast within enclosure

Blast-resilient metro rolling stock RR-6.4.3.2.2.1 E1 P +1

Litter bins

Blast-resistant litter bins guidance CPNI (2008) RR-6.4.3.2.10.1a E3 P+3

Contradiction - visibility vs ballistic/blast-resistance of waste bins FW-5.1.3f, W-5.1.3t PCon; FW-5.5.3c and fire containment FW-5.5.4e PCon

Glass

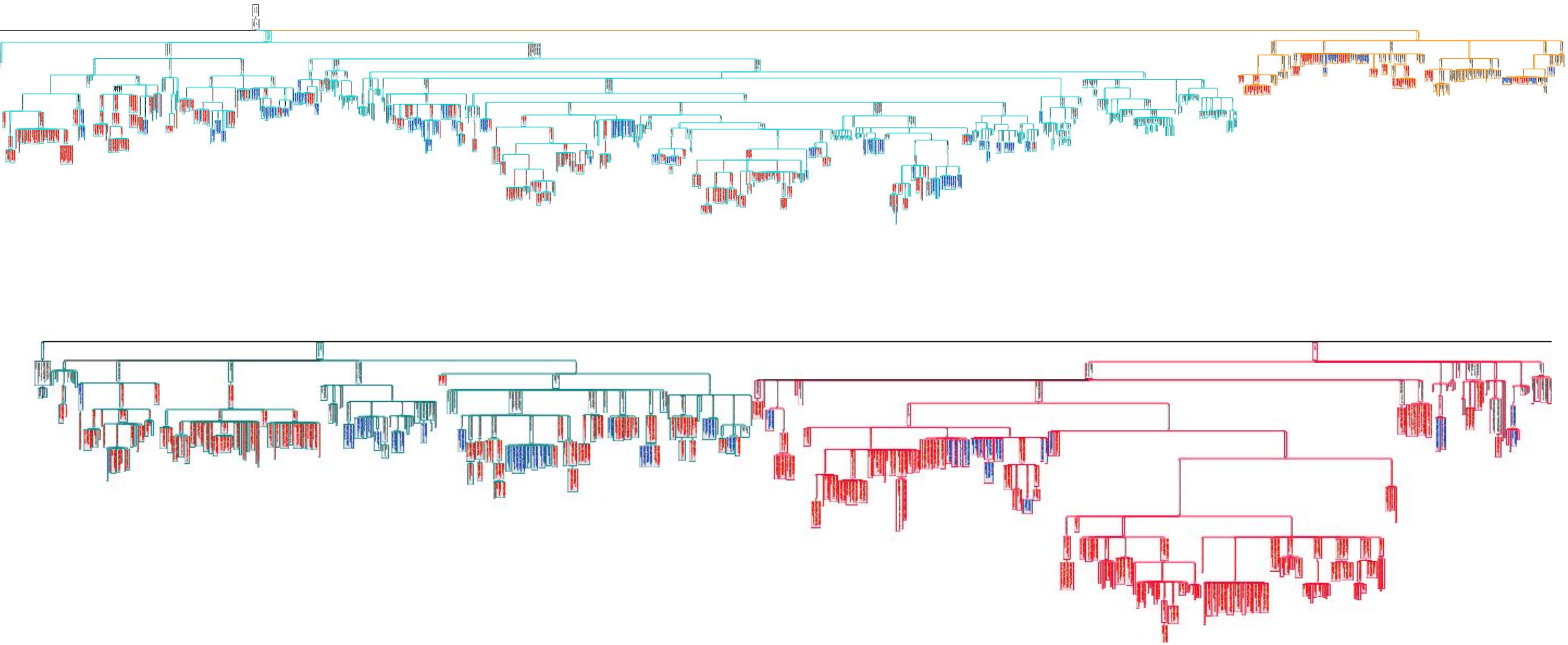
Human target vector actions

Defensive barricade

Escape/ evacuation - see Preparedness

Protector actions

CAF: Entire Visual



Quality Assessment

Literature[1]	**Experience-based Knowledge** [2]
Best Practice	Recognised Good Practice
Good Practice	Context-Dependent Practice
Potentially Good Practice	Contradictory Practice
Highlighted Practice	Indeterminate Practice
Practice to Avoid	Practice to Avoid
[1] Based on nature & strength of supporting evidence	[2] Based on professional expertise & practitioner knowledge

8 General Principles

University of HUDDERSFIELD

1. Adopt standardised EU-level definitions of all terms relating to security at MMPTs
2. Set up holistic governance structures & partnership working arrangements at MMPTs
3. Implement basic interventions for physical protection and harm mitigation at MMPTs
4. Manage and control the movement of people using MMPTs
5. Maximise opportunities to conduct effective surveillance at MMPTs
6. Ensure security approaches & interventions are appropriate for MMPT site and context
7. Provide Training of staff working at MMPTs
8. Strike a balance between the need for security and other priorities at MMPTs

Principle 7

Provide Training of staff working at MMPTs

Recommended Practice	Practices/ Areas of Concern
Training in: ❖ How to identify and report suspicious situations ❖ Who to report to ❖ How to communicate information to site users ❖ Awareness of terrorism ❖ Familiarity with first response procedures in event of an attack **Plus:** ❖ Consistency in content and quality of training for all staff (security, cleaners, retail) ❖ Regular assessments of staff competence	❖ Failure to provide customer service training where required – ensure staff are 'approachable' by passengers

Principle 8

<u>Strike a balance</u> between the need for security & other priorities at MMPTs

Recommended Practice	Practices/ Areas of Concern
❖ Unobtrusive security interventions that do not disrupt people’s daily routines or normal business activities ❖ Interventions that are appropriate and proportionate ❖ Strike balance between generating alertness and fear ❖ Consideration of security design requirements at earliest possible stage in design process	❖ Airport style security at MMPTs ❖ Luggage screening especially random screening contradicts privacy, liberty values ❖ Complex ticket queueing procedures that generate crowding and aggression

MMPT Security Baseline

- Our research findings suggest each MMPT should consider
- **Developing and implementing** a baseline security plan comprising:
    - A communications policy;
    - A physical security strategy;
    - Movement control plan;
    - Site surveillance protocol
    - Essential security awareness training programme for all staff catering for different levels (strategic, operational, tactical)

