



**AUSTRALIAN
CRIMINAL
INTELLIGENCE
COMMISSION**



Australian Government

Australian Institute of Criminology

Understanding and Reducing the Risk of Terrorist Attacks at Passenger Terminals: Workshop Introduction

**Paul Ekblom
University of Huddersfield**

November 2016

Paul Ekblom

Applied Criminology Centre,
University of Huddersfield, UK
p.ekblom2@hud.ac.uk

Full project team: Alex Hirschfield (project leader), Rachel Armitage, Kris Christmann, Paul Ekblom, Steve Lui, Leanne Monchuk, Andrew Newton and Michelle Rogerson

What's coming up

1. Introduction
 - Background to the PReEMPT Project – what works against terrorist attacks in complex stations
 - The shortfall of evidence of what works
 - Methods – introducing the Conceptual Attack Framework
 - Illustrations from the Fieldwork
 - Handling the evidence – rating quality of evidence, quality of practice, organising the findings
 - Introducing the toolkit
2. Understanding threat
 - Basic CAF model – threat, risk, opportunity, security
 - Classification of terrorists' tactical attack methods
 - Attack procedure – the stages of planning and execution

3. Reducing risk
 - Security action framework and findings – a process-based, detailed characterisation of Protective and Preparatory action to reduce risk of attacks
 - Putting security action together in practice – outline of a toolkit
4. Policy issues and future work

Process Review and Evaluation of Multi-Modal Passenger Terminal Security

For EU DG Mobility and Transport

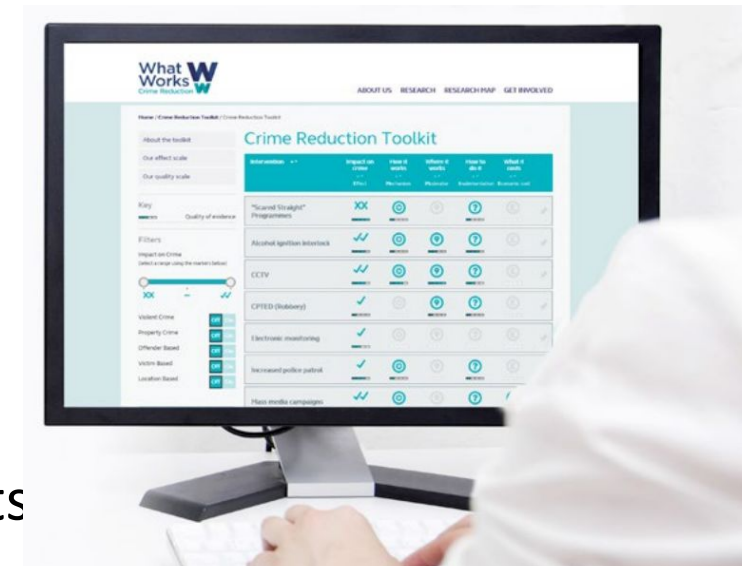
- **To understand** how MMPTs operate and tactical security challenges they face
- **To identify** 'best practice' solutions to secure MMPTs from terrorist attacks and serious crime
- **To produce** an indicative toolkit
- **To inform** the development of a pan EU Land Transportation Security Strategy

How to identify What Works?

- Originally EU asked us for **meta-analysis** of evaluation literature
- But we had read Lum's (2005-9) systematic review of CT evidence
 - Scanned some **20000 studies** representing **billions of \$£€**
 - Only **7** passed a 'relaxed' methodological quality filter
 - These were **very general** and **not necessarily relevant to land transport MMPTs** – e.g. 'screening of passengers at airports is cost-effective'
- And we know that evaluating impact of interventions on **very rare events** is very difficult
 - RCT and quasi-experimental designs impossible

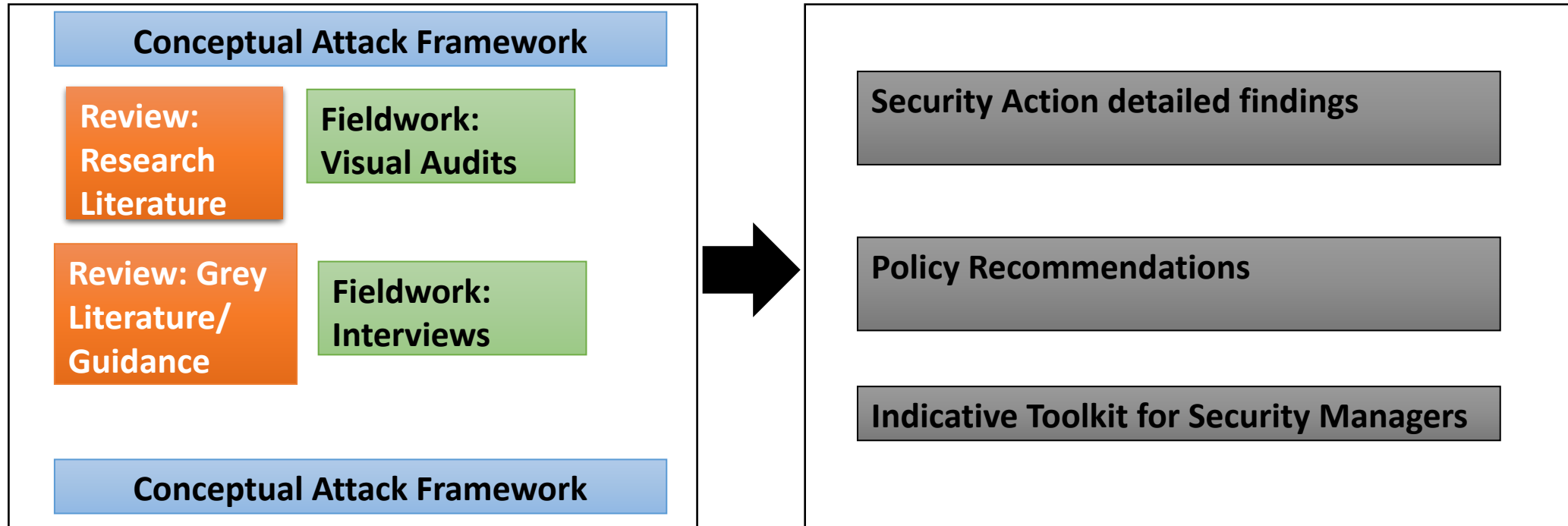
What to do instead of conventional Systematic Review?

- So a conventional meta-analysis not feasible
- Nor can 'EMMIE'-type guidance (Systematic+Realist Review) be produced in same way
 - Effect – the impact on crime
 - Mechanism – how it works
 - Moderators – where it works best
 - Implementation – how to do it
 - Economic assessment – what it costs
- But practitioners and policymakers ASAP!
- How then to make the best of what knowledge exists
- Developed an alternative approach based on Mixed Methods and a Scientific Realistic approach to knowledge – emphasis on **how it works, in what contexts**



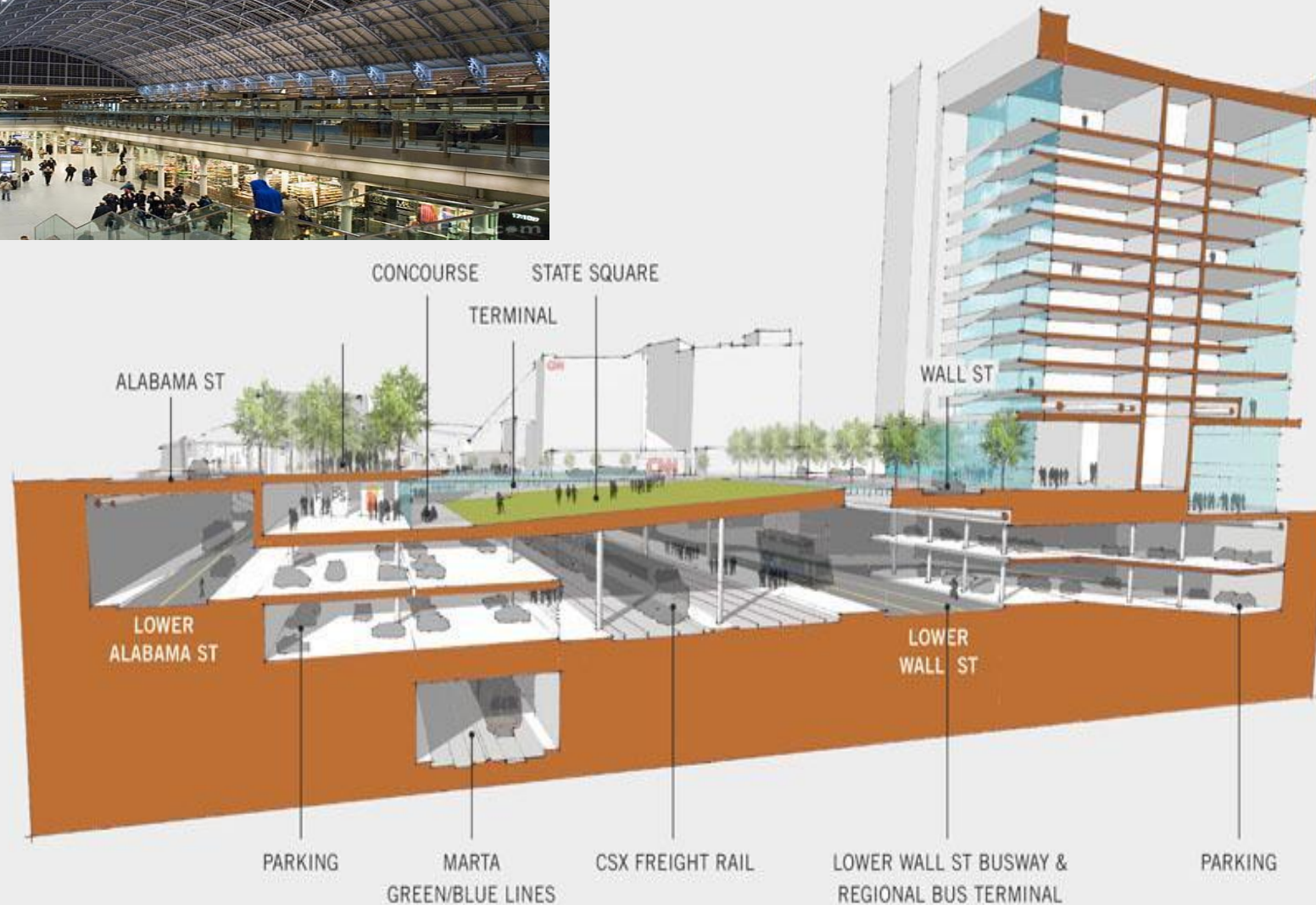
ce –

Mixed Methods Approach built around a Conceptual Attack Framework



- Conceptual Attack Framework (CAF) had to:
 - Handle complexity of MMPTs, and complexity/ diversity of terrorist attacks
 - Cope with huge variety of findings – nature, scope, level, quality, origin, format
 - Connect with theory & terminology in SCP, security
 - Prime the planning of Realist Literature Review and Fieldwork
 - Facilitate synthesis of results at strategic, operational and tactical levels
 - Feed into/ help to structure (eventual) practical toolkit, beginning with outline version

Complexity of MMPT



Transport, Infrastructure & Land Use	Integral/ Adjoining Retail/Leisure Facilities	What varies between MMPTs
<u>Transport Mode</u> Over-ground Rail Metro System Tram System Bus Station Taxi Rank <u>Infrastructure</u> 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

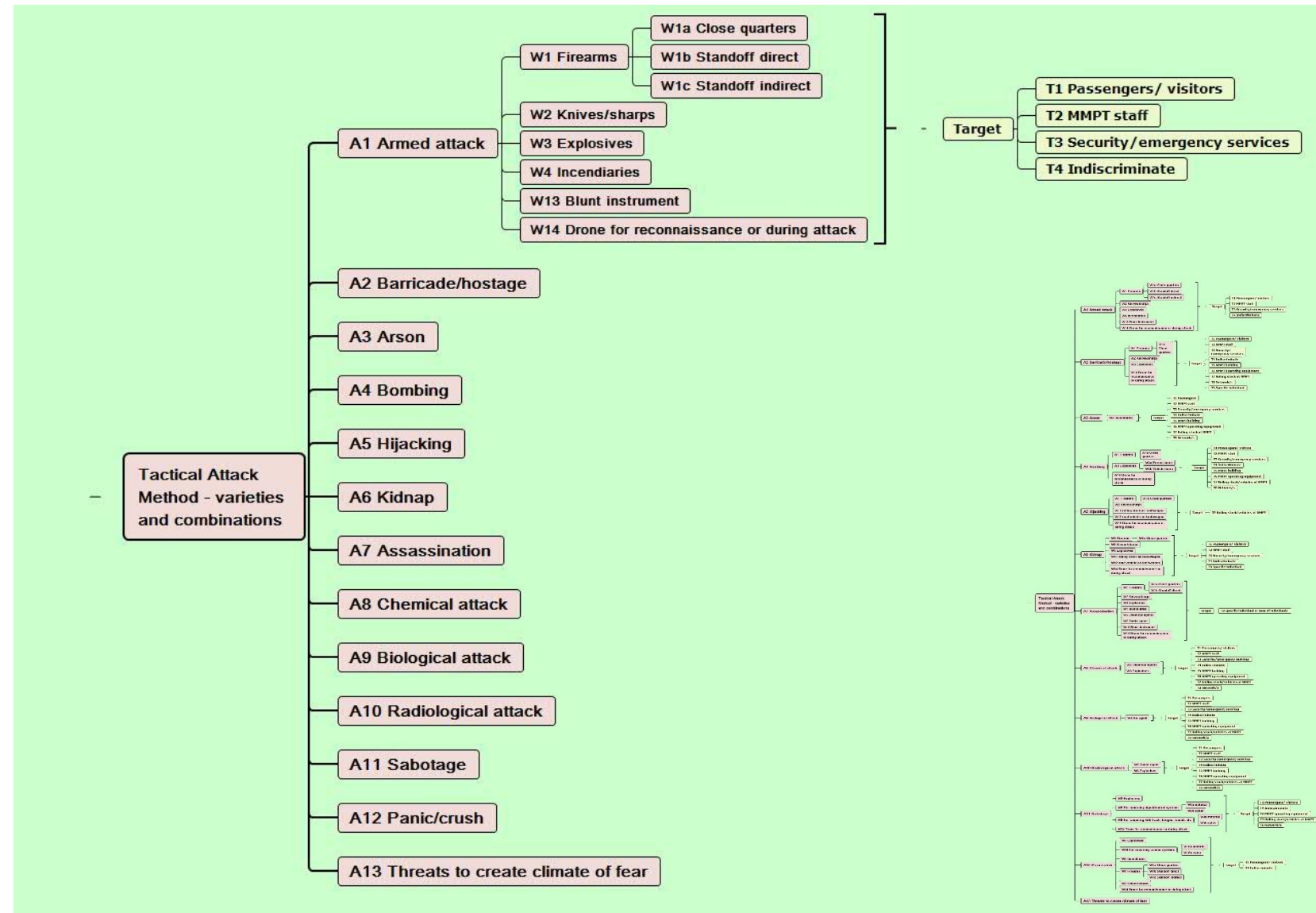
Diversity of attacks & interventions

- **Rand study of terrorist attacks** identified:
 - 13 attack **methods** (marauding, bombing, arson etc)
 - 14 **weapon** types (guns, bombs, chemicals etc)
- We identified 9 **target types** (passengers, security personnel, buildings etc)
- UK Police's **Project Griffin** identified 11 stages of generic **attack procedure**, each with a greater/lesser number of alternative script tracks
- We know from SCP that there are diverse **interventions**:
 - 25 Techniques, 5+ CPTED principles
 - 11 generic proximal causal factors for crime/terror events (Conjunction of Terrorist Opportunity)
 - 11 Ds – mechanisms by which to influence offenders...
- A helluva lot of permutations/combinations for practitioners!

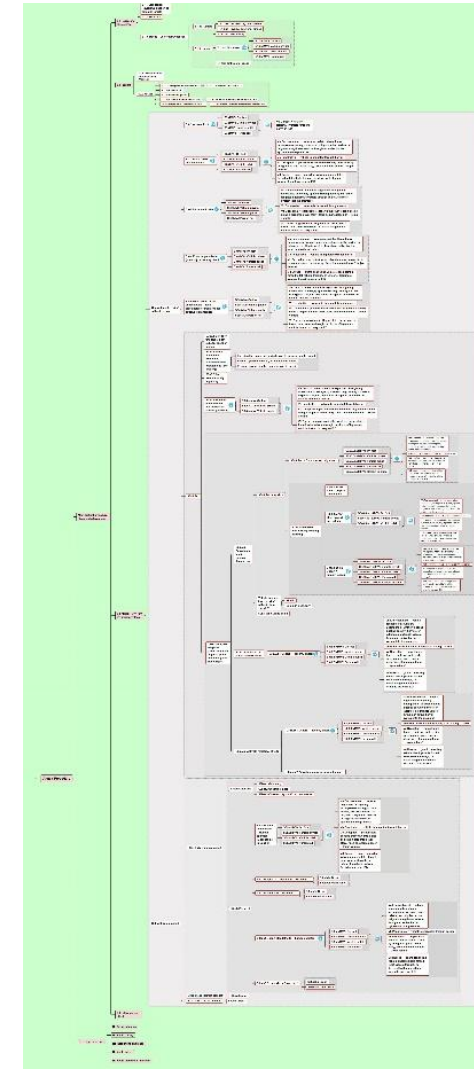
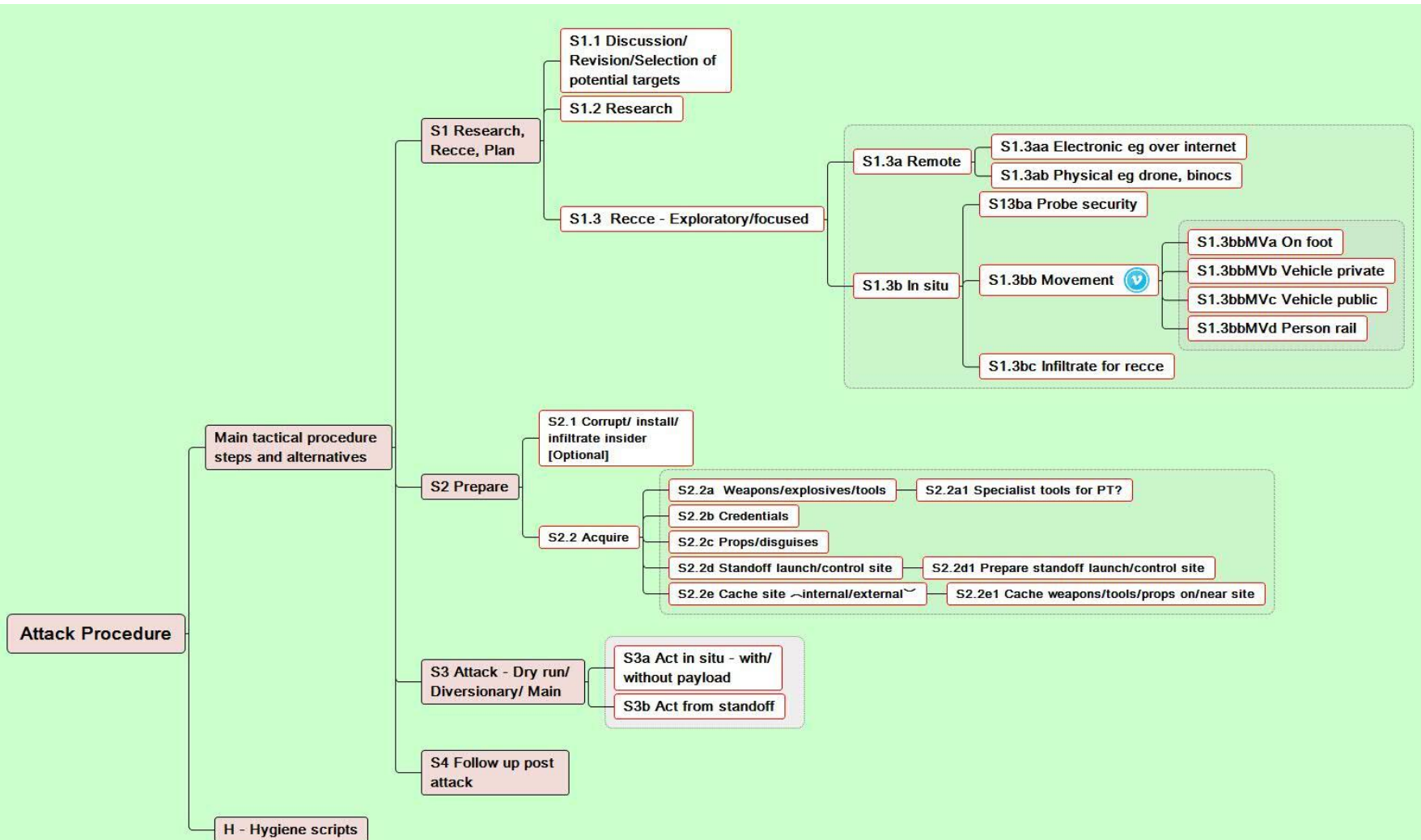
Conceptual Attack Framework