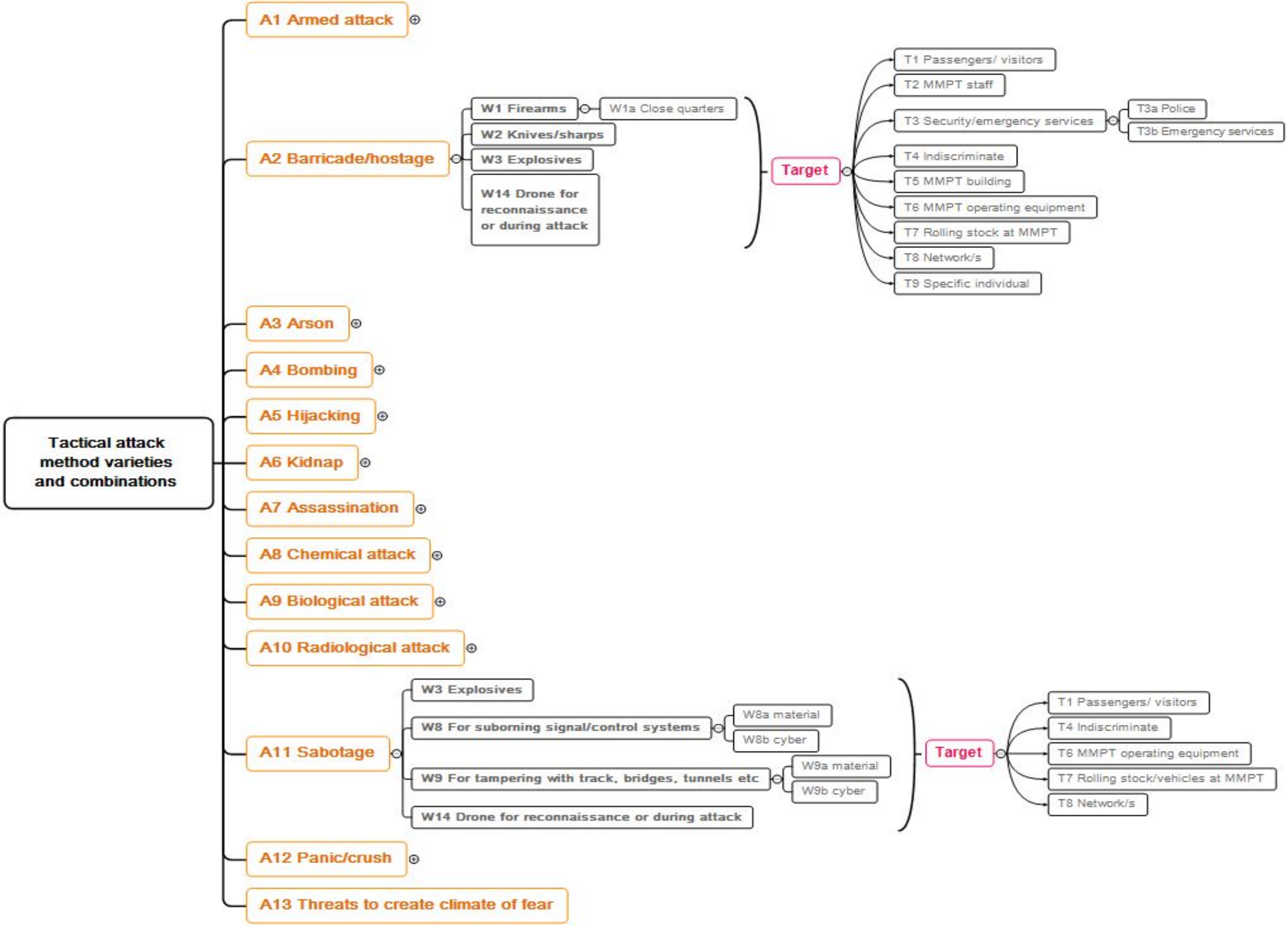
CAF and Indicative Toolkit Demo

University of HUDDERSFIELD

Note to interpreters: The following slides are animated – some of the text boxes are only visible when the slide is played.

The very detailed boxes, e.g. at rh side of Slide 34, hidden by blank boxes, AND THE MAJORITY OF Slide 43, will not be spoken but are just meant to show the presence of more information.

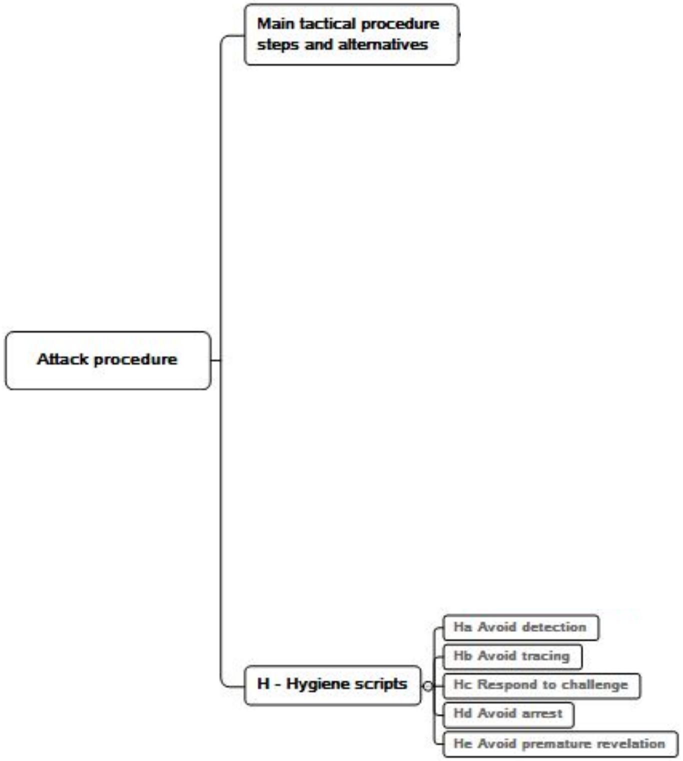
CAF: Illustrations I – Tactical attack methods



Tactical attack method varieties and combinations

- A1 Armed attack
- A2 Barricade/hostage
  - W1 Firearms
    - W1a Close quarters
  - W2 Knives/sharps
  - W3 Explosives
  - W14 Drone for reconnaissance or during attack
  - Target
    - T1 Passengers/ visitors
    - T2 MMPT staff
    - T3 Security/emergency services
      - T3a Police
      - T3b Emergency services
    - T4 Indiscriminate
    - T5 MMPT building
    - T6 MMPT operating equipment
    - T7 Rolling stock at MMPT
    - T8 Network/s
    - T9 Specific individual
- A3 Arson
- A4 Bombing
- A5 Hijacking
- A6 Kidnap
- A7 Assassination
- A8 Chemical attack
- A9 Biological attack
- A10 Radiological attack
- A11 Sabotage
  - W3 Explosives
  - W8 For suborning signal/control systems
    - W8a material
    - W8b cyber
  - W9 For tampering with track, bridges, tunnels etc
    - W9a material
    - W9b cyber
  - W14 Drone for reconnaissance or during attack
  - Target
    - T1 Passengers/ visitors
    - T4 Indiscriminate
    - T6 MMPT operating equipment
    - T7 Rolling stock/vehicles at MMPT
    - T8 Network/s
- A12 Panic/crush
- A13 Threats to create climate of fear

CAF: Illustrations II – Attack procedure



Attack procedure

Main tactical procedure steps and alternatives

H - Hygiene scripts

Ha Avoid detection

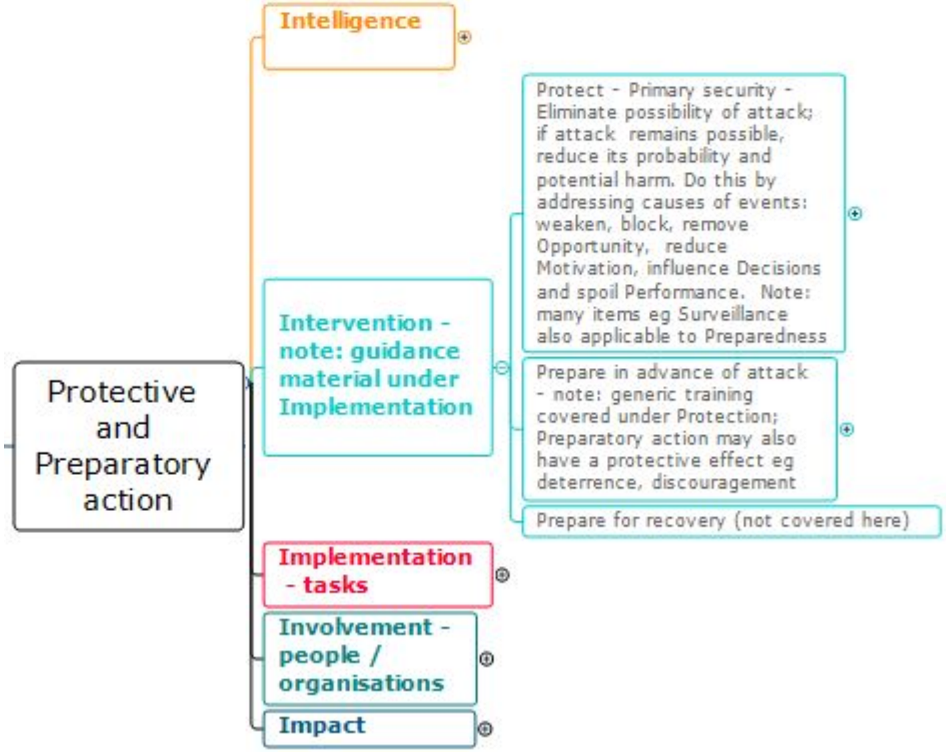
Hb Avoid tracing

Hc Respond to challenge

Hd Avoid arrest

He Avoid premature revelation

CAF: Illustrations III – Security action - Intervention



Protective and Preparatory action

Intelligence

Intervention - note: guidance material under Implementation

Protect - Primary security - Eliminate possibility of attack; if attack remains possible, reduce its probability and potential harm. Do this by addressing causes of events: weaken, block, remove Opportunity, reduce Motivation, influence Decisions and spoil Performance. Note: many items eg Surveillance also applicable to Preparedness

Prepare in advance of attack - note: generic training covered under Protection; Preparatory action may also have a protective effect eg deterrence, discouragement

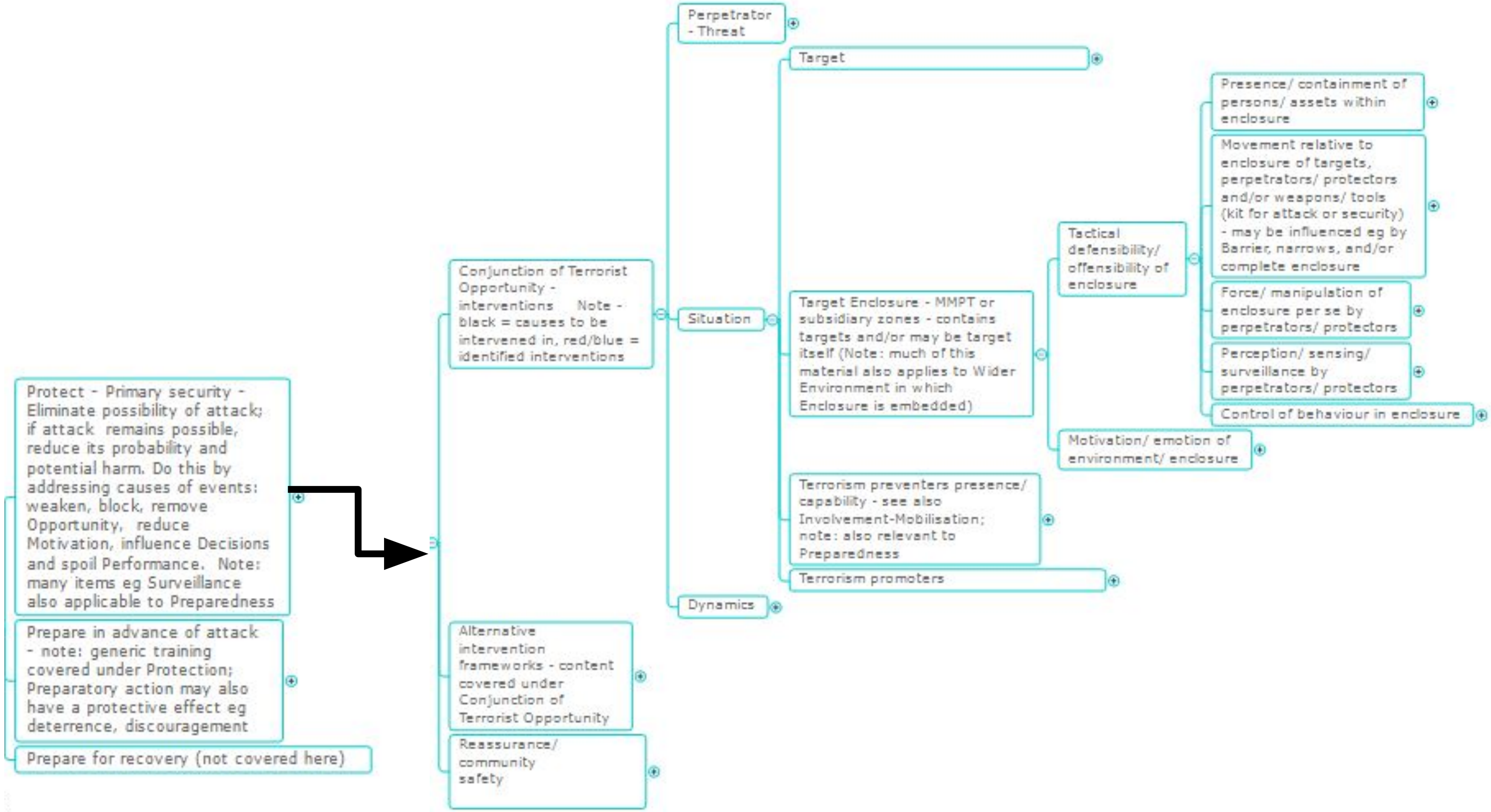
Prepare for recovery (not covered here)

Implementation - tasks

Involvement - people / organisations

Impact

CAF: Illustrations IV – Security action – Intervention – Protect



Protect - Primary security - Eliminate possibility of attack; if attack remains possible, reduce its probability and potential harm. Do this by addressing causes of events: weaken, block, remove Opportunity, reduce Motivation, influence Decisions and spoil Performance. Note: many items eg Surveillance also applicable to Preparedness

Prepare in advance of attack - note: generic training covered under Protection; Preparatory action may also have a protective effect eg deterrence, discouragement

Prepare for recovery (not covered here)

Conjunction of Terrorist Opportunity - interventions Note - black = causes to be intervened in, red/blue = identified interventions

Alternative intervention frameworks - content covered under Conjunction of Terrorist Opportunity

Reassurance/ community safety

Perpetrator - Threat

Situation

Dynamics

Target

Target Enclosure - MMPT or subsidiary zones - contains targets and/or may be target itself (Note: much of this material also applies to Wider Environment in which Enclosure is embedded)

Terrorism preventers presence/ capability - see also Involvement-Mobilisation; note: also relevant to Preparedness

Terrorism promoters

Tactical defensibility/ offensibility of enclosure

Motivation/ emotion of environment/ enclosure

Presence/ containment of persons/ assets within enclosure

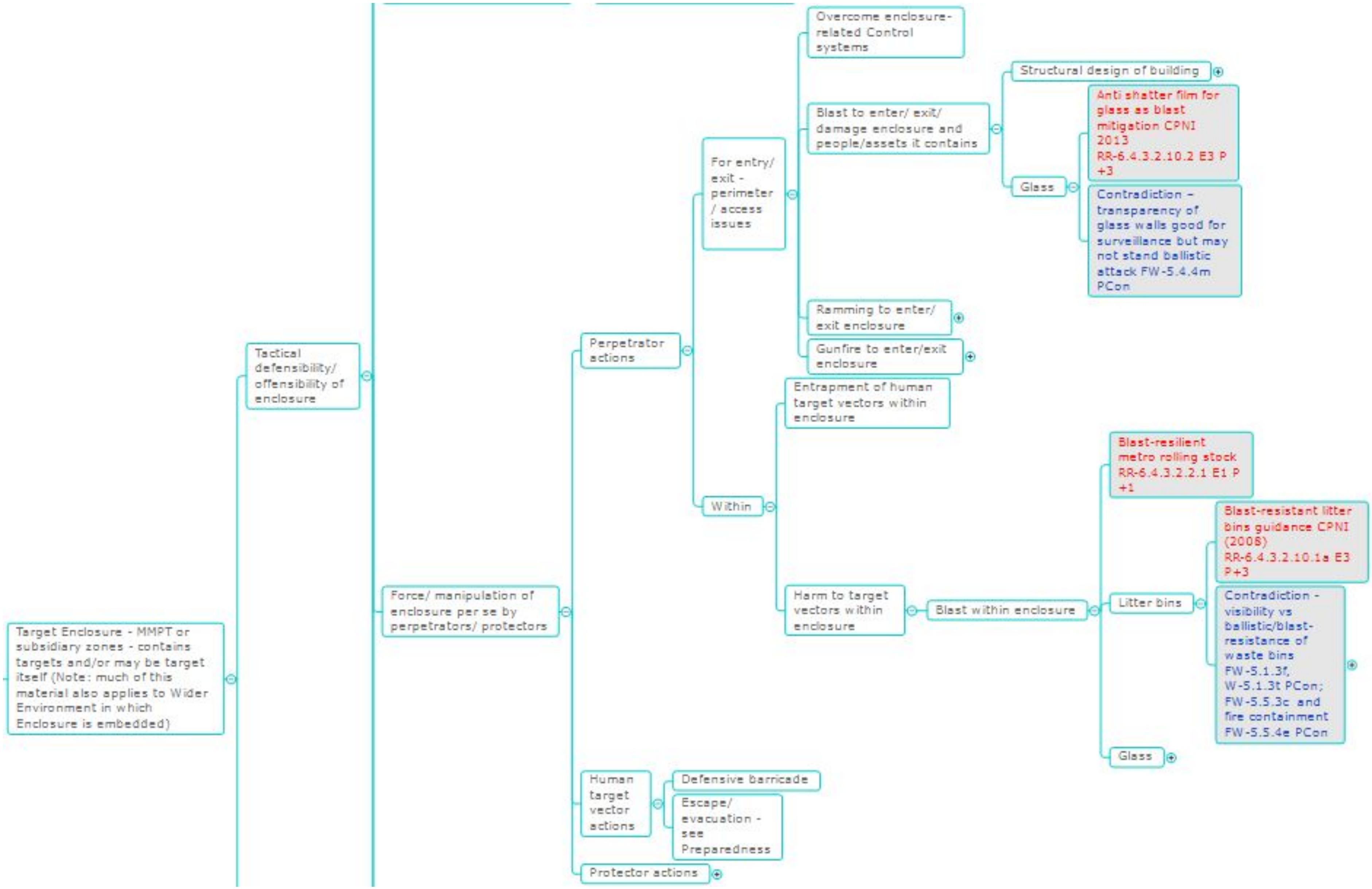
Movement relative to enclosure of targets, perpetrators/ protectors and/or weapons/ tools (kit for attack or security) - may be influenced eg by Barrier, narrows, and/or complete enclosure