- Maps out theoretically plausible **attacks**
 - Attack **Methods** – **Weapons** – **Targets**
 - Attack **Procedures** (scripts)
- Maps out theoretically plausible **security responses**, based on
 - **Conjunction of Terrorist Opportunity** – covers 11 immediate causes of attack events, and interventions to block those causes
 - **5Is process model of doing security** – Intelligence, Intervention, Implementation, Involvement, Impact *[Nothing to do with the 5Is grouping!]*
 - Covers both **Prevention** (centred on opportunity reduction) and **Preparing for first response** *[As in UK CONTEST, prevention is here called **Protection**]*
- Takes detailed **findings** from literature and fieldwork
- Organises them on '**knowledge trees**'
 - Aids retrieval
 - Links with theory
 - Puts like with like
 - Identifies knowledge missing from literature and practitioner experience – 'for gaps you need maps'

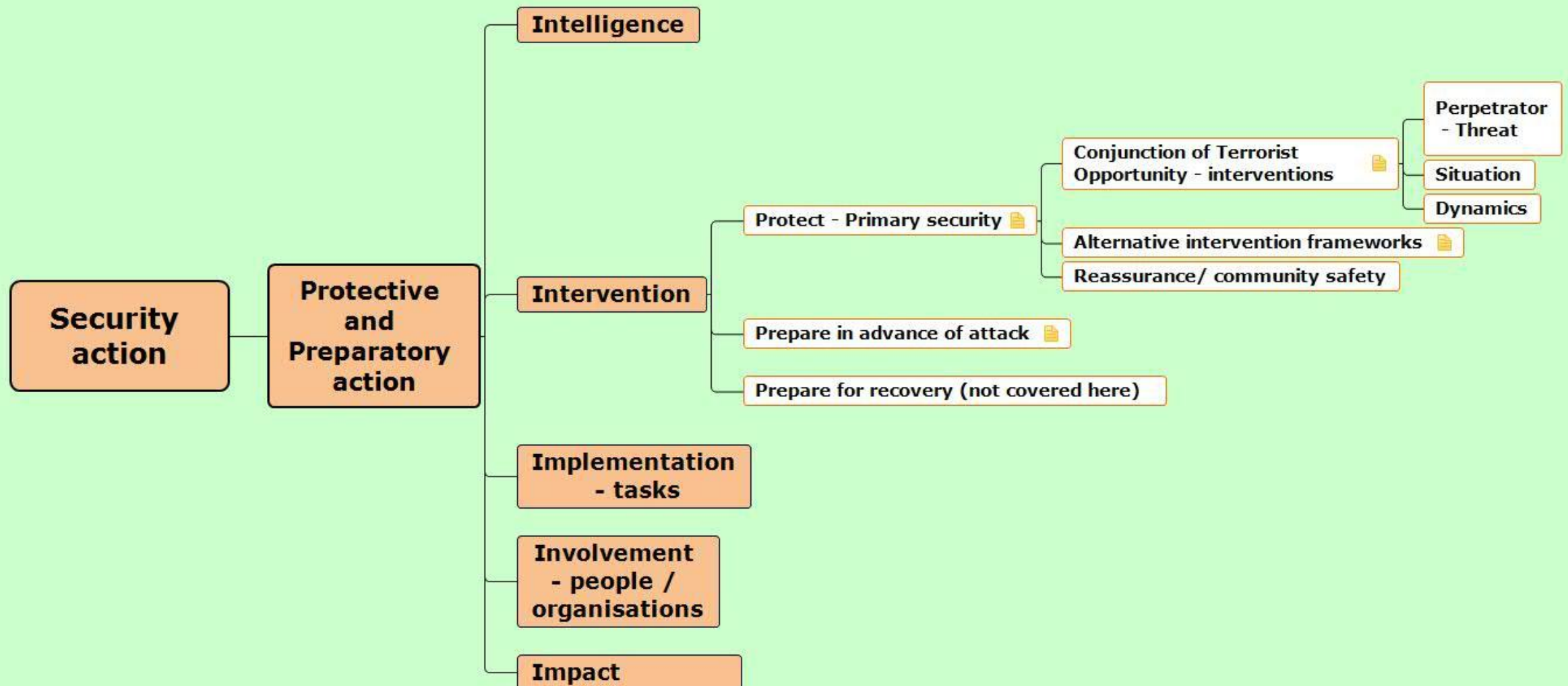
Conceptual Attack Framework – Tactical Attack Methods



Conceptual Attack Framework – Attack Procedures

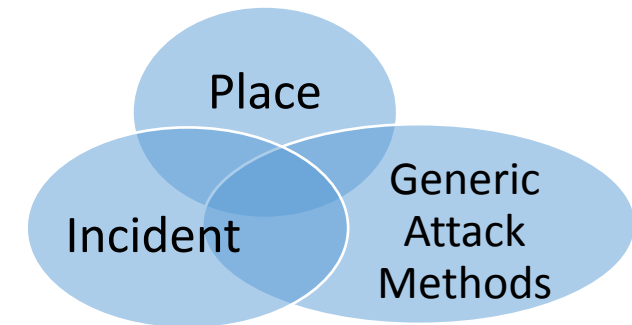


Conceptual Attack Framework – Security action based on 5Is



Research 1) Realist Literature Review

- Based on relevance and plausibility
 - Developing a synthesis of knowledge
 - Less concern with quantification, effect sizes and standardisation
 - More concern with theoretical plausibility, context
 - Include 'experience based knowledge'
- Searched 15 Bibliographic Data Bases
 - Keyword searches
- Approached relevant organisations and experts
- 409 relevant items identified (abstract/title)
 - 143 published/266 grey literature
- 139 documents reviewed in depth
 - Inclusion/Exclusion Criteria



Research 2) Fieldwork

- To experience contrasting MMPT environments
 - 4 stations in several EU countries
 - Interviews with police officers, counter-terrorism security advisers, other security personnel and site managers
- 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

Fieldwork slides thanks to Prof Rachel Armitage & Dr Lean



1. Surveillance & monitoring













2. Physical protection



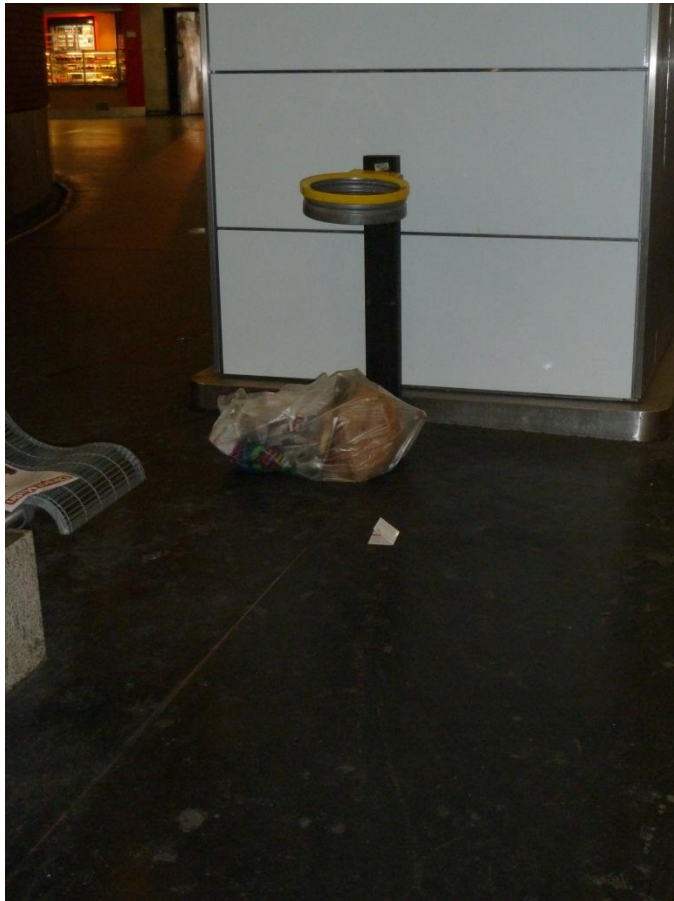


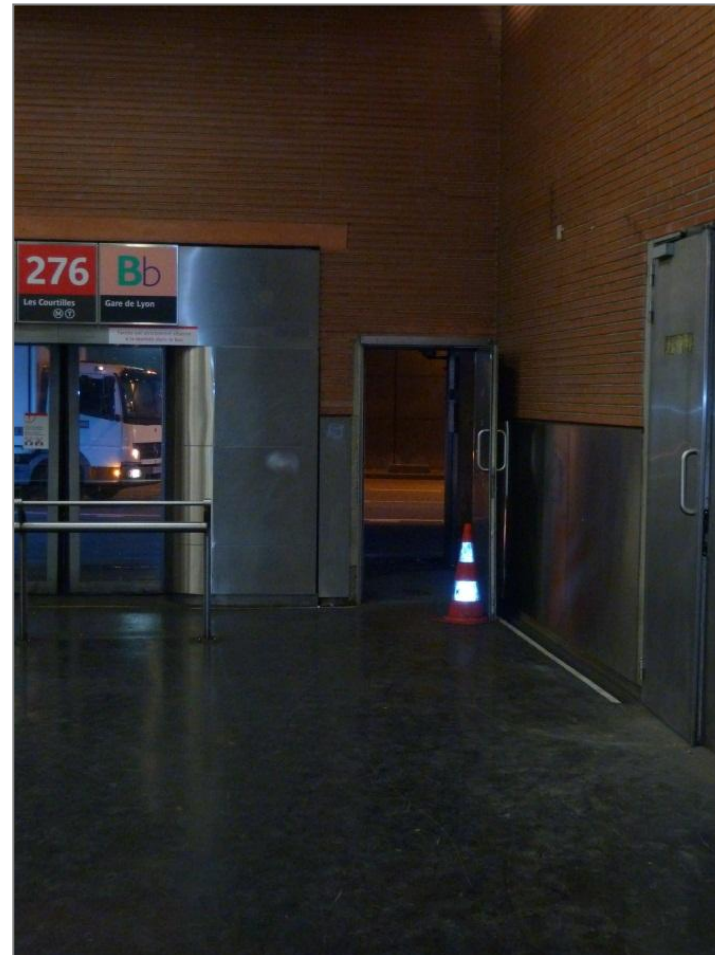
3. Movement control



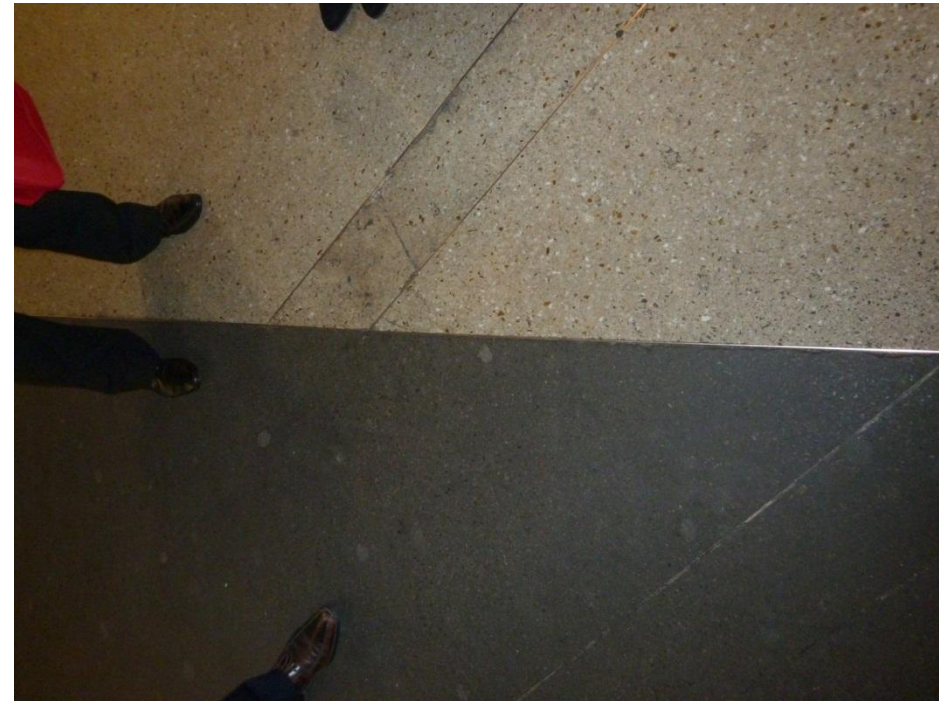


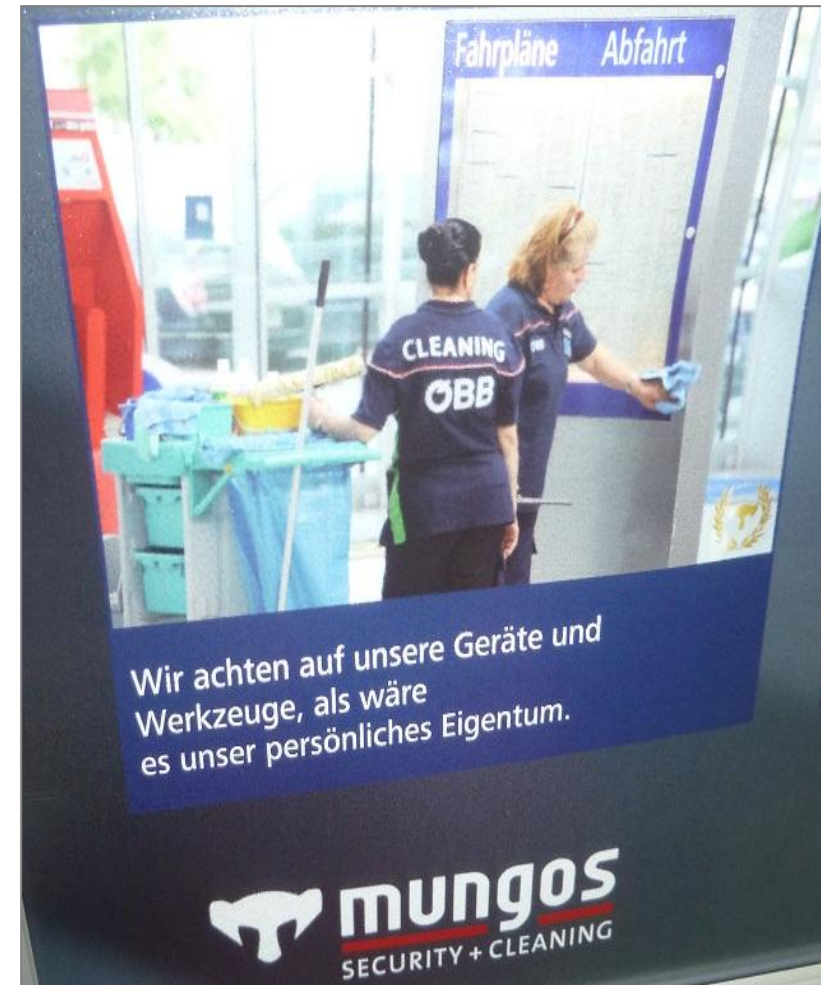
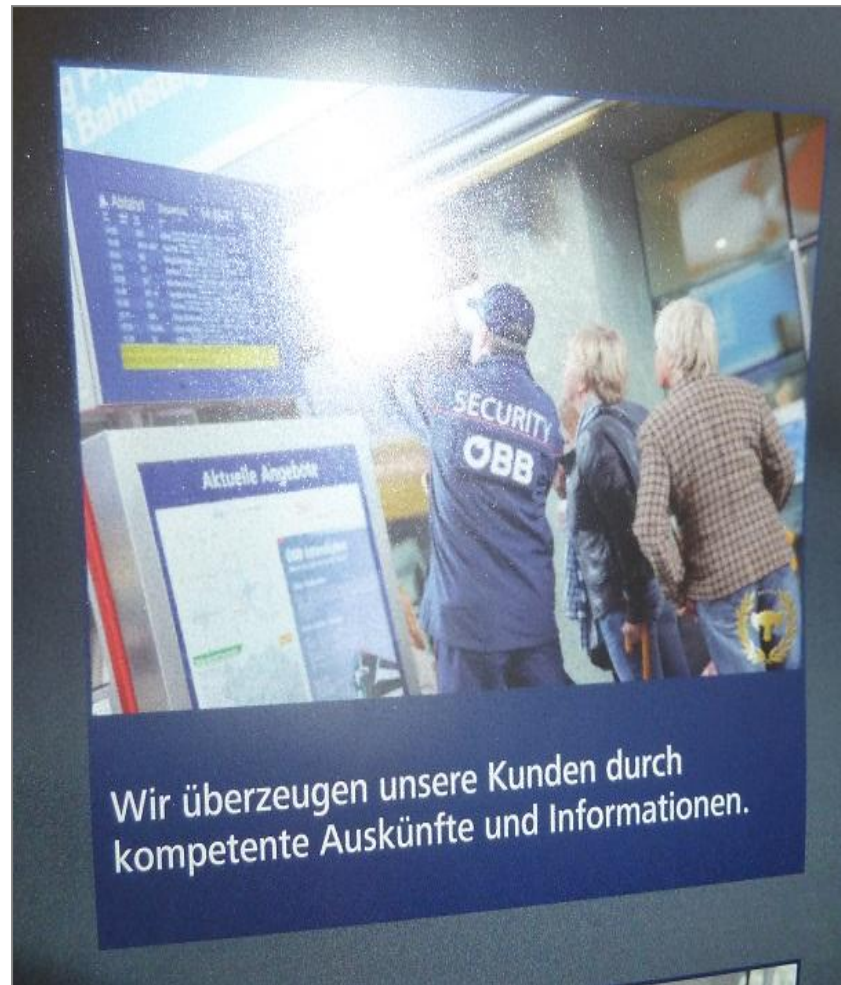
4. Management & maintenance