Force/ manipulation of enclosure per se by perpetrators/ protectors

Perception/ sensing/ surveillance by perpetrators/ protectors

Control of behaviour in enclosure

CAF: Illustrations V – Adding in the findings



Target Enclosure - MMPT or subsidiary zones - contains targets and/or may be target itself (Note: much of this material also applies to Wider Environment in which Enclosure is embedded)

Tactical defensibility/ offensibility of enclosure

Force/ manipulation of enclosure per se by perpetrators/ protectors

Perpetrator actions

For entry/ exit - perimeter / access issues

Overcome enclosure-related Control systems

Blast to enter/ exit/ damage enclosure and people/assets it contains

Structural design of building

Glass

Anti shatter film for glass as blast mitigation CPNI 2013 RR-6.4.3.2.10.2 E3 P +3

Contradiction – transparency of glass walls good for surveillance but may not stand ballistic attack FW-5.4.4m PCon

Ramming to enter/ exit enclosure

Gunfire to enter/exit enclosure

Within

Entrapment of human target vectors within enclosure

Harm to target vectors within enclosure

Blast within enclosure

Blast-resilient metro rolling stock RR-6.4.3.2.2.1 E1 P +1

Litter bins

Blast-resistant litter bins guidance CPNI (2008) RR-6.4.3.2.10.1a E3 P+3

Contradiction - visibility vs ballistic/blast-resistance of waste bins FW-5.1.3f, W-5.1.3t PCon; FW-5.5.3c and fire containment FW-5.5.4e PCon

Glass

Human target vector actions

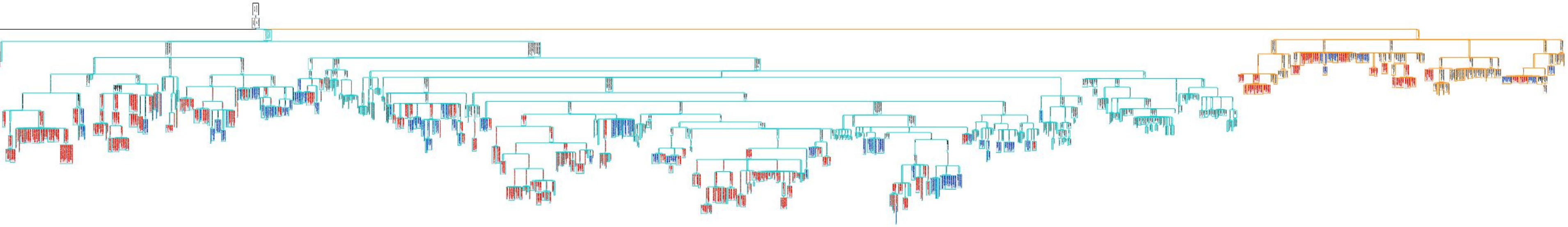
Defensive barricade

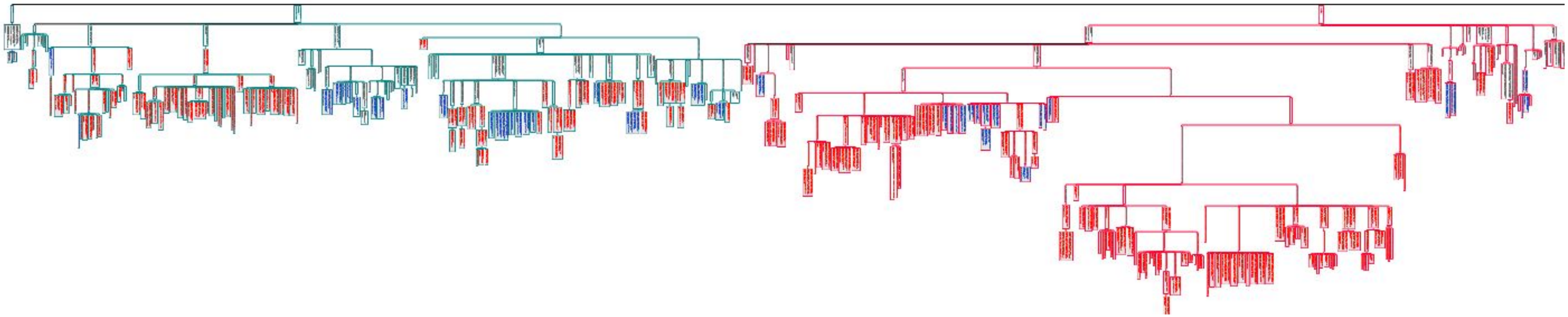
Escape/ evacuation - see Preparedness

Protector actions

CAF: Illustrations VI – All the findings

University of HUDDERSFIELD

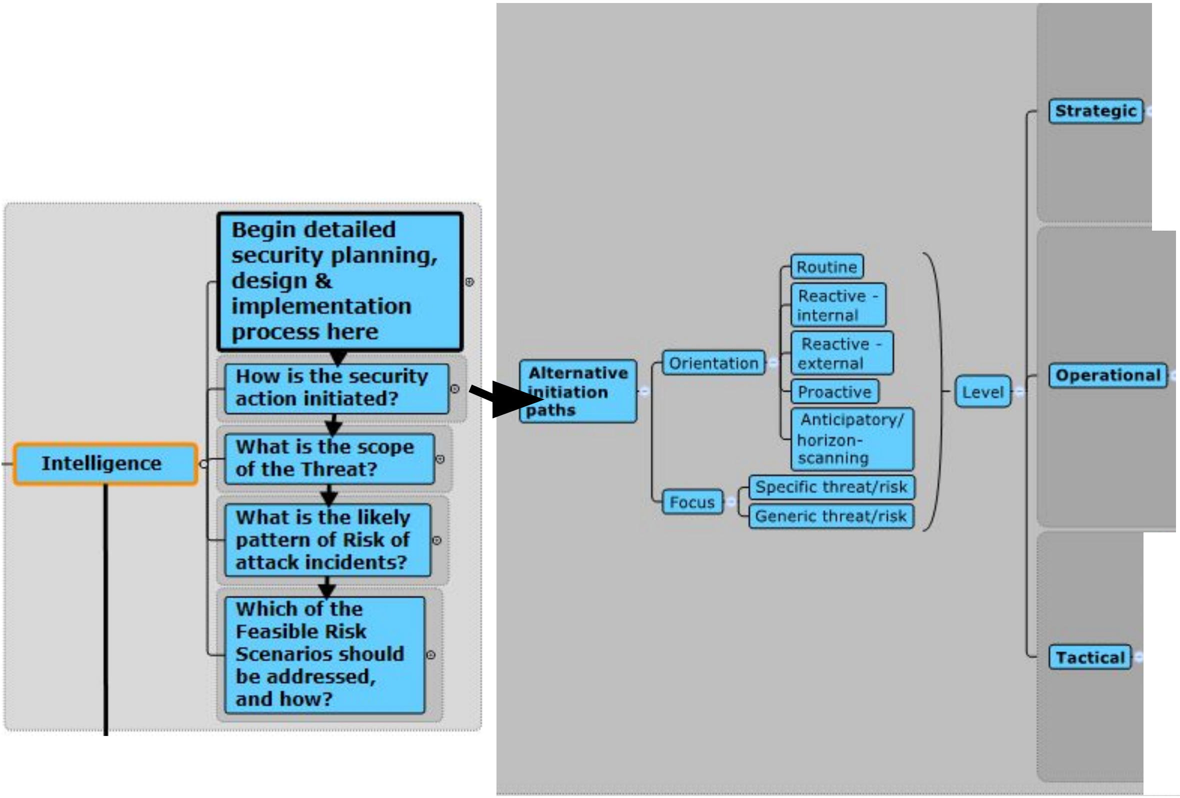




Indicative toolkit – based on 5Is process model

Indicative toolkit process

Intelligence – Initiation of security action at MMPT



Intelligence

Begin detailed security planning, design & implementation process here

How is the security action initiated?

What is the scope of the Threat?

What is the likely pattern of Risk of attack incidents?

Which of the Feasible Risk Scenarios should be addressed, and how?

Alternative initiation paths

Orientation

- Routine
- Reactive - internal
- Reactive - external
- Proactive
- Anticipatory/ horizon-scanning

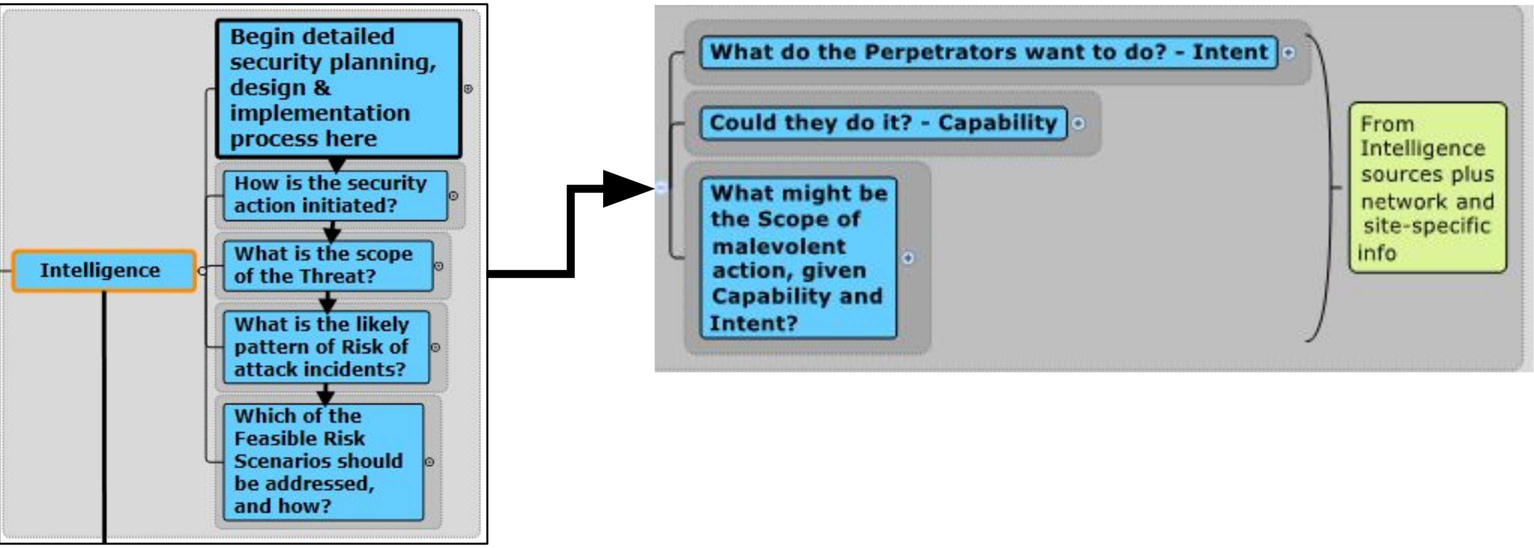
Focus

- Specific threat/risk
- Generic threat/risk

Level

- Strategic
- Operational
- Tactical

Intelligence – Scope of threat



Intelligence

Begin detailed security planning, design & implementation process here

How is the security action initiated?

What is the scope of the Threat?

What is the likely pattern of Risk of attack incidents?

Which of the Feasible Risk Scenarios should be addressed, and how?

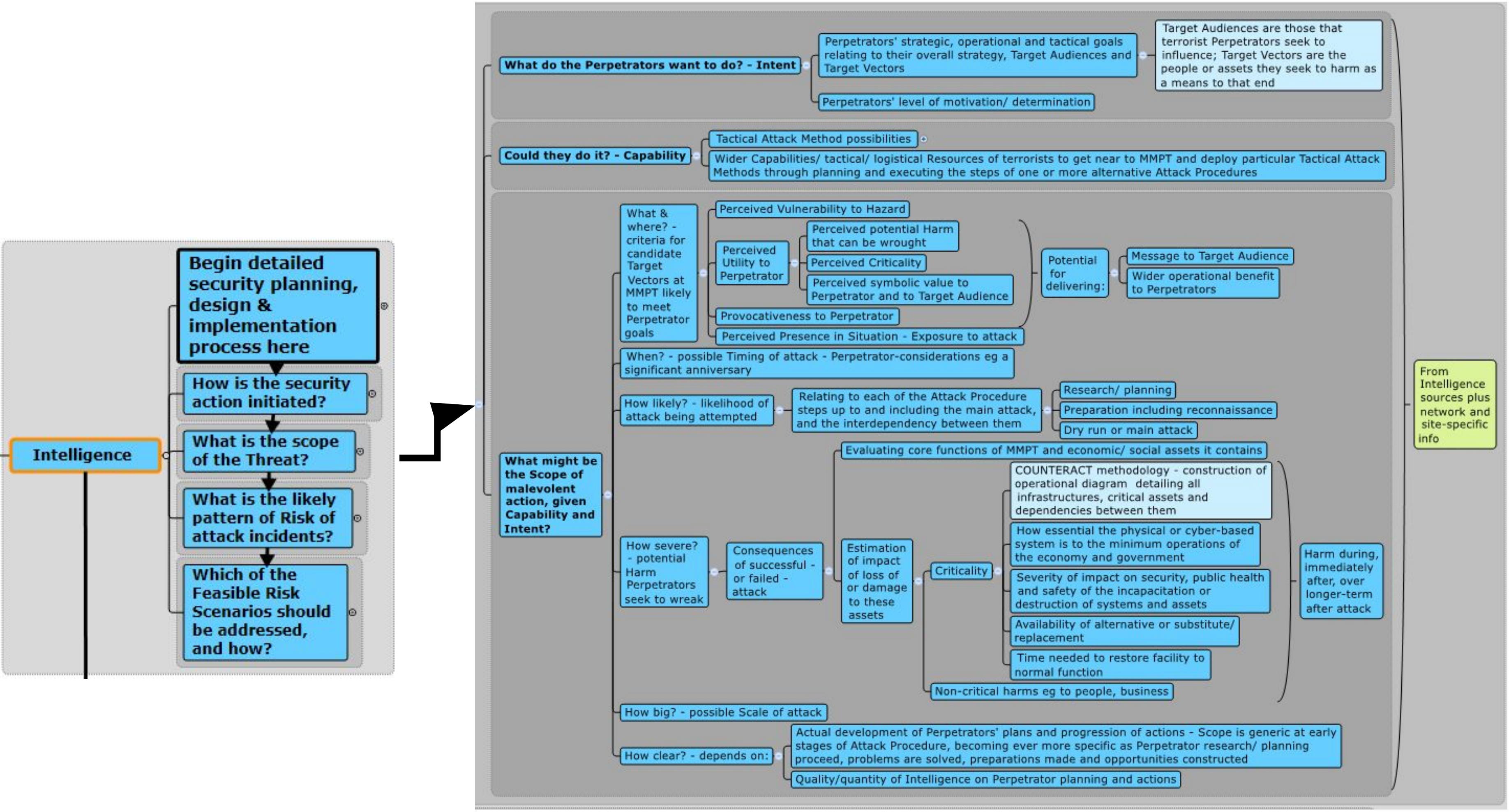
What do the Perpetrators want to do? - Intent

Could they do it? - Capability

What might be the Scope of malevolent action, given Capability and Intent?