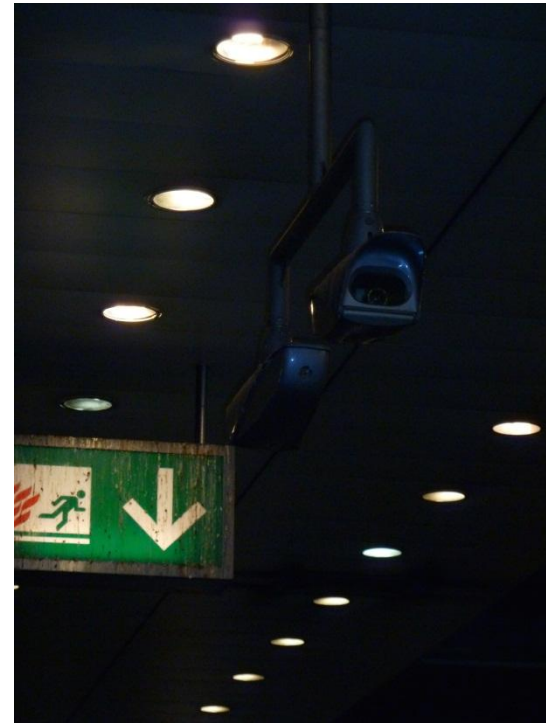


5. Governance

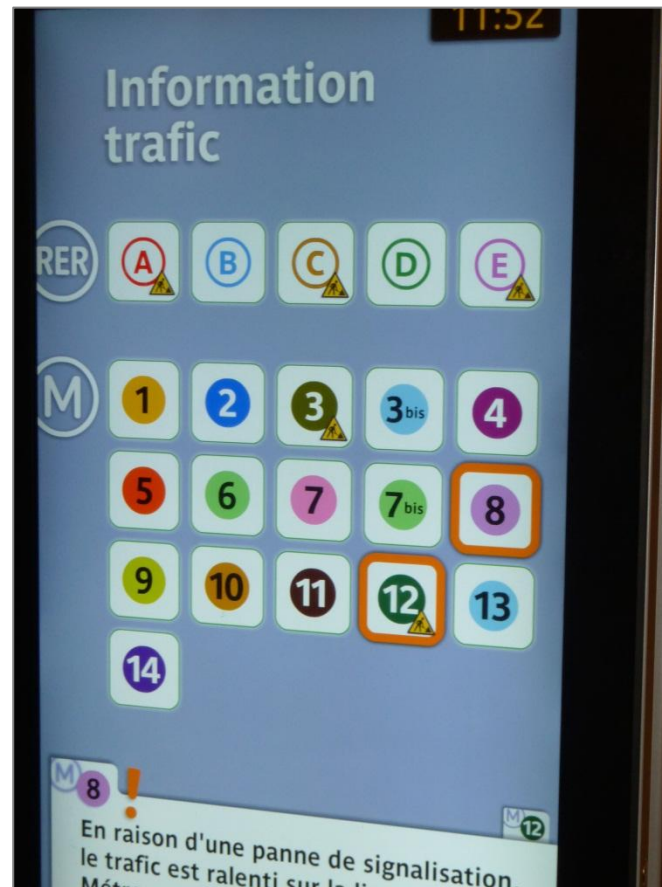




6. Emergency preparedness







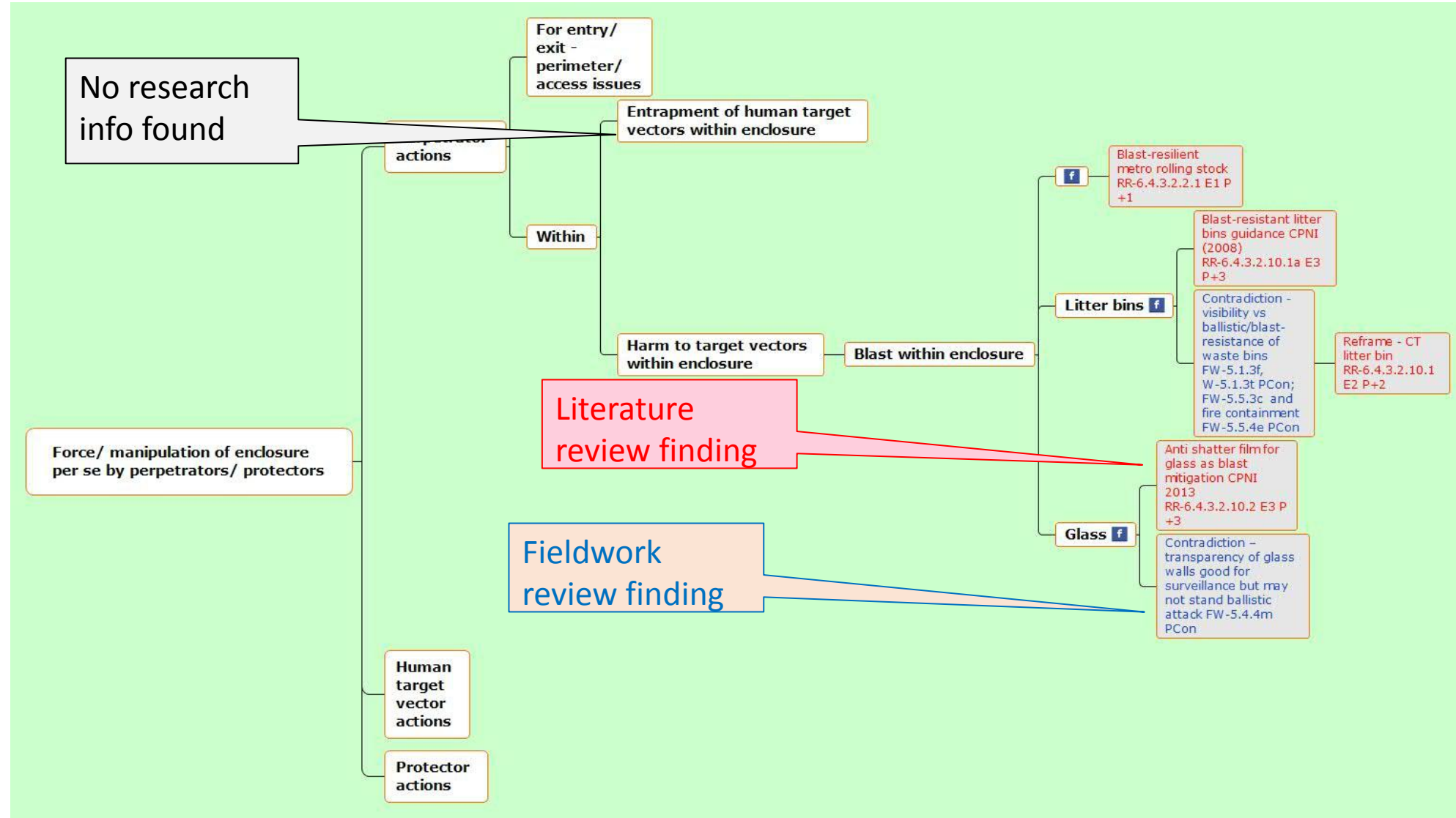
Evidence Quality Assessment – Literature

Evidence quality	Type of Evidence	Practice quality
E1	Experimental Comparative Designs	P+1 'Best Practice' – strong research evidence that the practice was effective in its implementation and impact and outperformed alternatives
E2	Experimental Observational and Simulation Designs	P+2 'Good Practice' – strong research evidence of effectiveness in implementation & impact, without comparative element; or moderate research evidence with/without comparison
E3	Expert Consensus	P+3 'Potentially Good Practice' – assessments of implementation and impact moderate to strong, with/without comparison but based on consensus of opinions from experts & respected authorities/ organisations rather than research
E4	Expert Opinion	P+4 'Highlighted Practice' – claimed as effective or ineffective in literature but without supporting evidence
E1,2,3		P- 'Practices to avoid' – literature suggests these not beneficial; and strong-moderate research evidence and/or a consensus of expert opinion to support this claim

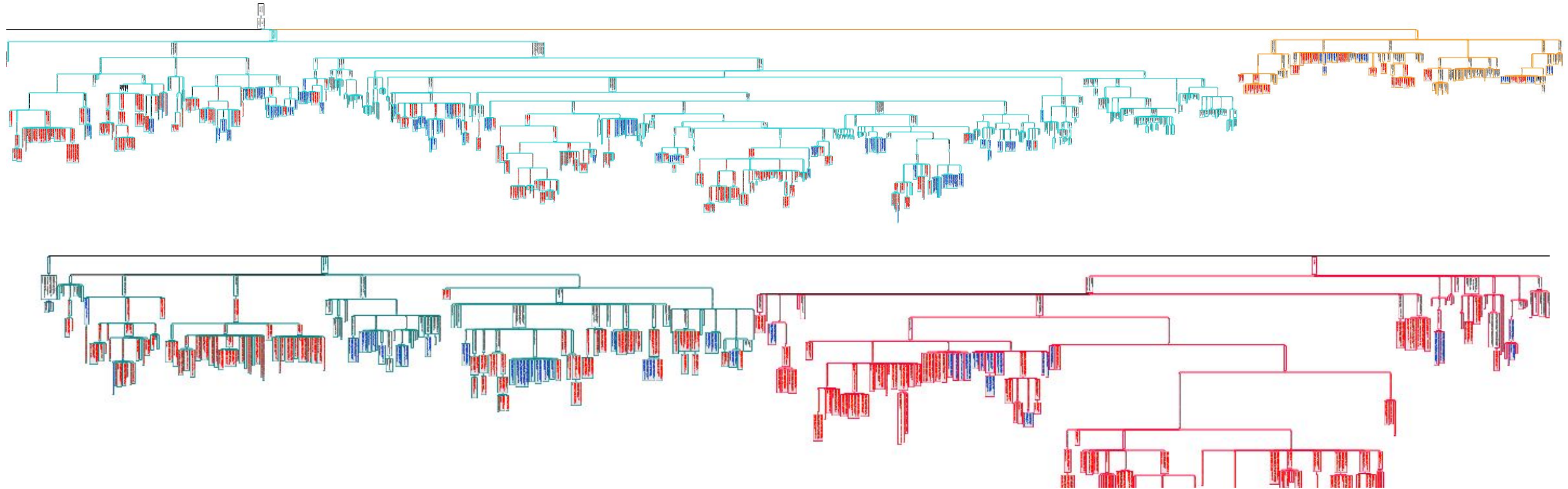
Evidence Quality Assessment – Fieldwork

Practice quality level		Description
P+	Recognised Good Practice	A practice judged to be good practice depending on context
P+/-	Practice positive/negative	A practice that may be good or that should be avoided depending on context
P0	Indeterminate practice	A practice where there is neutral or uncertain evidence to make a judgement either way
PCon	Contradictory Practice	Identification of a contradiction in the effects of the practice requiring resolution e.g. through re-design / modification
P-	Practices to avoid	Practices assessed as less than satisfactory (irrespective of context)

CAF: Consolidating Findings

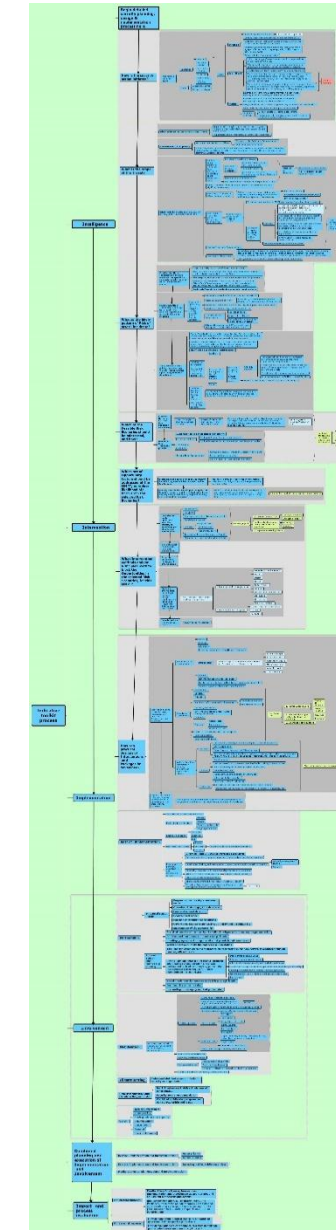
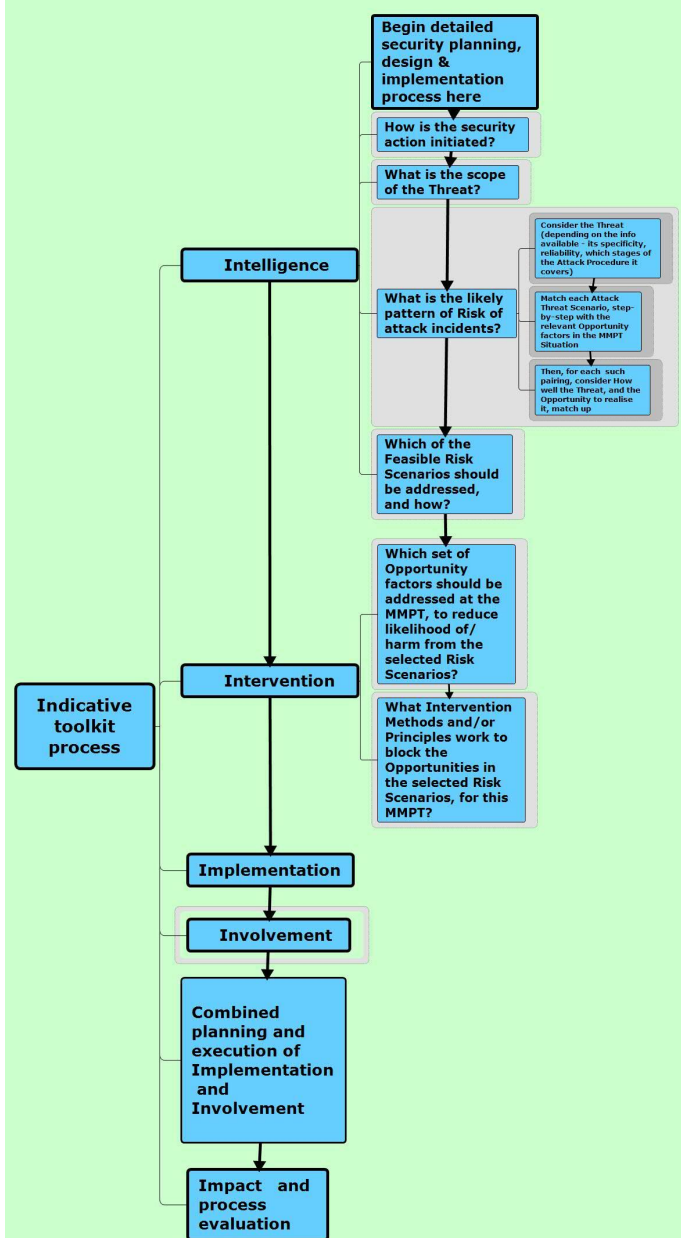


CAF: Entire Visual of findings – 130+ from **Fieldwork** and 200+ from **Realist Review**

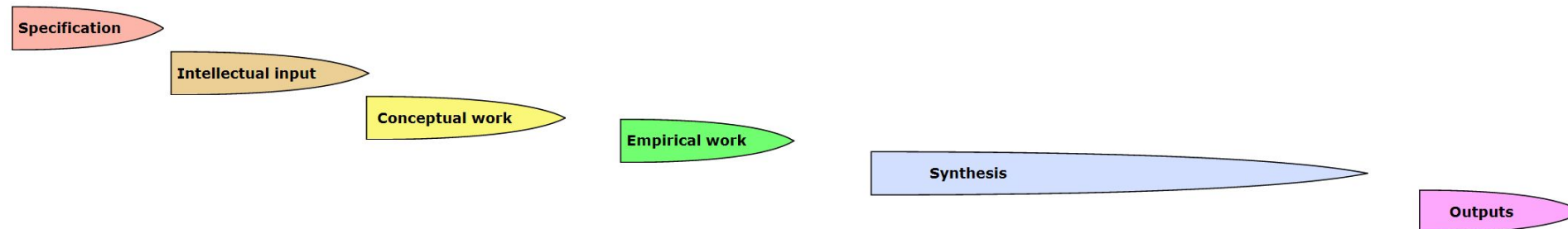


- A process which empowers users to:
 - Think perpetrator, and threat
 - Think opportunity for terrorism/crime, generated by the design and operation of the MMPT
 - Think security
 - Think designer, and the wider requirements for the business, the users and society
 - Think manager
 - Think future –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

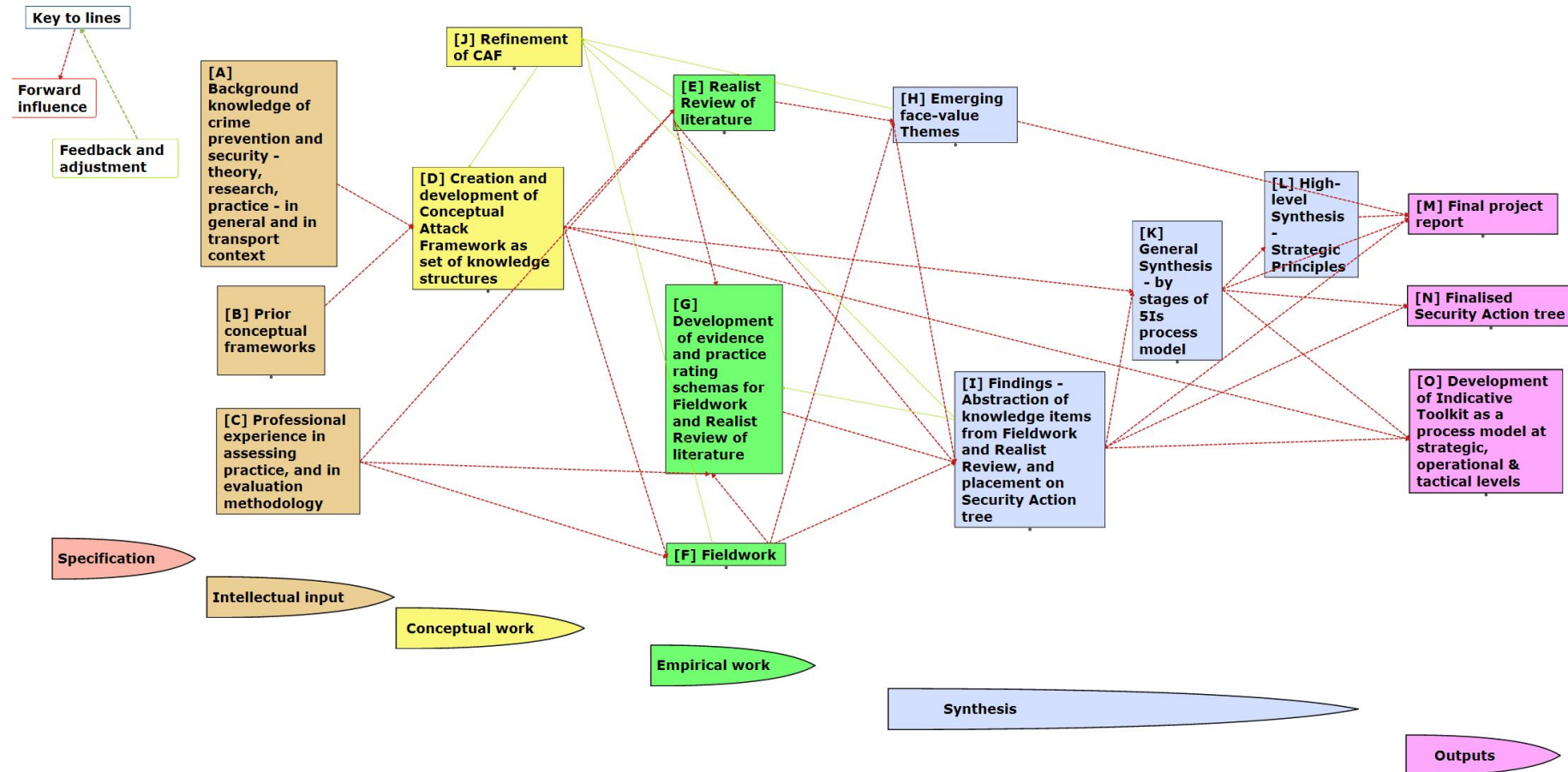
Indicative toolkit realisation



How it all fits together



How it all fits together





**AUSTRALIAN
CRIMINAL
INTELLIGENCE
COMMISSION**



Australian Government

Australian Institute of Criminology

Understanding and Reducing the Risk of Terrorist Attacks at Passenger Terminals: Workshop slides presenting the Conceptual Attack Framework