From Intelligence sources plus network and site-specific info

Intelligence – Scope of threat



Intelligence

- Begin detailed security planning, design & implementation process here
- How is the security action initiated?
- What is the scope of the Threat?
- What is the likely pattern of Risk of attack incidents?
- Which of the Feasible Risk Scenarios should be addressed, and how?

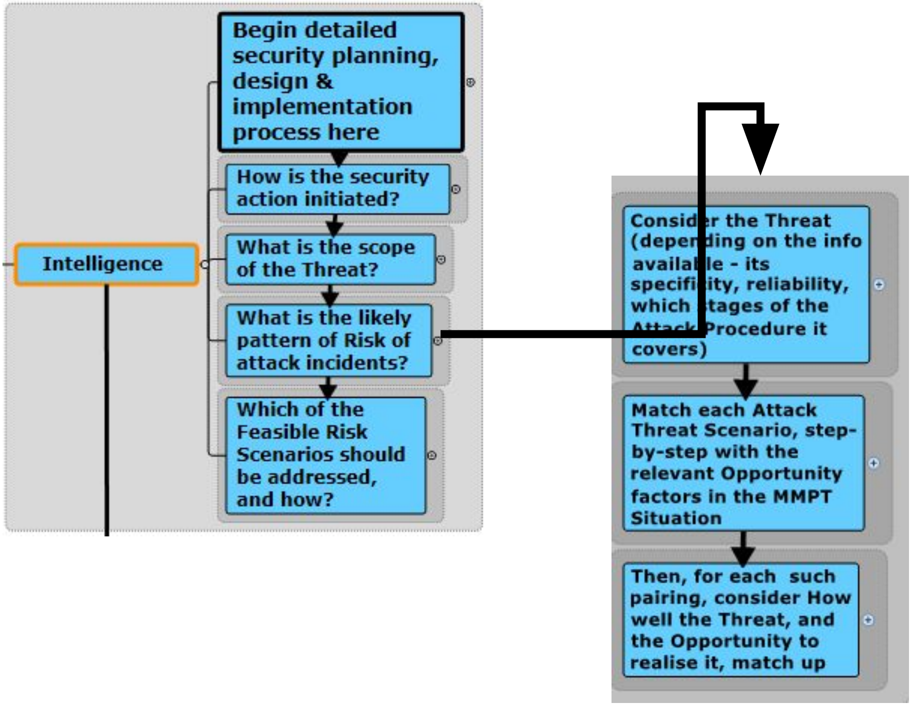
What do the Perpetrators want to do? - Intent
- Perpetrators' strategic, operational and tactical goals relating to their overall strategy, Target Audiences and Target Vectors
  - Target Audiences are those that terrorist Perpetrators seek to influence; Target Vectors are the people or assets they seek to harm as a means to that end
- Perpetrators' level of motivation/ determination

Could they do it? - Capability
- Tactical Attack Method possibilities
- Wider Capabilities/ tactical/ logistical Resources of terrorists to get near to MMPT and deploy particular Tactical Attack Methods through planning and executing the steps of one or more alternative Attack Procedures

What might be the Scope of malevolent action, given Capability and Intent?
- What & where? - criteria for candidate Target Vectors at MMPT likely to meet Perpetrator goals
  - Perceived Vulnerability to Hazard
  - Perceived Utility to Perpetrator
    - Perceived potential Harm that can be wrought
    - Perceived Criticality
    - Perceived symbolic value to Perpetrator and to Target Audience
  - Provocativeness to Perpetrator
  - Perceived Presence in Situation - Exposure to attack
  - Potential for delivering:
    - Message to Target Audience
    - Wider operational benefit to Perpetrators
- When? - possible Timing of attack - Perpetrator-considerations eg a significant anniversary
- How likely? - likelihood of attack being attempted
  - Relating to each of the Attack Procedure steps up to and including the main attack, and the interdependency between them
    - Research/ planning
    - Preparation including reconnaissance
    - Dry run or main attack
- How severe? - potential Harm Perpetrators seek to wreak
  - Consequences of successful - or failed - attack
    - Evaluating core functions of MMPT and economic/ social assets it contains
    - Estimation of impact of loss of or damage to these assets
      - Criticality
        - COUNTERACT methodology - construction of operational diagram detailing all infrastructures, critical assets and dependencies between them
        - How essential the physical or cyber-based system is to the minimum operations of the economy and government
        - Severity of impact on security, public health and safety of the incapacitation or destruction of systems and assets
        - Availability of alternative or substitute/ replacement
        - Time needed to restore facility to normal function
      - Non-critical harms eg to people, business
      - Harm during, immediately after, over longer-term after attack
- How big? - possible Scale of attack
- How clear? - depends on:
  - Actual development of Perpetrators' plans and progression of actions - Scope is generic at early stages of Attack Procedure, becoming ever more specific as Perpetrator research/ planning proceed, problems are solved, preparations made and opportunities constructed
  - Quality/quantity of Intelligence on Perpetrator planning and actions

From Intelligence sources plus network and site-specific info

Intelligence – Threat + opportunity – > pattern of risk



Intelligence

Begin detailed security planning, design & implementation process here

How is the security action initiated?

What is the scope of the Threat?

What is the likely pattern of Risk of attack incidents?

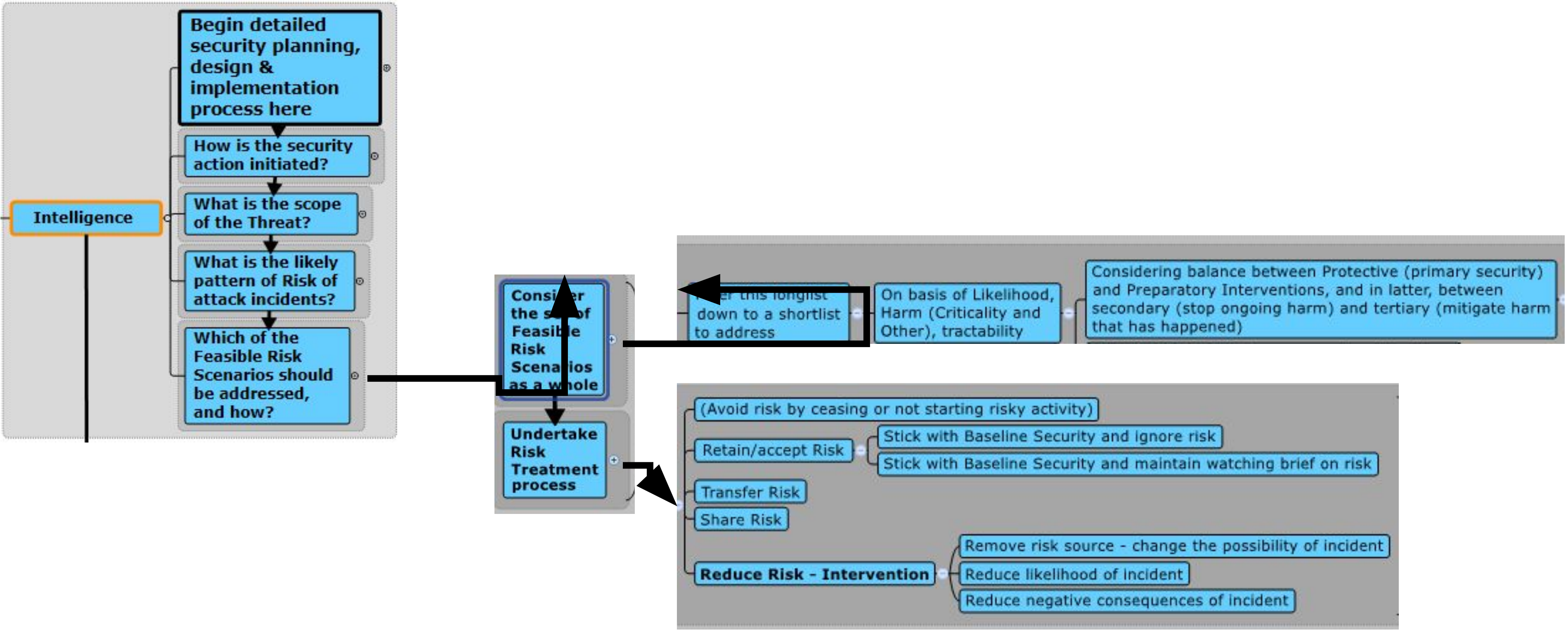
Which of the Feasible Risk Scenarios should be addressed, and how?

Consider the Threat (depending on the info available - its specificity, reliability, which stages of the Attack Procedure it covers)

Match each Attack Threat Scenario, step-by-step with the relevant Opportunity factors in the MMPT Situation

Then, for each such pairing, consider How well the Threat, and the Opportunity to realise it, match up

Intelligence – Which risk scenarios to address, how?



Intelligence

Begin detailed security planning, design & implementation process here

How is the security action initiated?

What is the scope of the Threat?

What is the likely pattern of Risk of attack incidents?

Which of the Feasible Risk Scenarios should be addressed, and how?

Consider the set of Feasible Risk Scenarios as a whole

Filter this longlist down to a shortlist to address

On basis of Likelihood, Harm (Criticality and Other), tractability

Considering balance between Protective (primary security) and Preparatory Interventions, and in latter, between secondary (stop ongoing harm) and tertiary (mitigate harm that has happened)

Undertake Risk Treatment process

(Avoid risk by ceasing or not starting risky activity)

Retain/accept Risk

- Stick with Baseline Security and ignore risk
- Stick with Baseline Security and maintain watching brief on risk

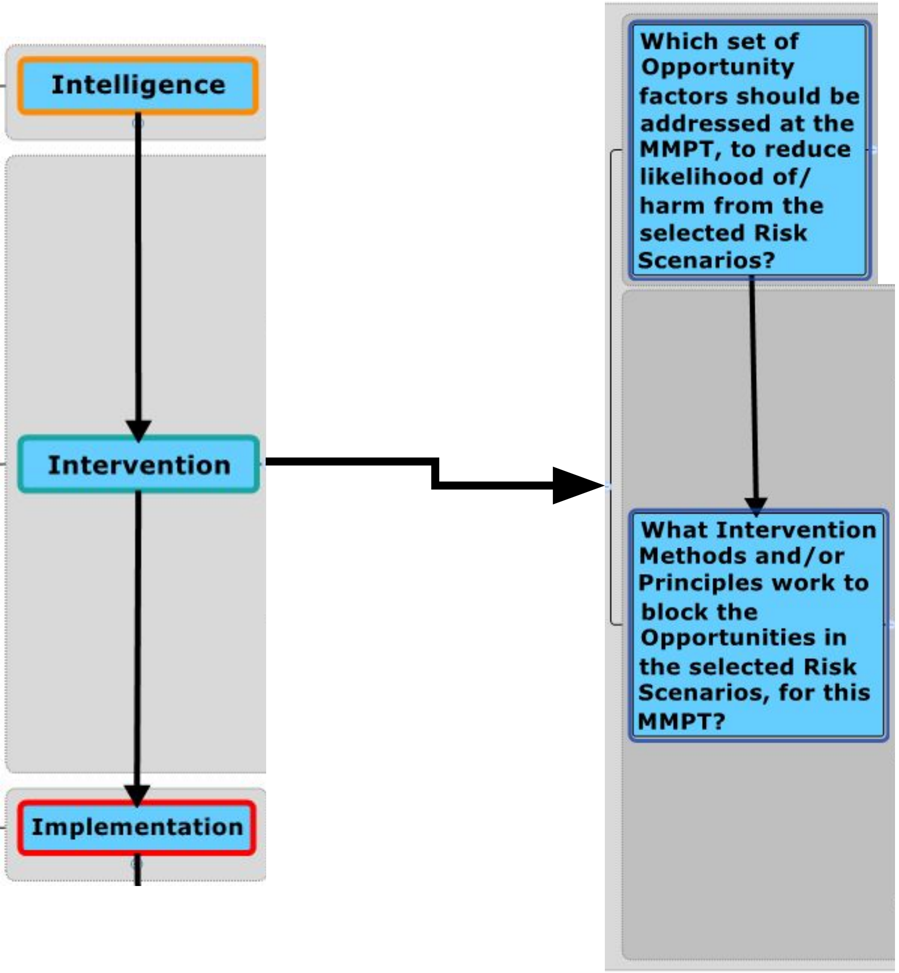
Transfer Risk

Share Risk

Reduce Risk - Intervention

- Remove risk source - change the possibility of incident
- Reduce likelihood of incident
- Reduce negative consequences of incident

Intervention – blocking, deterring, thwarting attack



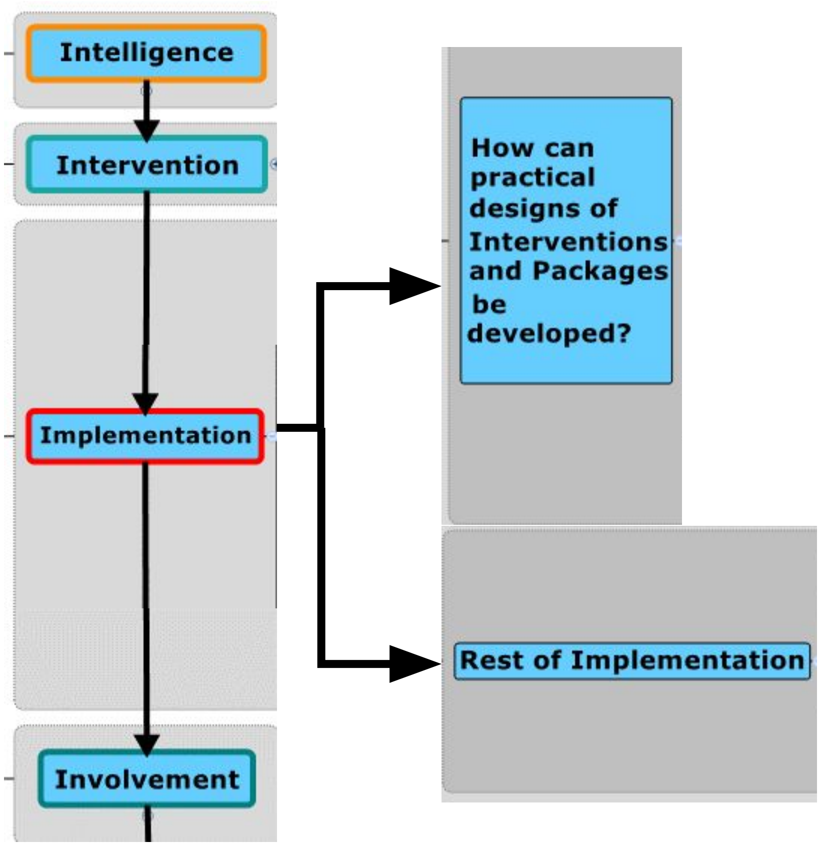
Intelligence

Intervention

Implementation

Which set of Opportunity factors should be addressed at the MMPT, to reduce likelihood of/ harm from the selected Risk Scenarios?

What Intervention Methods and/or Principles work to block the Opportunities in the selected Risk Scenarios, for this MMPT?