Paul Ekblom

University of Huddersfield

November 2016

Conceptual Attack Framework

CAF aims to provide a systematic, rigorous and theory-oriented way of:

- Understanding the **threat** from terrorism and serious crime
- Envisioning the **risk** which that threat generates in combination with **opportunity and motivational factors** in the immediate attack situation
- Supporting the development, design and deployment of existing and innovative **security** measures addressing those situational factors, to **protect** (reducing the likelihood of attack incidents) and **prepare** (mitigating immediate and consequential harm should those incidents occur)
- Helping to out-innovate adaptive offenders in the crime/security arms race

CAF aims to be

- Systematic, rigorous, and theory-oriented
- Complementary to empirical 'what works' approaches, but capable of offering useful and plausible guidance to policy and practice in the many cases where reliable evaluative knowledge does not exist
- An enabler of practical thinking, communication and knowledge exchange through the clear articulation of problems, causes and solutions

CAF was developed from the **Conjunction of Terrorist Opportunity** framework and its more generic forbear, the **Conjunction of Criminal Opportunity**

Also the **5Is** process model of doing crime prevention and security

The detail of CAF: Understanding Threat, Reducing Risk

Coming up:

1. Understanding threat

- Basic CAF model – **threat, risk, opportunity, security**
- Classification of terrorists' **tactical attack methods**
- **Attack procedure** – the stages of planning and execution

2. Reducing risk

- **Security action framework** and findings – a process-based, detailed characterisation of Protective and Preparatory action to reduce risk of attacks
- Putting security action together in practice – outline of a **toolkit**

Target Audience – the individuals, groups or institutions which are intended to be influenced by the attack, for example the government, a community or a private company

Target Vector – the person or assets that are harmed in order to deliver the terrorist message or deliver an operational gain to the Perpetrator

**Target
vector**

Target Audience

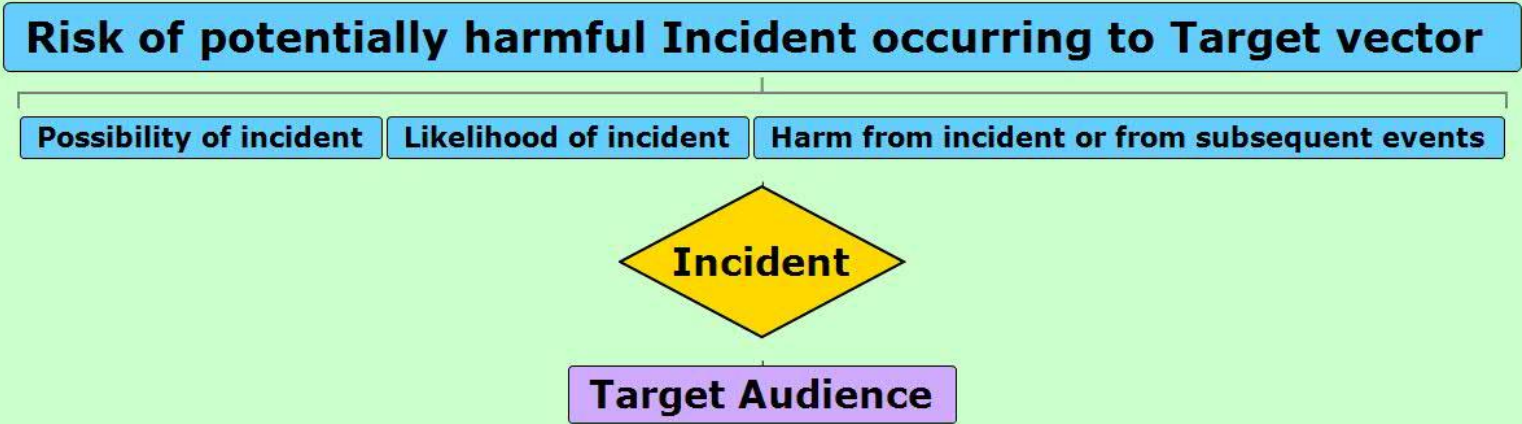
**Target
vector**



Target Audience

The **Risk** of the incident occurring to the Target vector has three aspects

**Target
vector**



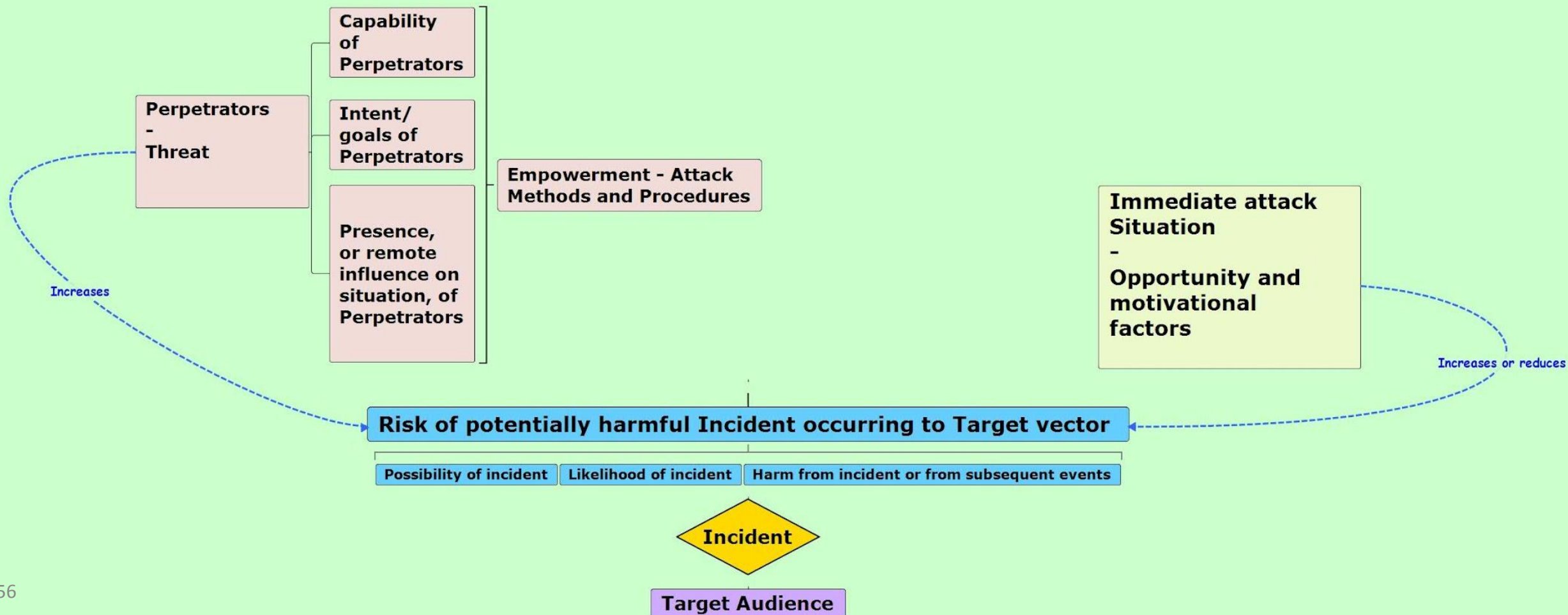
The **Threat** from Perpetrators combines with **Opportunity** factors in the Immediate attack Situation, to generate the **Risk** of terrorist or crime Incidents directed against the Target vector



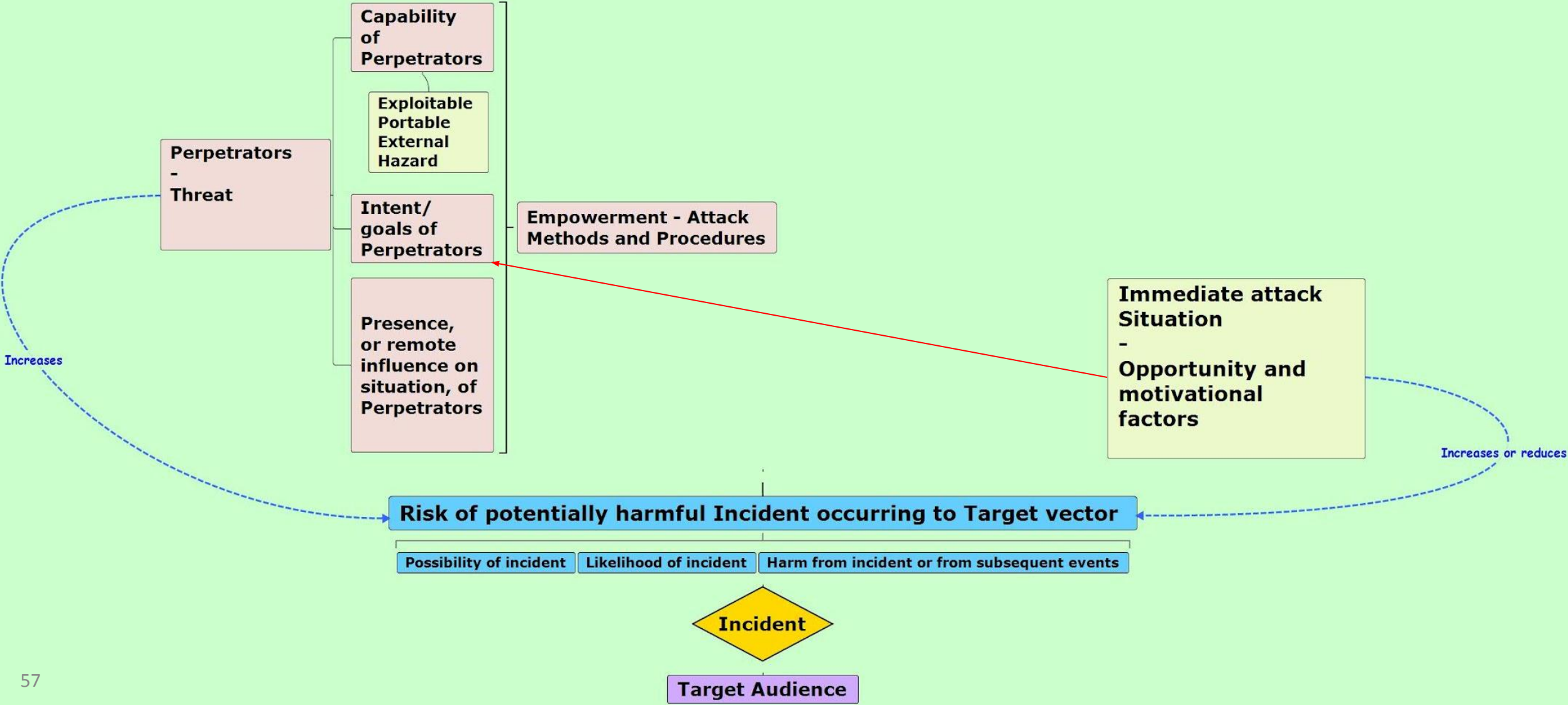
The Threat from Perpetrators comprises their

- Capability
- Intent and Goals
- Presence which could be physically in the Situation, or with remote access and influence on it, including via the Internet, or drones

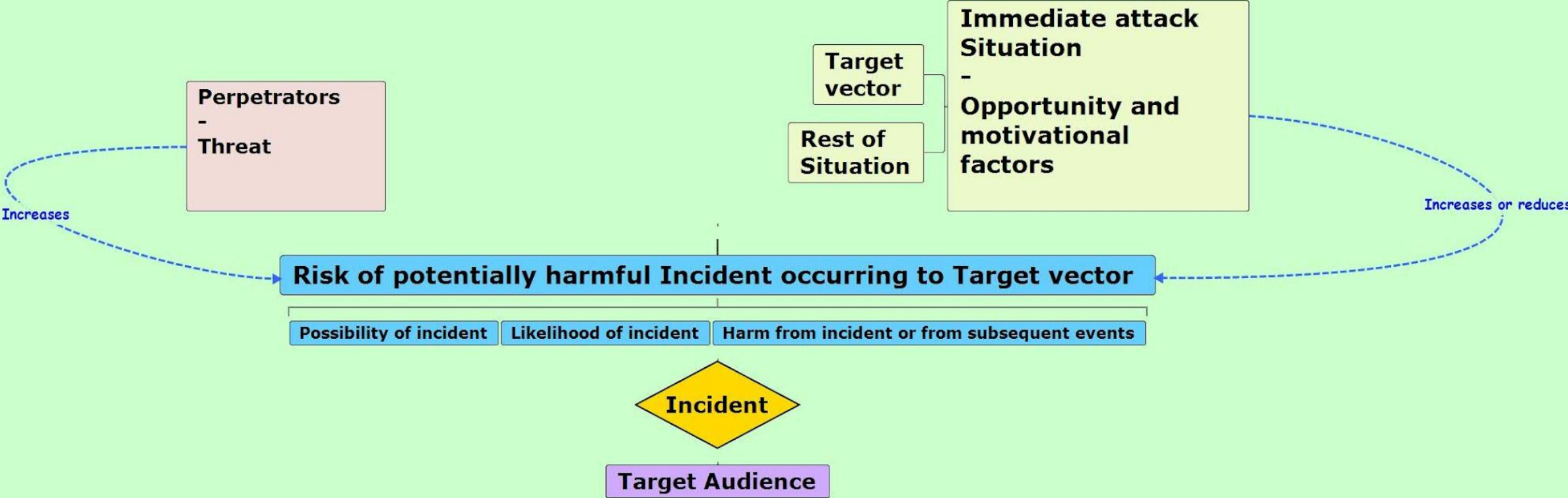
Together these empower them to deliver a range of attack methods and follow a range of attack procedures



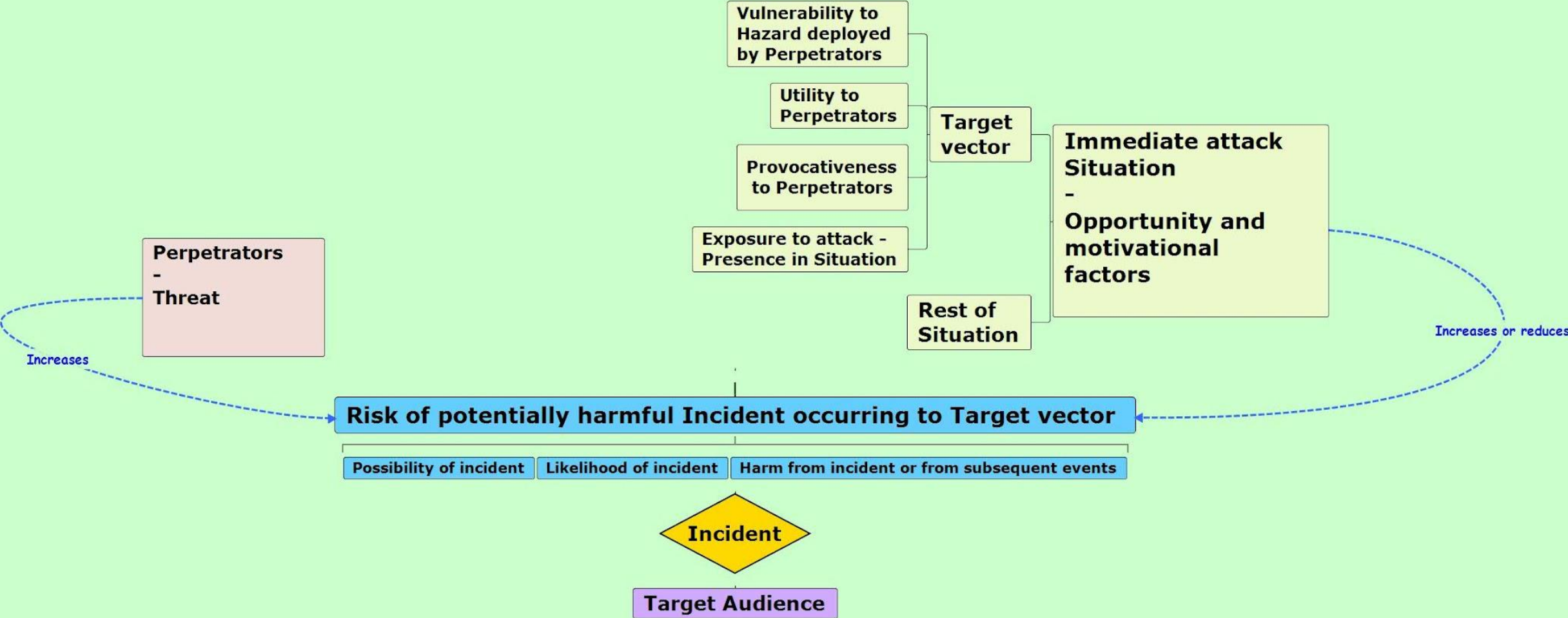
On the **Situational** side the environment supplies not only various Opportunity factors, but also **motivating** influences on the Perpetrators such as ‘provocations’, and Exploitable portable external hazards that they can bring in such as fuel tankers



We can divide the Situational influences into those relating to the Target vector (people, assets or network the Perpetrators wish to attack) and the remainder

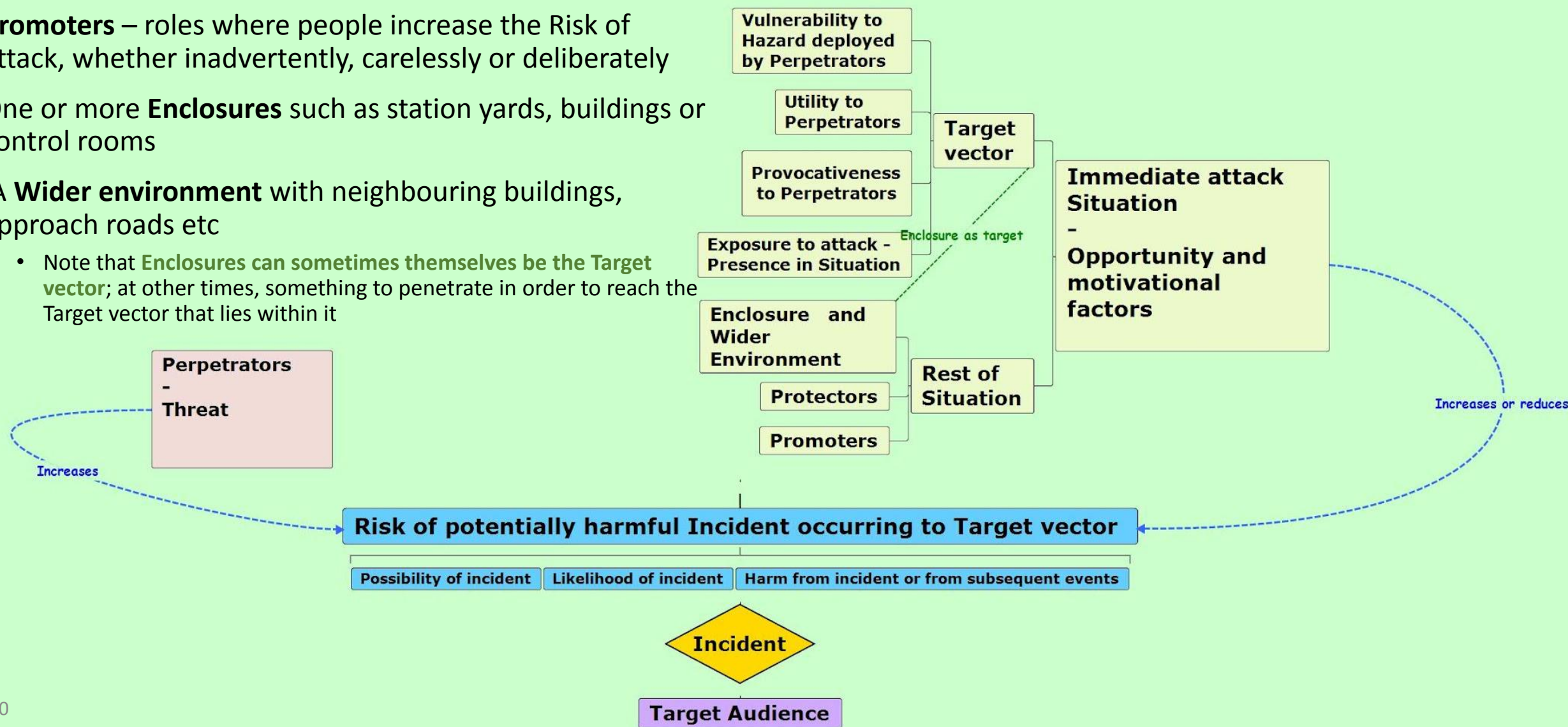


The **Target Vector's** attributes include Vulnerability to particular Hazards, utility and provocativeness to Perpetrators, and some level of Exposure to attack – they are present in the situation and in some way accessible