Intelligence

Intervention

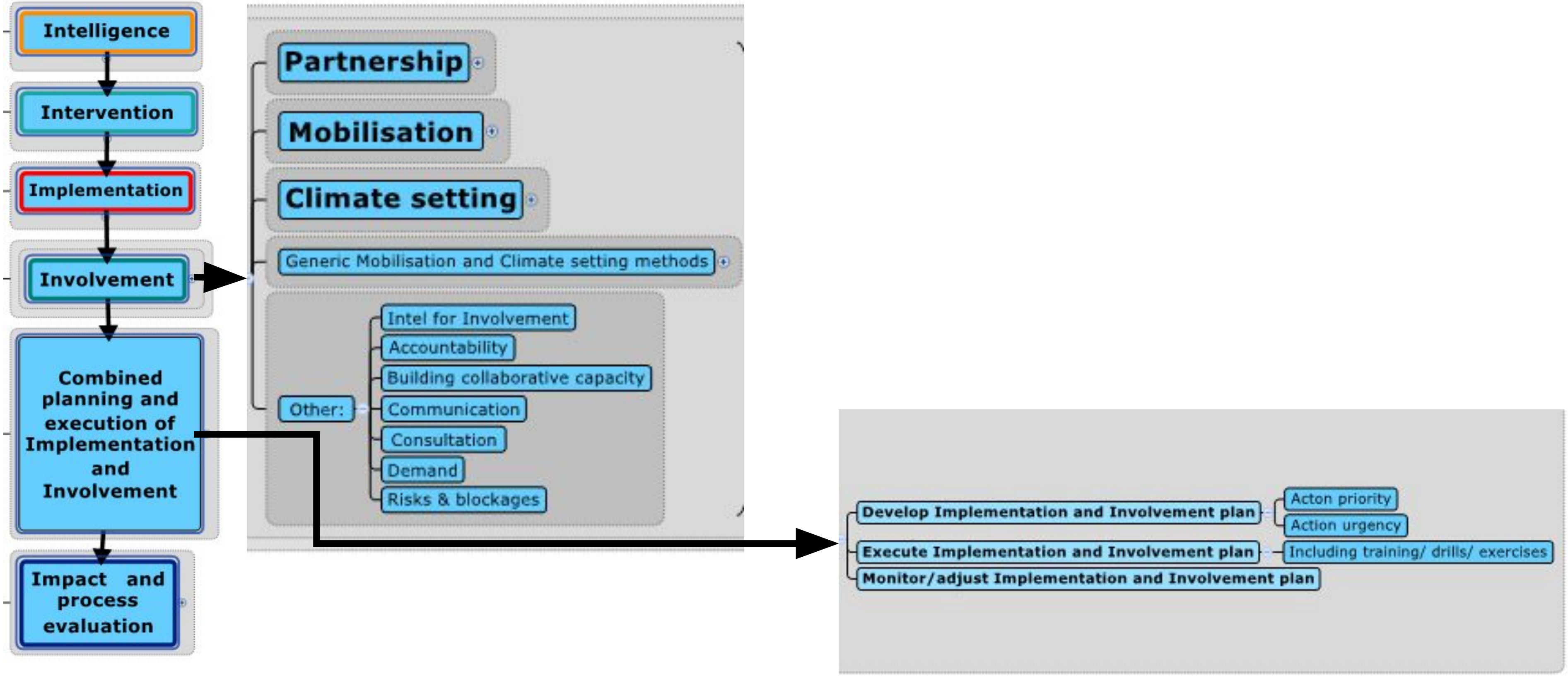
Implementation

Involvement

How can practical designs of Interventions and Packages be developed?

Rest of Implementation

Involvement – People and organisation dimension



Intelligence

Intervention

Implementation

Involvement

Combined planning and execution of Implementation and Involvement

Impact and process evaluation

Partnership

Mobilisation

Climate setting

Generic Mobilisation and Climate setting methods

Other:

- Intel for Involvement
- Accountability
- Building collaborative capacity
- Communication
- Consultation
- Demand
- Risks & blockages

Develop Implementation and Involvement plan

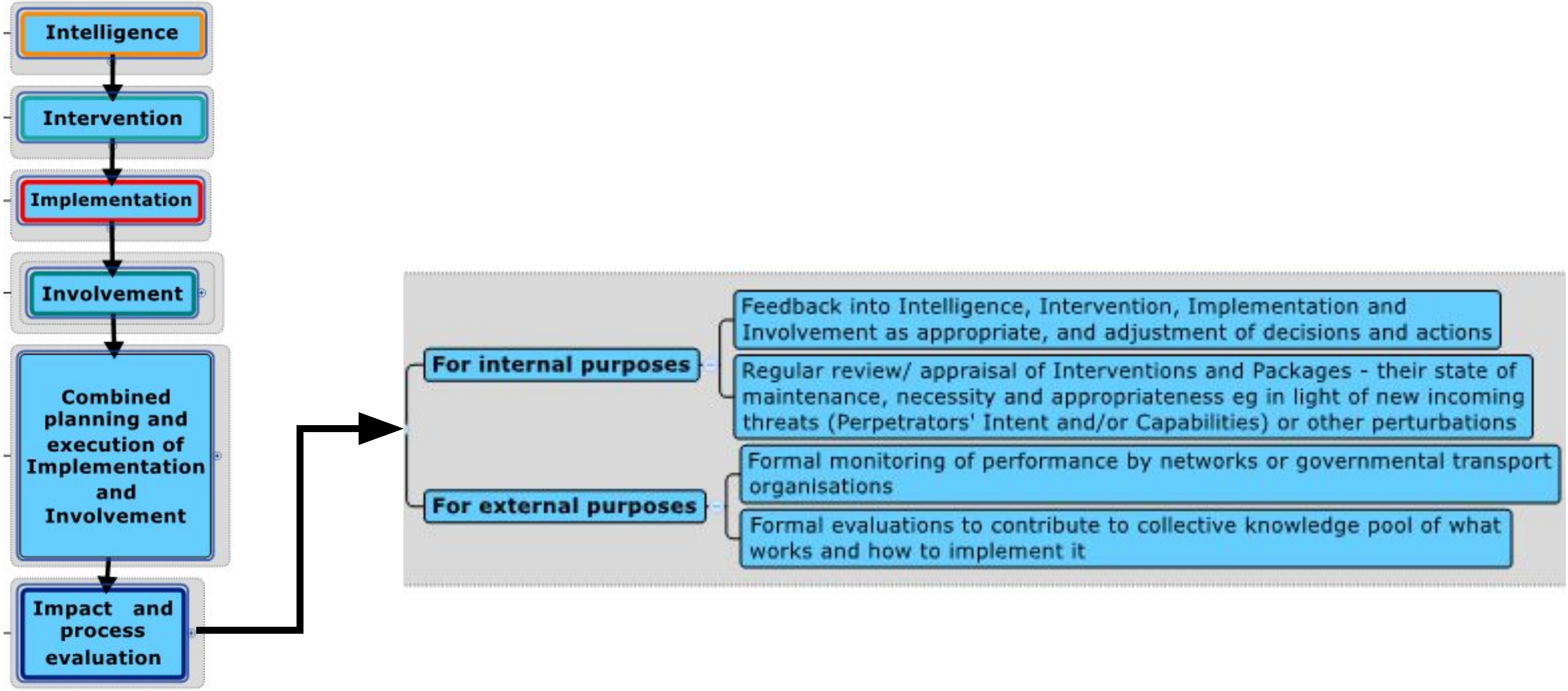
- Acton priority
- Action urgency

Execute Implementation and Involvement plan

- Including training/ drills/ exercises

Monitor/adjust Implementation and Involvement plan

Impact and process evaluation



Intelligence

Intervention

Implementation

Involvement

Combined planning and execution of Implementation and Involvement

Impact and process evaluation

For internal purposes

- Feedback into Intelligence, Intervention, Implementation and Involvement as appropriate, and adjustment of decisions and actions
- Regular review/ appraisal of Interventions and Packages - their state of maintenance, necessity and appropriateness eg in light of new incoming threats (Perpetrators' Intent and/or Capabilities) or other perturbations

For external purposes

- Formal monitoring of performance by networks or governmental transport organisations
- Formal evaluations to contribute to collective knowledge pool of what works and how to implement it

Future Steps: Objectives

University of HUDDERSFIELD

- To develop toolkit (or similar for end users) that can
  - capture practice-relevant knowledge on security approaches
  - organise it for efficient storage and retrieval
  - disseminate it
  - engage and educate end users in how to apply it
  - facilitate implementation and involvement (organisational design)

- More widely, to encourage and assist:
  - Proportionality of intervention relative to risk
  - Customisation of security action to context
  - Adaptability to changes in technology, business and society
  - Evaluation of practices
  - Continued updating, growth, and adaptability of toolkit itself

Future Steps: Alternative Formats

University of HUDDERSFIELD

- Simple pdf guide with clickable tabs

- Interactive pdf worksheet
  - Users work through with guidance at each step

- Highly interactive html website
  - diverse users and diverse starting points
  - e.g. strategic>tactical; experienced>novice user)
  - leading them through the complexity of the task
  - customised to their needs, priorities, skill level and resources

- Table-top games for training and rehearsing for alternative scenarios

Future Steps: Common Approach

University of HUDDERSFIELD

- A process which empowers users to:
  - Think perpetrator, and threat
  - Think opportunity for terrorism/crime, generated by the design and operation of the MMPT
  - Think preventer, and security needs
  - Think designer, and the wider requirements for the business, the users and society
  - Think manager
  - Think future – resilience and adaptability in the long term