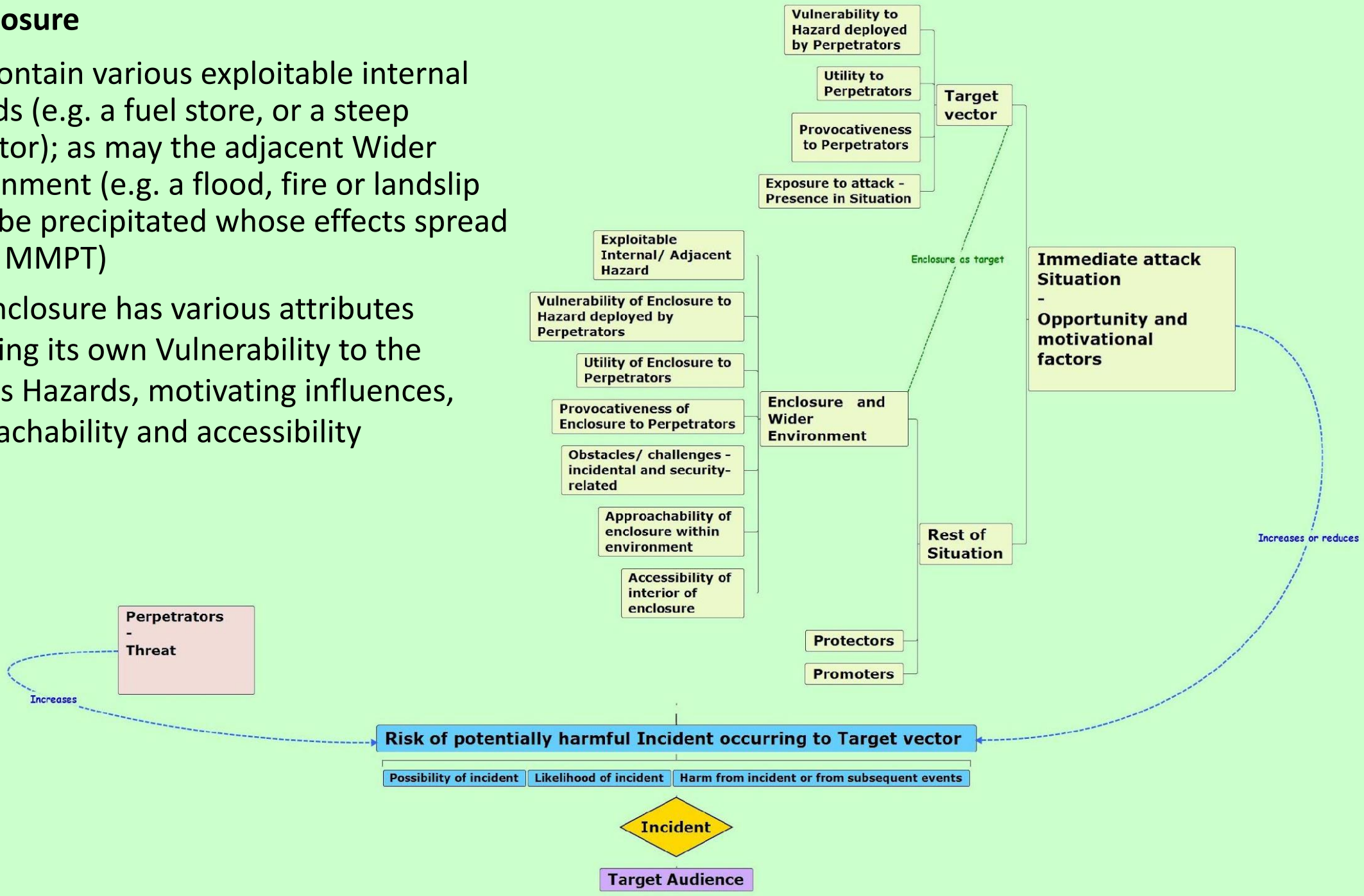
The rest of the Situation comprises

- **Protectors** – roles undertaken by people who reduce the Risk of attack before it happens or when underway – they may be staff, passengers, police, private security
- **Promoters** – roles where people increase the Risk of attack, whether inadvertently, carelessly or deliberately
- One or more **Enclosures** such as station yards, buildings or control rooms
- A **Wider environment** with neighbouring buildings, approach roads etc
 - Note that **Enclosures can sometimes themselves be the Target vector**; at other times, something to penetrate in order to reach the Target vector that lies within it

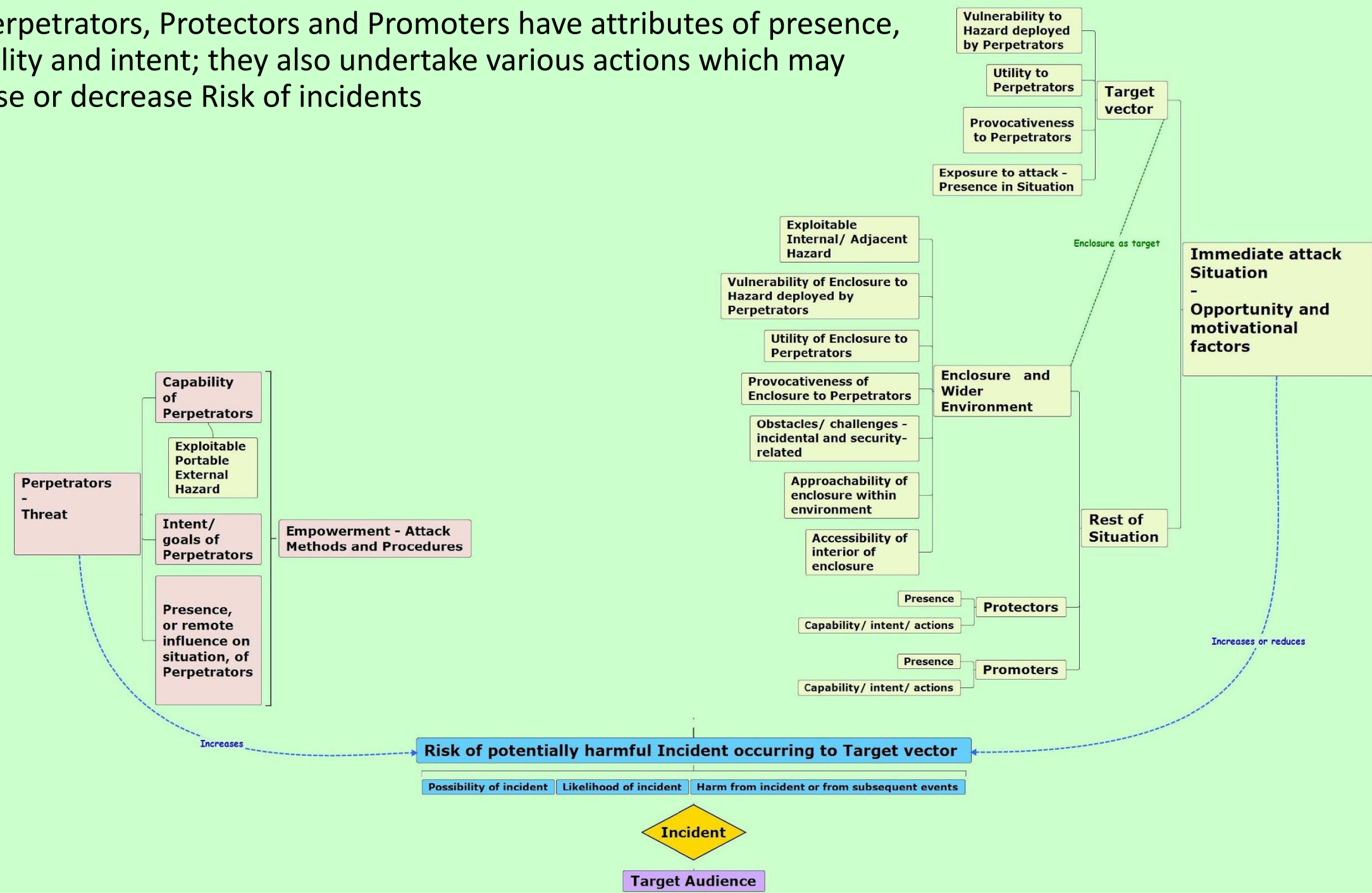


The Enclosure

- May contain various exploitable internal Hazards (e.g. a fuel store, or a steep escalator); as may the adjacent Wider environment (e.g. a flood, fire or landslide could be precipitated whose effects spread to the MMPT)
- The Enclosure has various attributes including its own Vulnerability to the various Hazards, motivating influences, approachability and accessibility

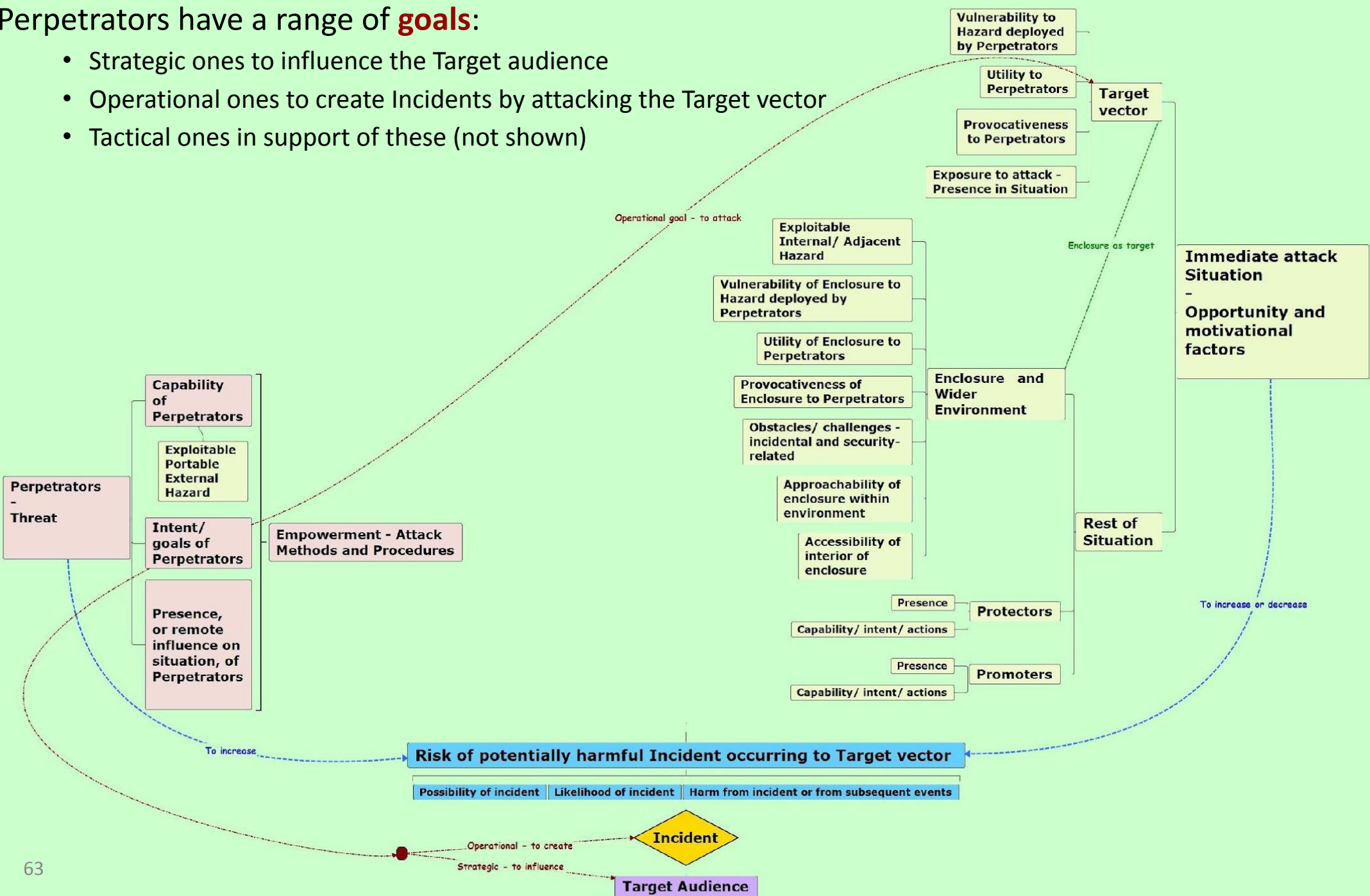


Like Perpetrators, Protectors and Promoters have attributes of presence, capability and intent; they also undertake various actions which may increase or decrease Risk of incidents



Perpetrators have a range of **goals**:

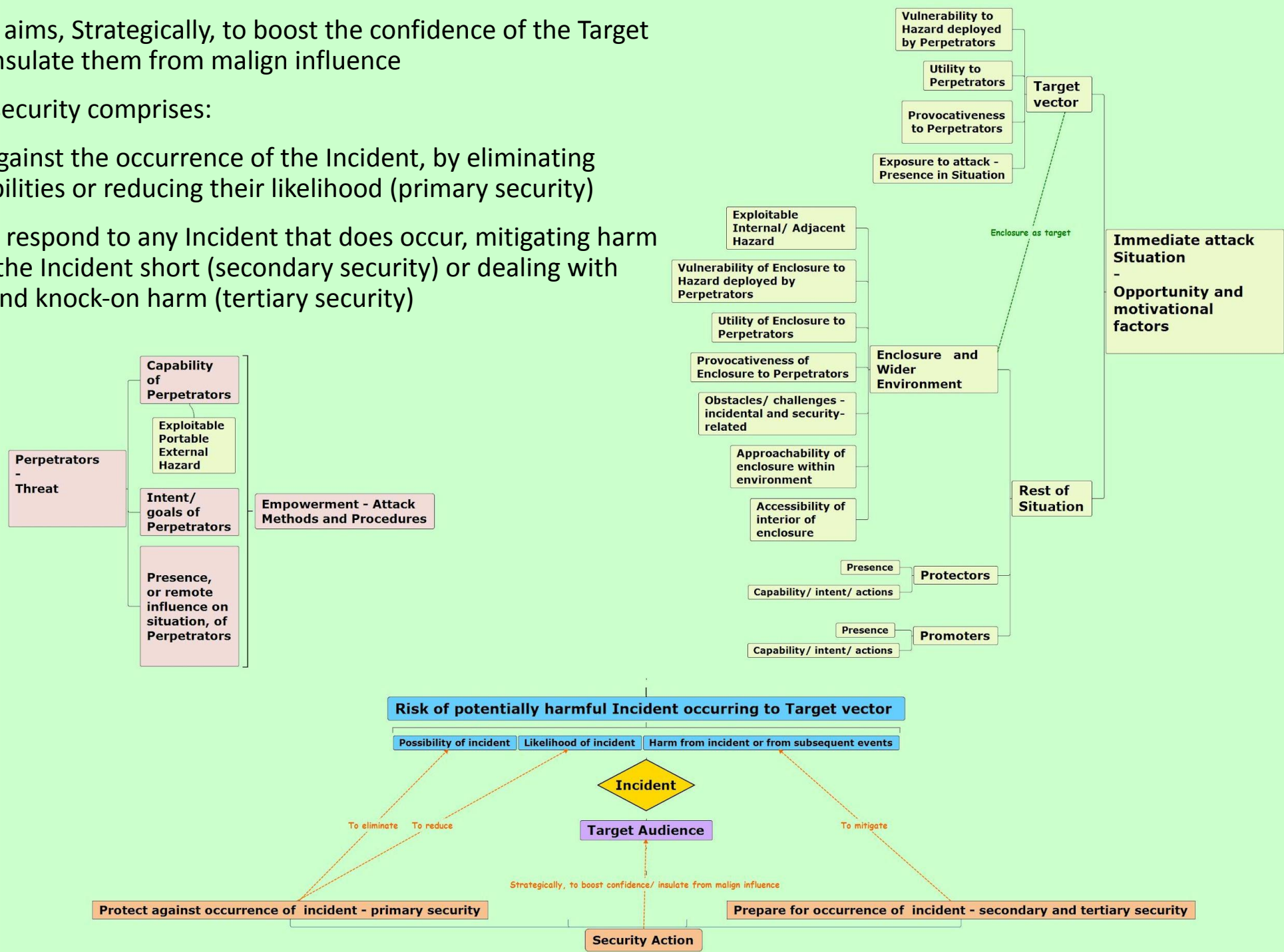
- Strategic ones to influence the Target audience
- Operational ones to create Incidents by attacking the Target vector
- Tactical ones in support of these (not shown)



Security action aims, Strategically, to boost the confidence of the Target audience and insulate them from malign influence

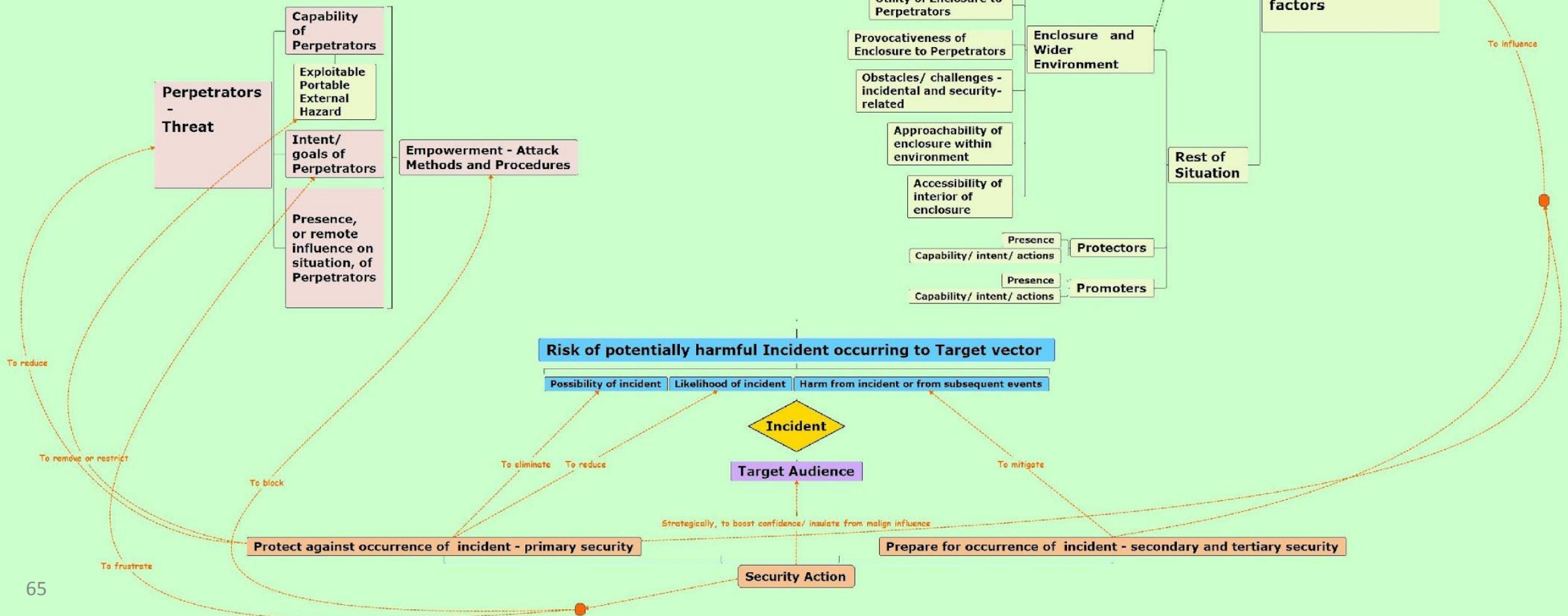
Operationally, security comprises:

- **Protecting** against the occurrence of the Incident, by eliminating attack possibilities or reducing their likelihood (primary security)
- **Preparing** to respond to any Incident that does occur, mitigating harm by stopping the Incident short (secondary security) or dealing with immediate and knock-on harm (tertiary security)



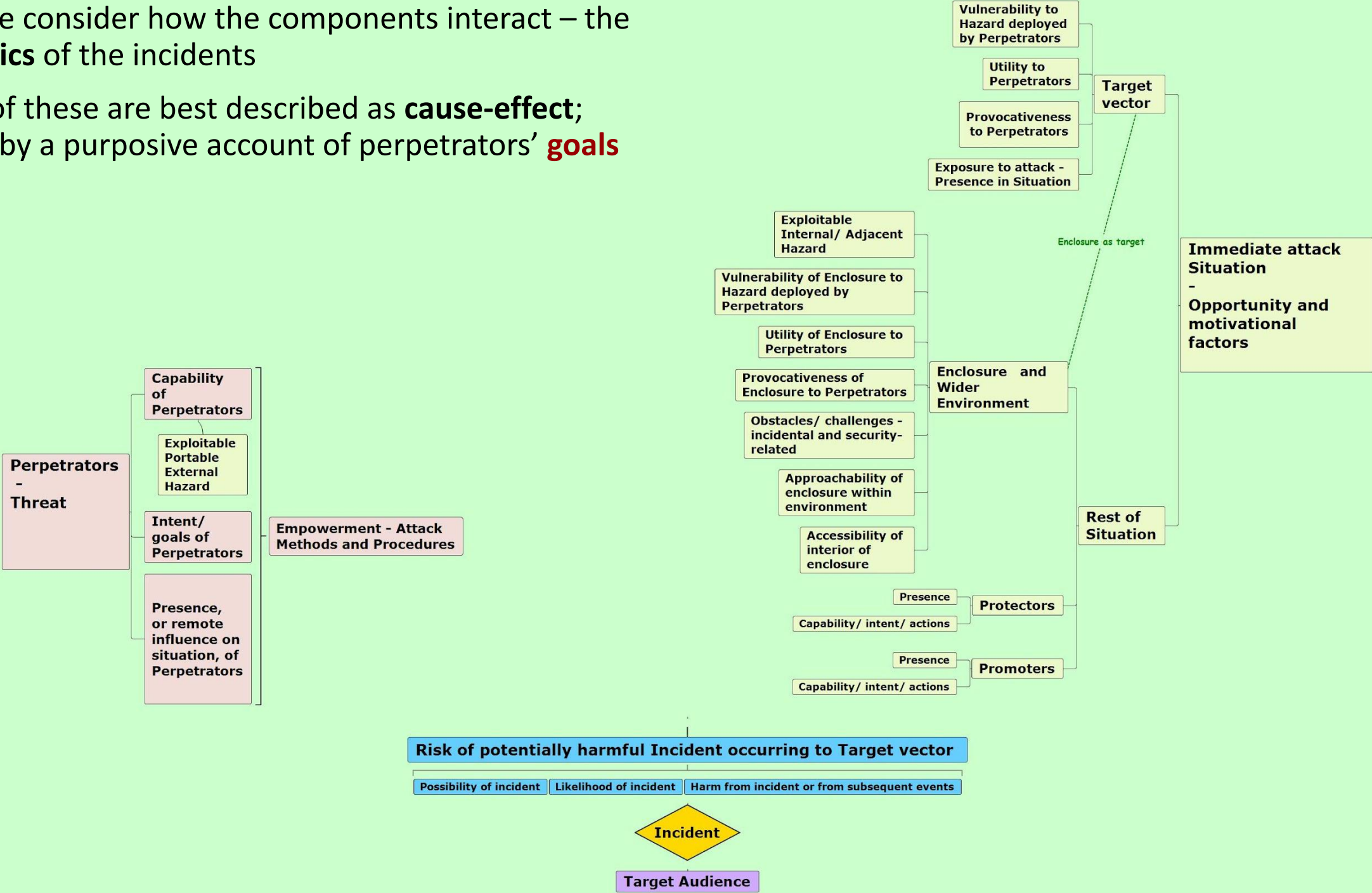
- Reducing the Threat from Perpetrators – by

- Frustrating their intentions/goals – by
 - Blocking their Attack methods and procedures
 - Removing/restricting Exploitable external hazards
 - Influencing the Opportunity and Motivational factors in the immediate attack Situation



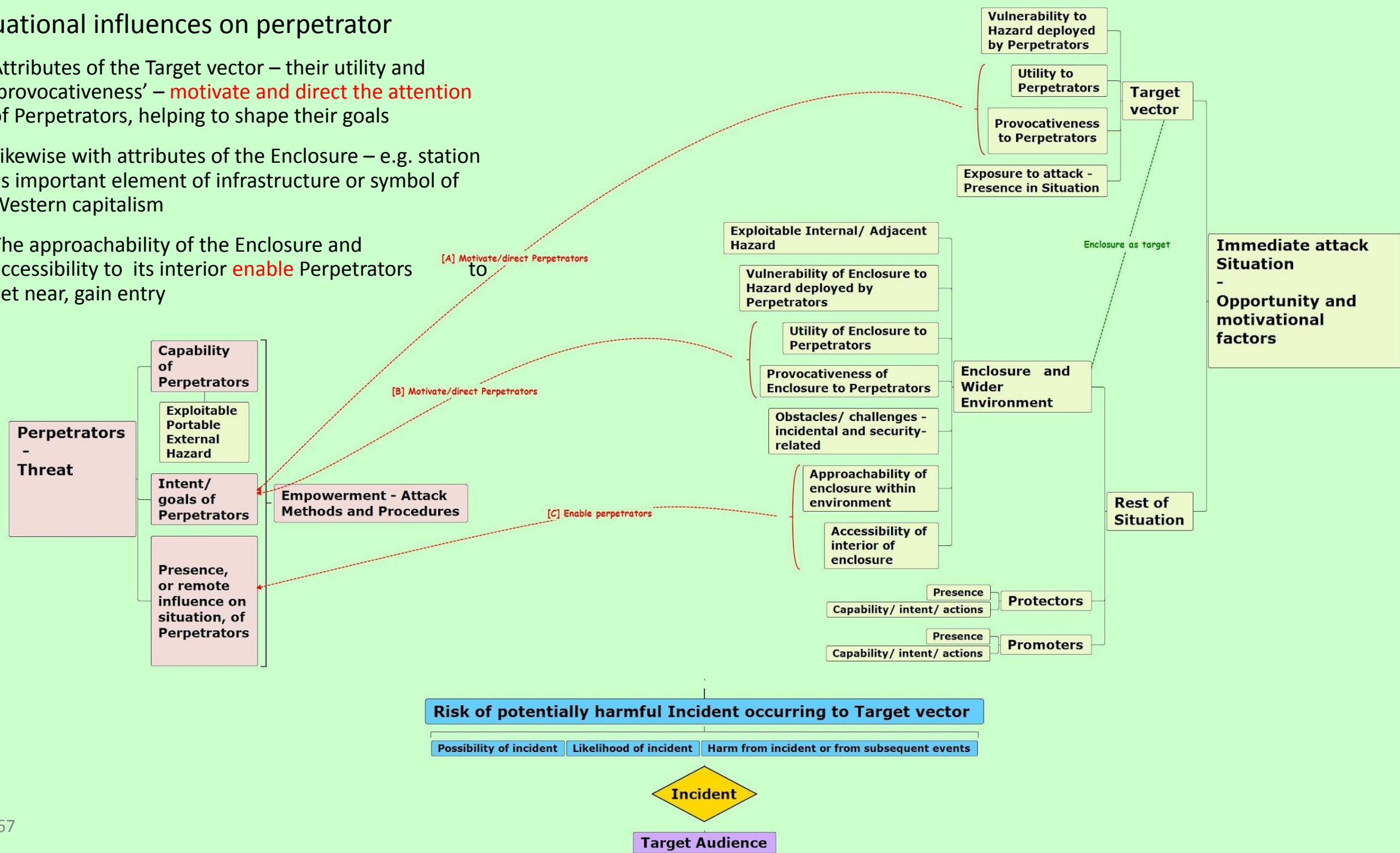
Now we consider how the components interact – the **dynamics** of the incidents

Some of these are best described as **cause-effect**;
others by a purposive account of perpetrators' **goals**



Situational influences on perpetrator

- Attributes of the Target vector – their utility and ‘provocativeness’ – **motivate and direct the attention** of Perpetrators, helping to shape their goals
- Likewise with attributes of the Enclosure – e.g. station as important element of infrastructure or symbol of Western capitalism
- The approachability of the Enclosure and accessibility to its interior **enable** Perpetrators to get near, gain entry

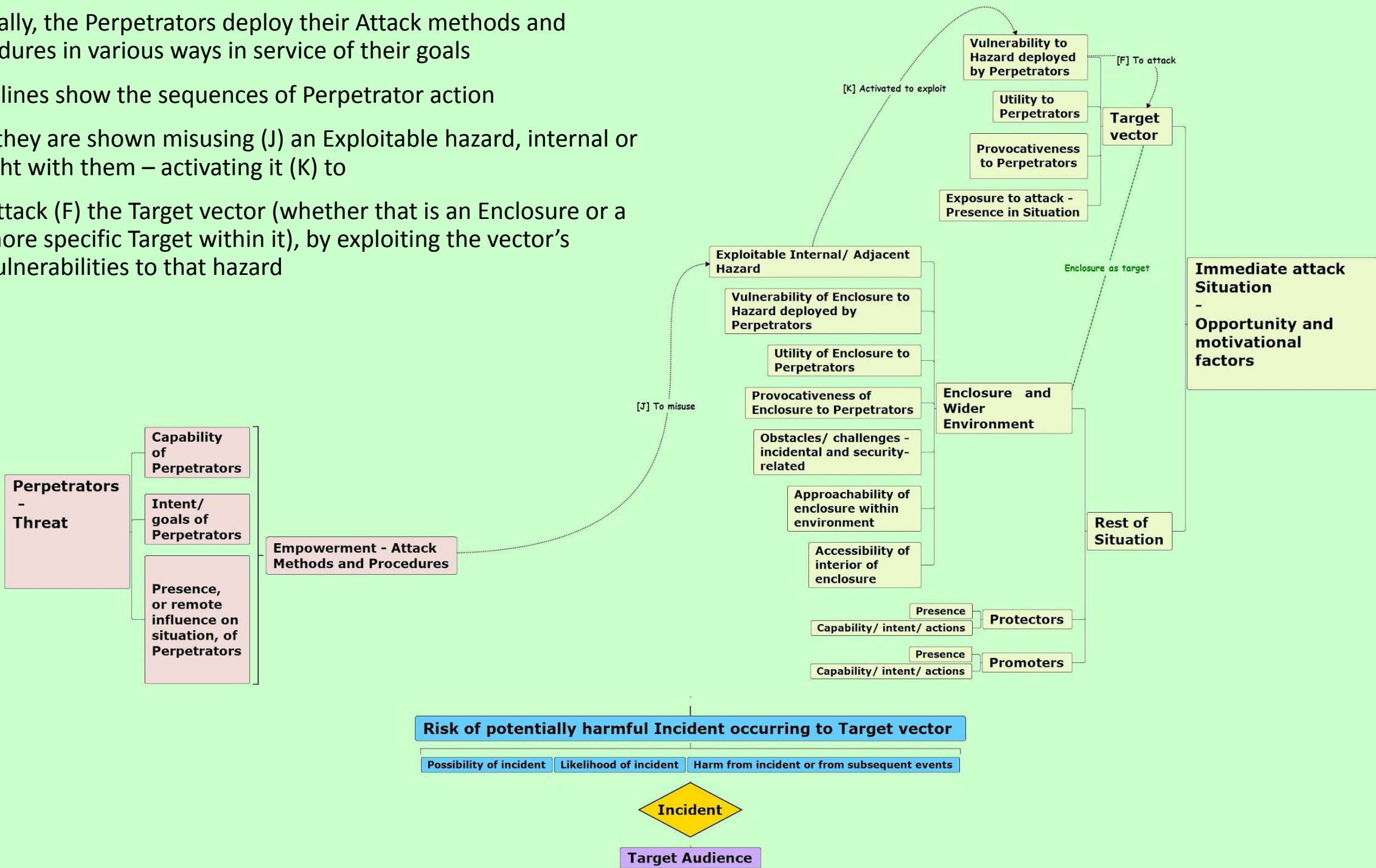


Tactically, the Perpetrators deploy their Attack methods and procedures in various ways in service of their goals

Black lines show the sequences of Perpetrator action

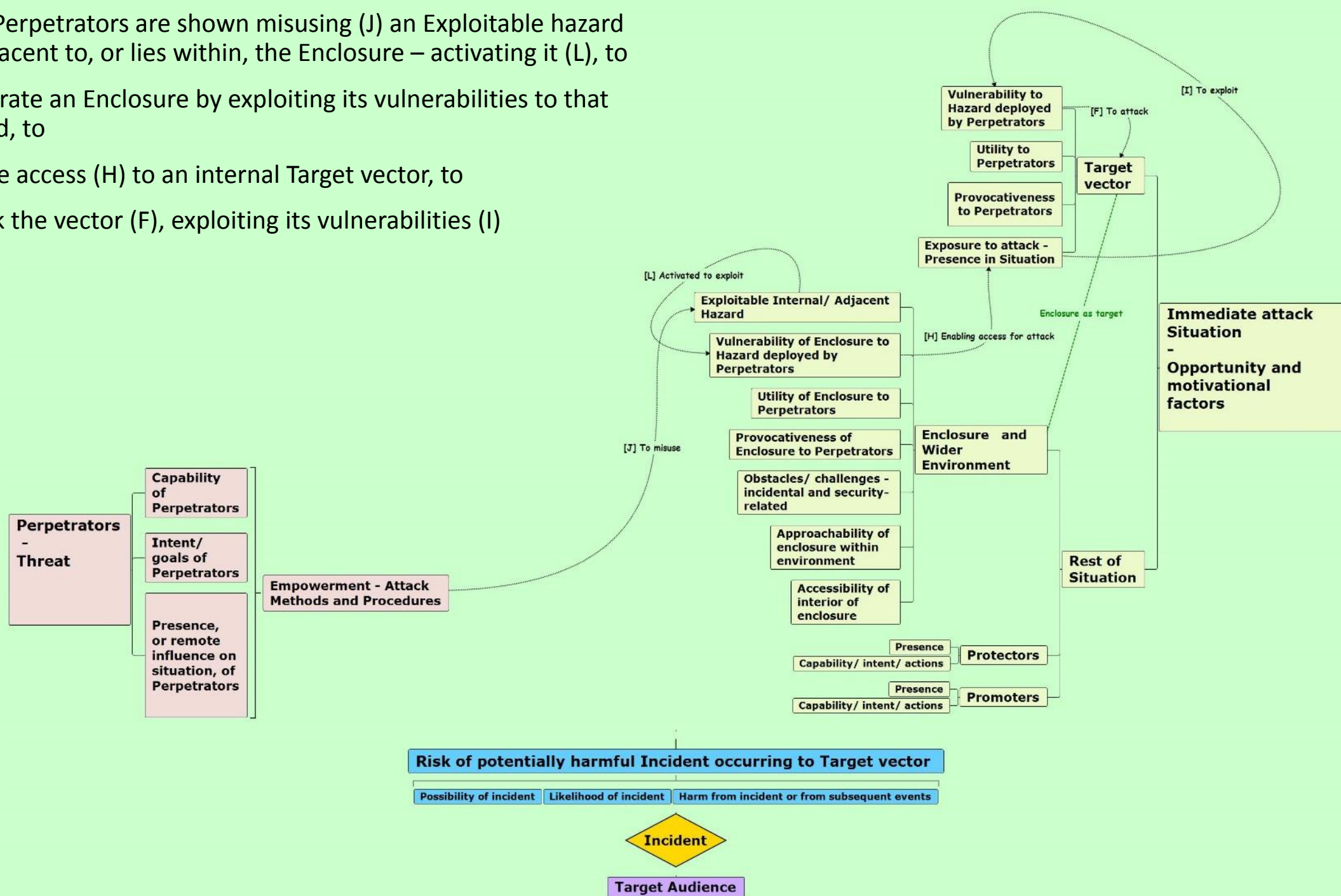
Here they are shown misusing (J) an Exploitable hazard, internal or brought with them – activating it (K) to

- 1. Attack (F) the Target vector (whether that is an Enclosure or a more specific Target within it), by exploiting the vector’s vulnerabilities to that hazard



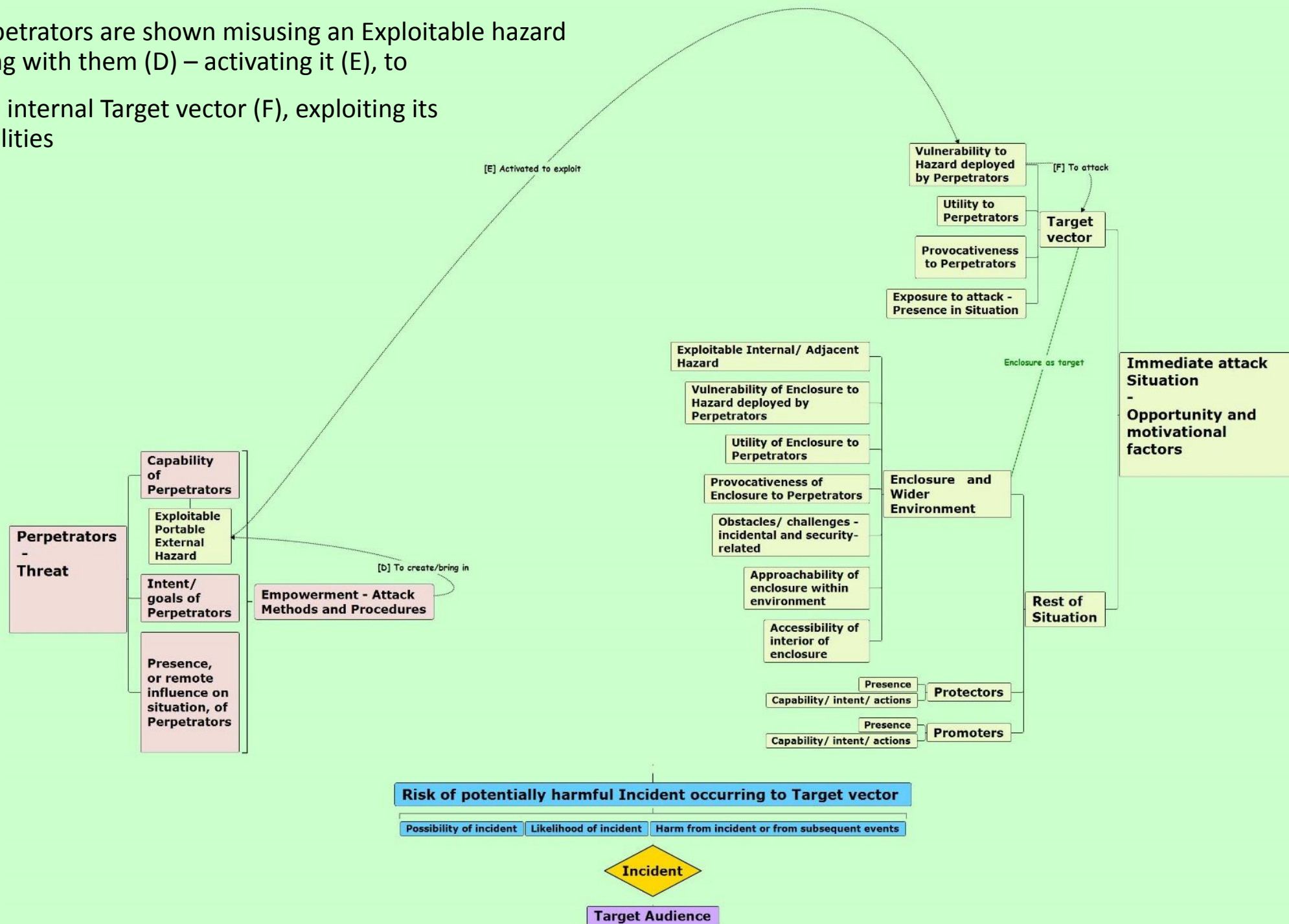
Here the Perpetrators are shown misusing (J) an Exploitable hazard that is adjacent to, or lies within, the Enclosure – activating it (L), to

1. Penetrate an Enclosure by exploiting its vulnerabilities to that hazard, to
2. Enable access (H) to an internal Target vector, to
3. Attack the vector (F), exploiting its vulnerabilities (I)



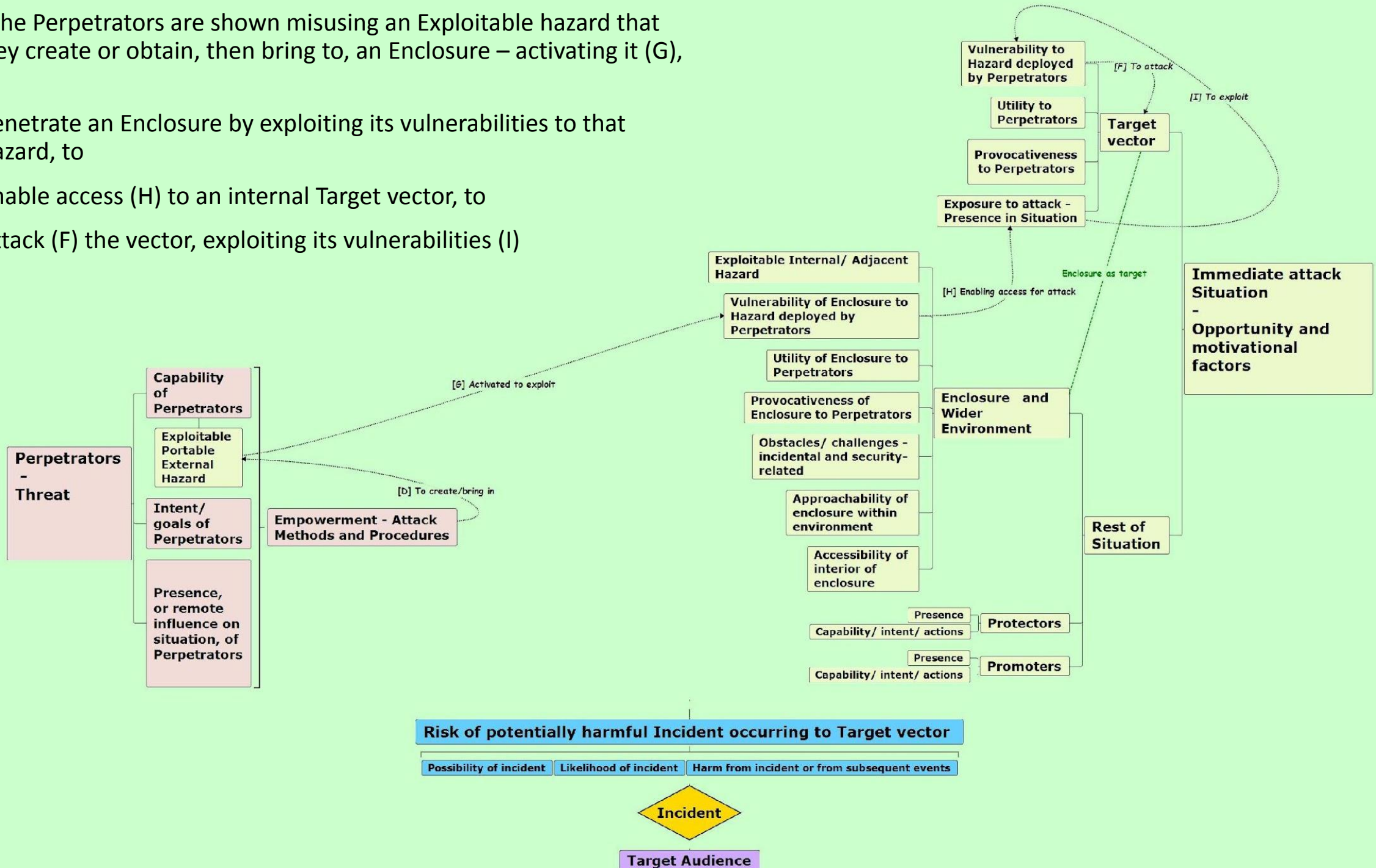
Here the Perpetrators are shown misusing an Exploitable hazard that they bring with them (D) – activating it (E), to

1. Attack an internal Target vector (F), exploiting its vulnerabilities



Here the Perpetrators are shown misusing an Exploitable hazard that (D) they create or obtain, then bring to, an Enclosure – activating it (G), to

1. Penetrate an Enclosure by exploiting its vulnerabilities to that hazard, to
2. Enable access (H) to an internal Target vector, to
3. Attack (F) the vector, exploiting its vulnerabilities (I)



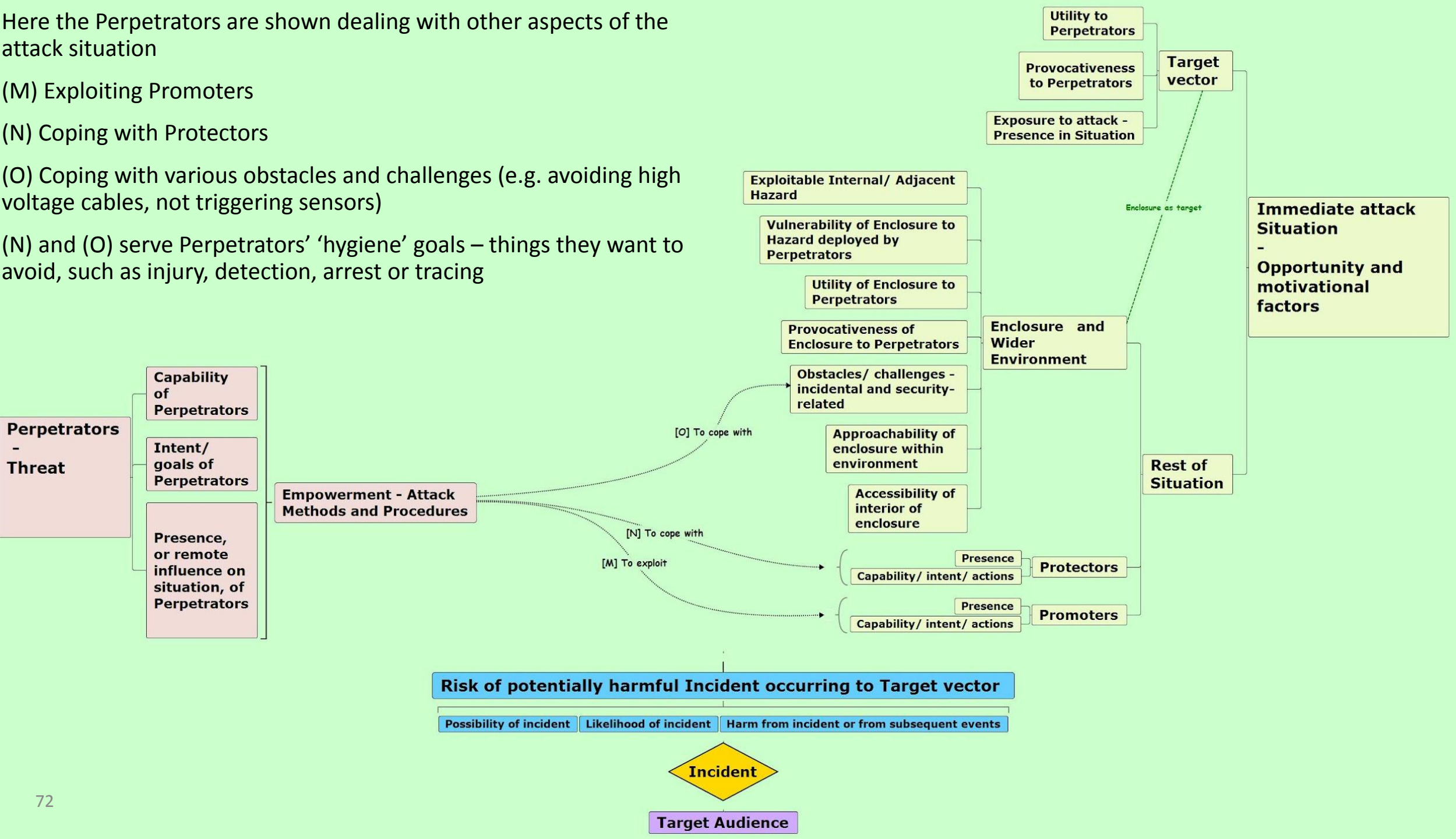
Here the Perpetrators are shown dealing with other aspects of the attack situation

(M) Exploiting Promoters

(N) Coping with Protectors

(O) Coping with various obstacles and challenges (e.g. avoiding high voltage cables, not triggering sensors)

(N) and (O) serve Perpetrators' 'hygiene' goals – things they want to avoid, such as injury, detection, arrest or tracing



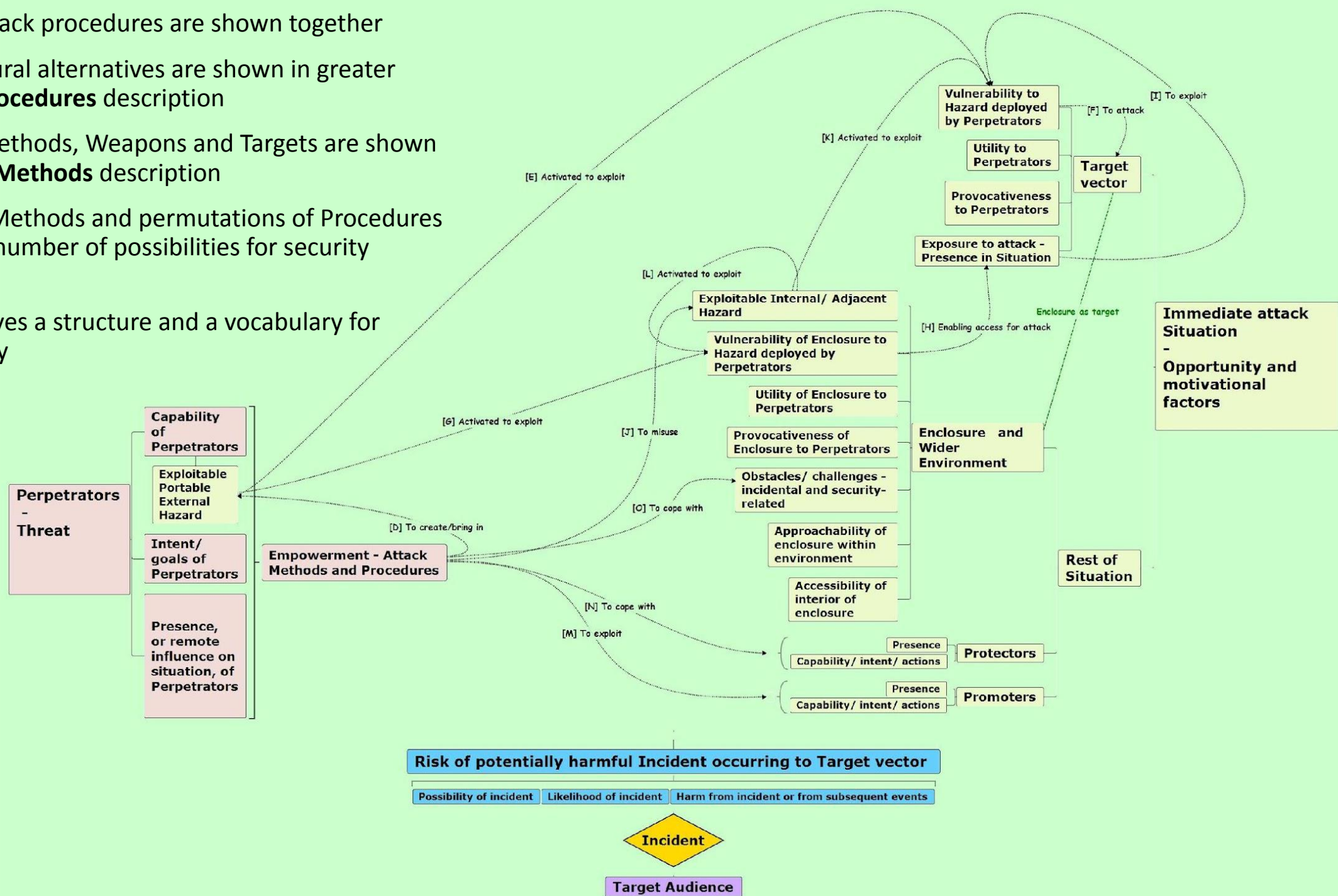
Here these various attack procedures are shown together

These diverse procedural alternatives are shown in greater detail in the **Attack Procedures** description

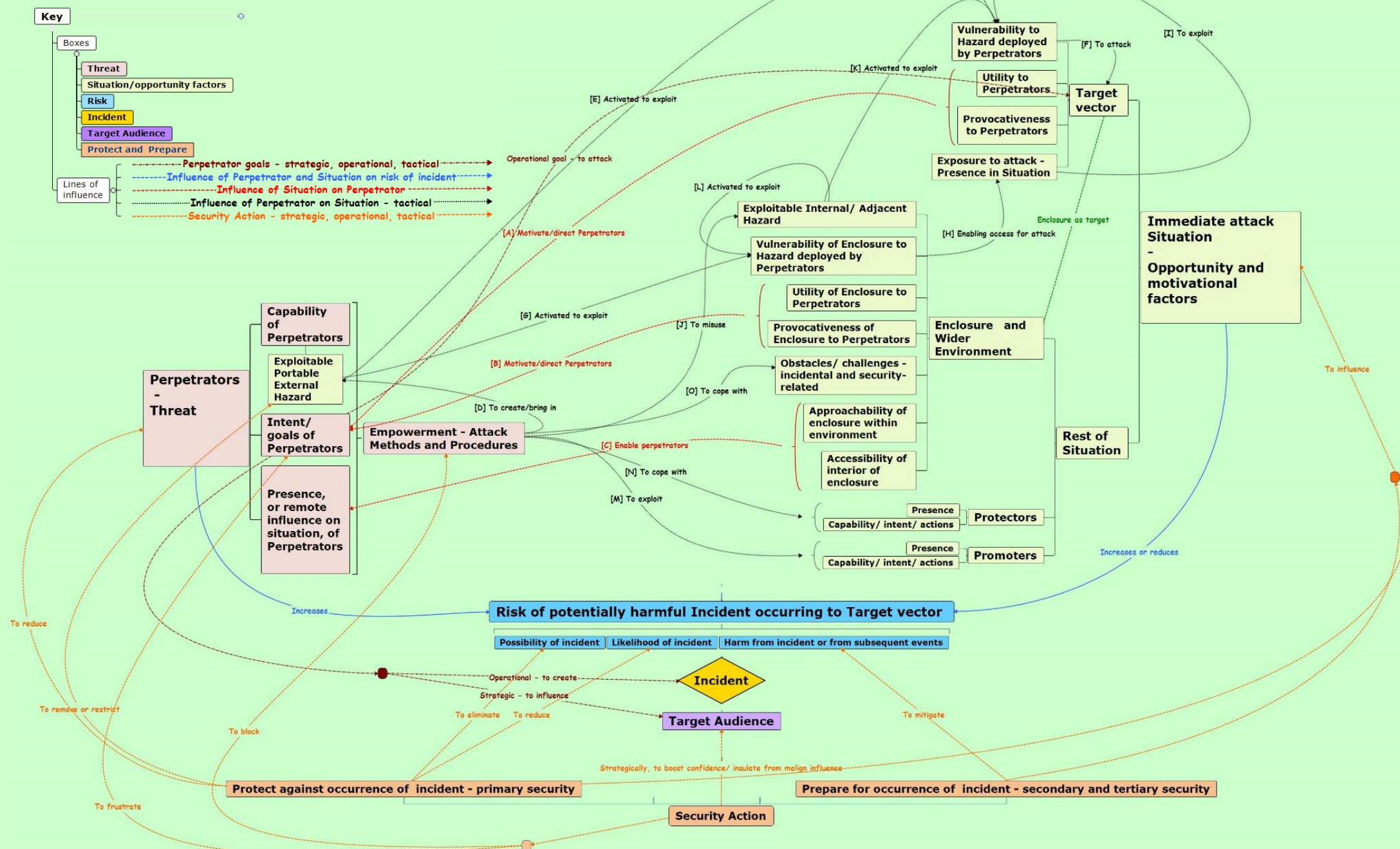
The range of Attack methods, Weapons and Targets are shown in the **Tactical Attack Methods** description

The combinations of Methods and permutations of Procedures make for a very large number of possibilities for security planners to consider

But this framework gives a structure and a vocabulary for doing so systematically



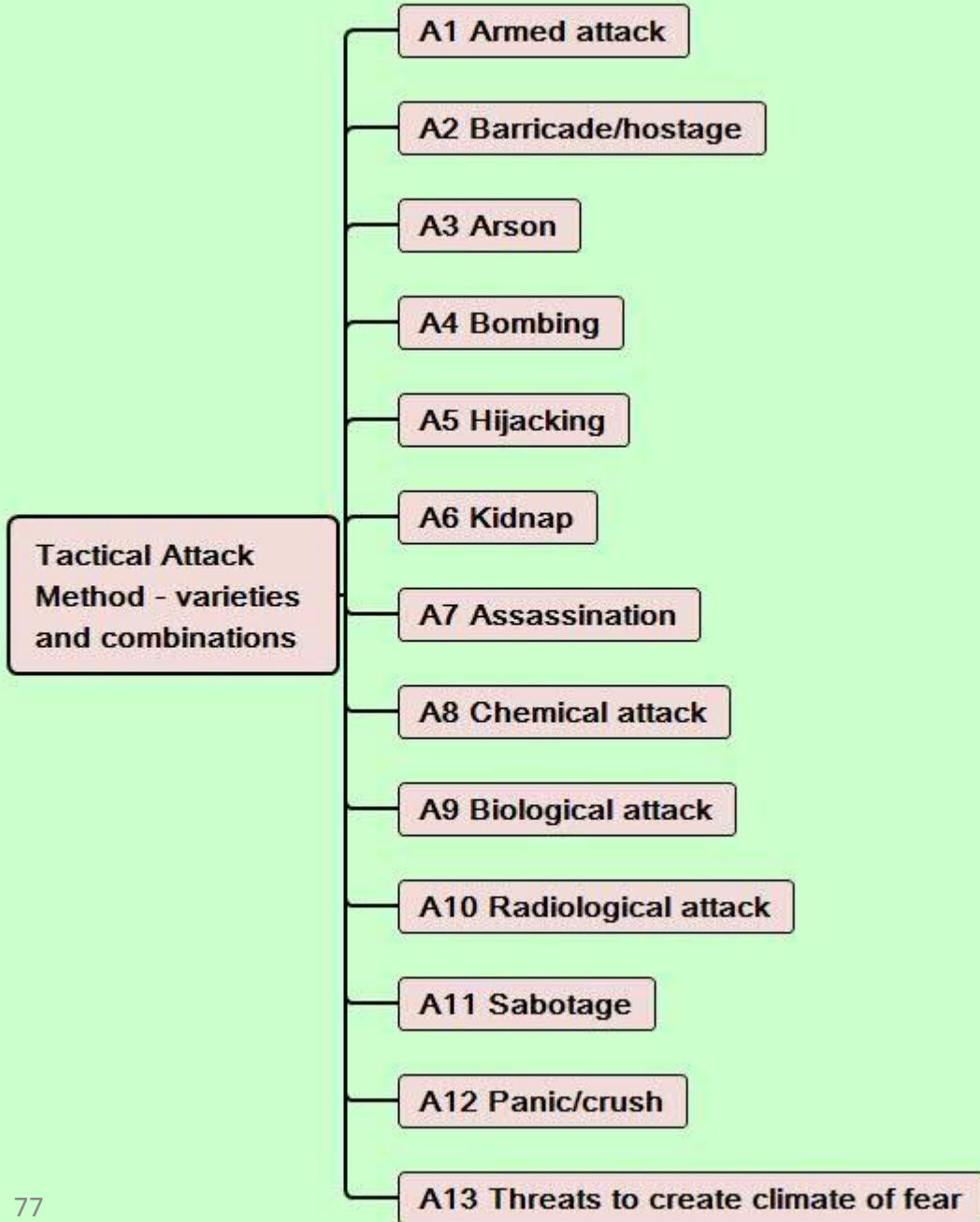
Here are all the interactions together

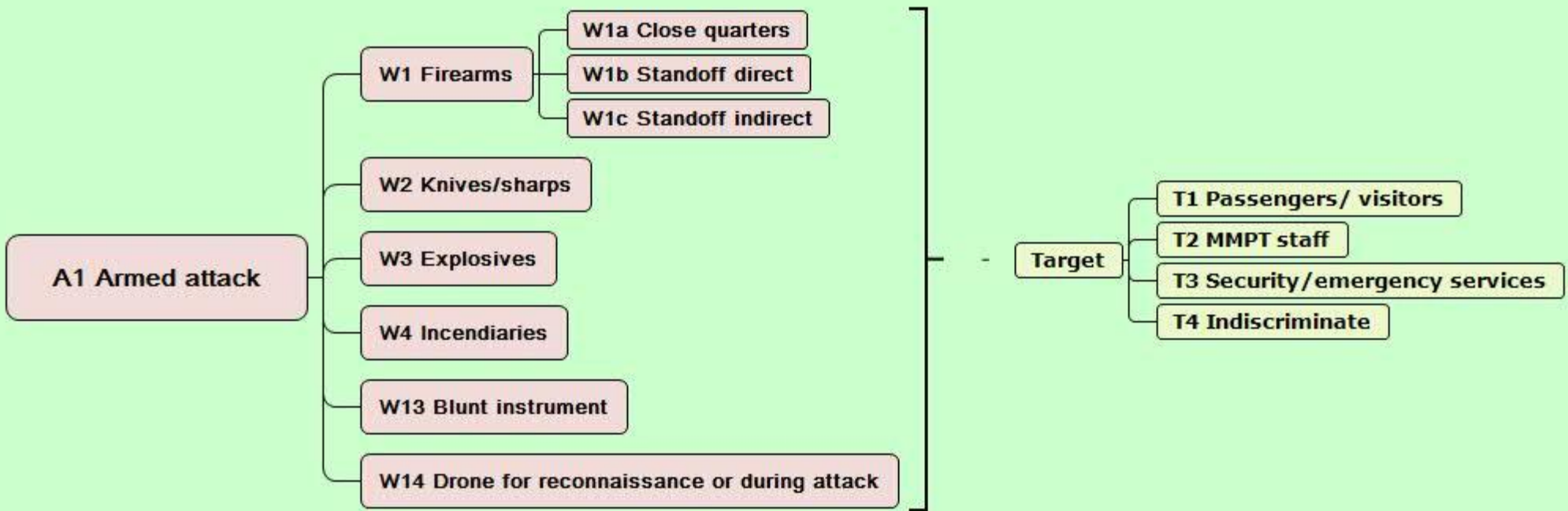


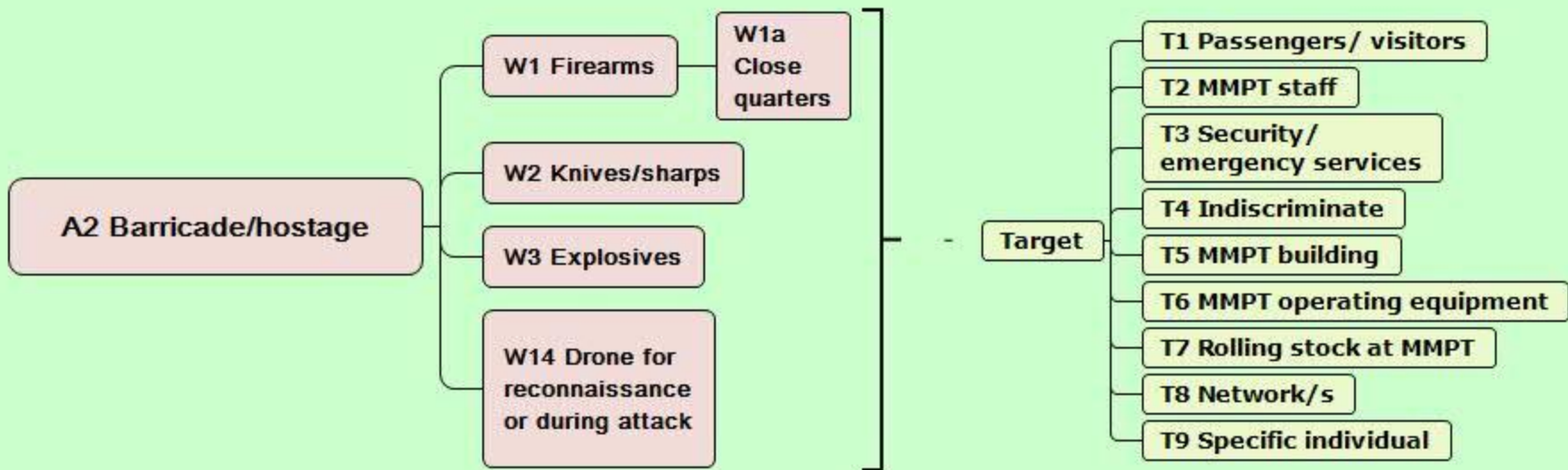
Based on Rand classification of terrorist attacks 1968-2009

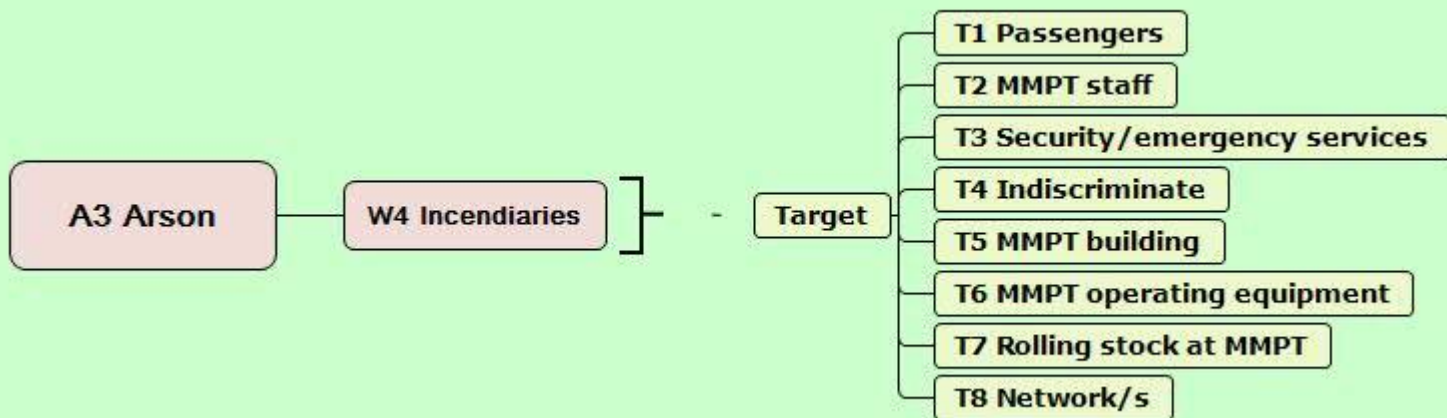
Think Perpetrator

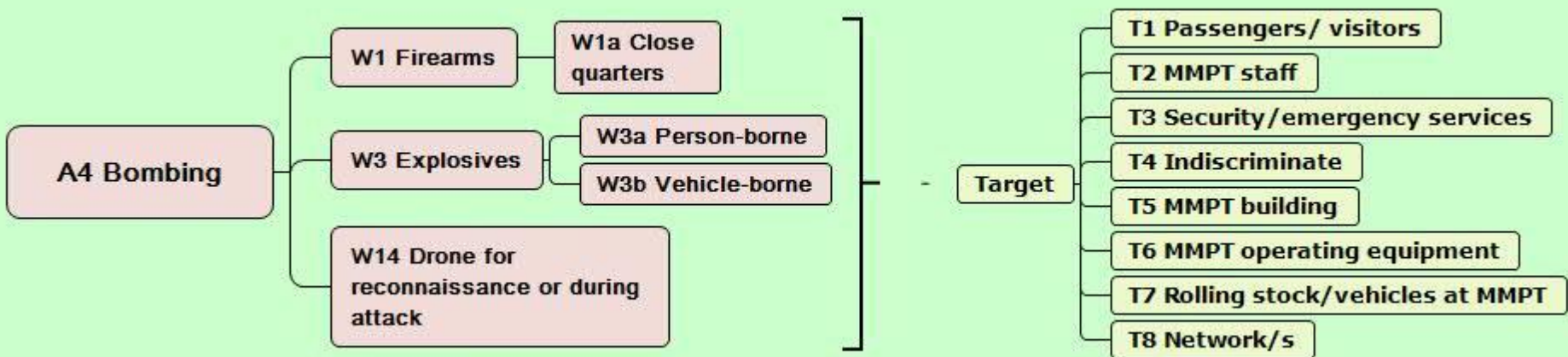
**Tactical Attack
Method - varieties
and combinations**

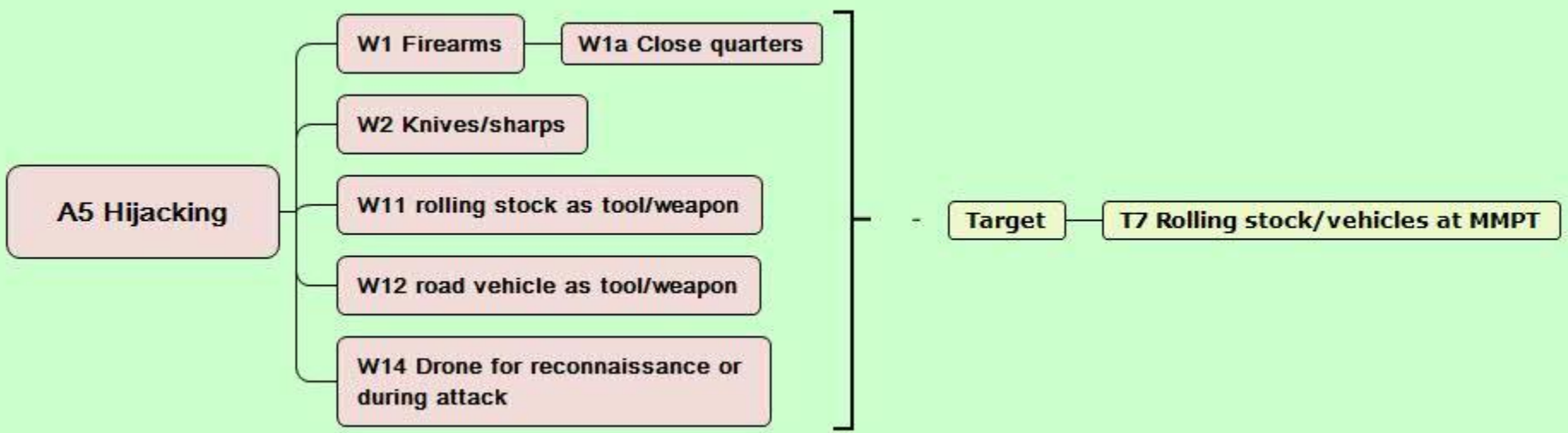


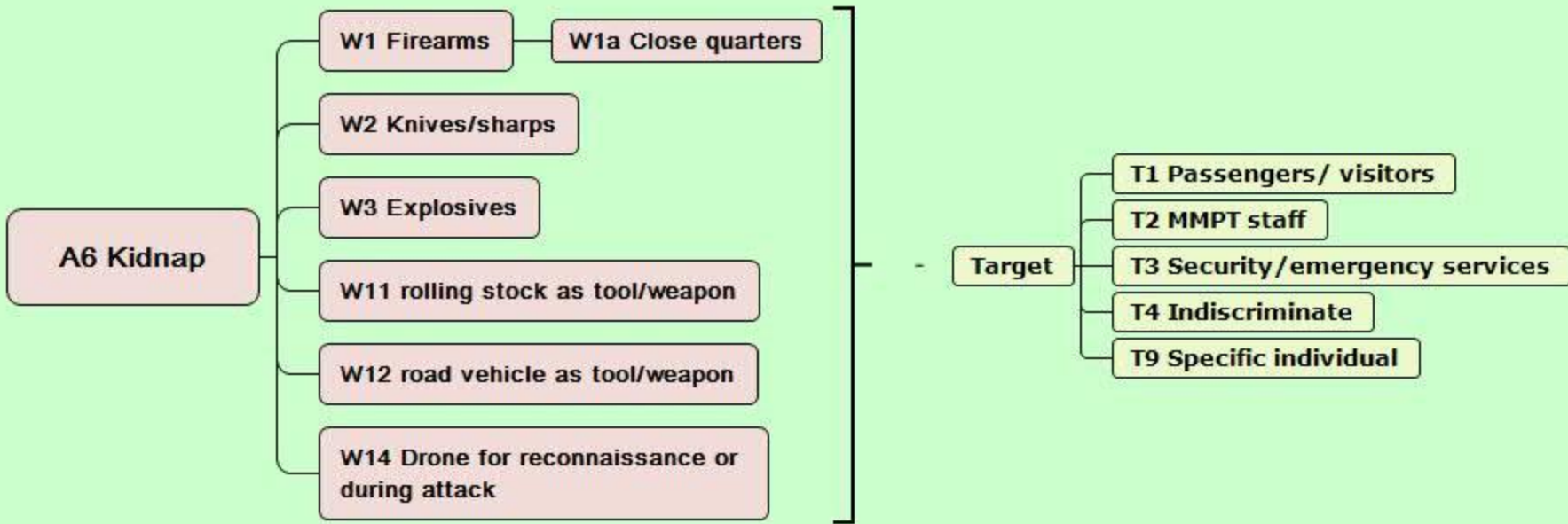


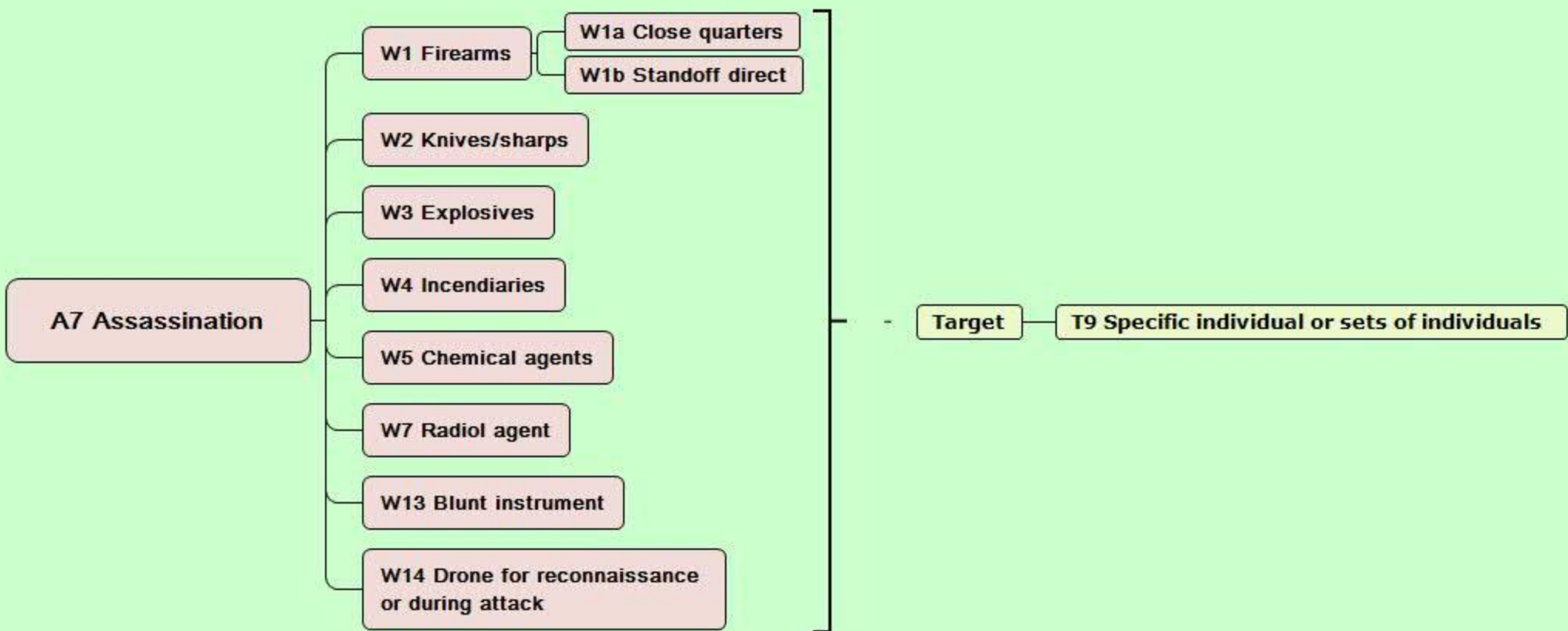


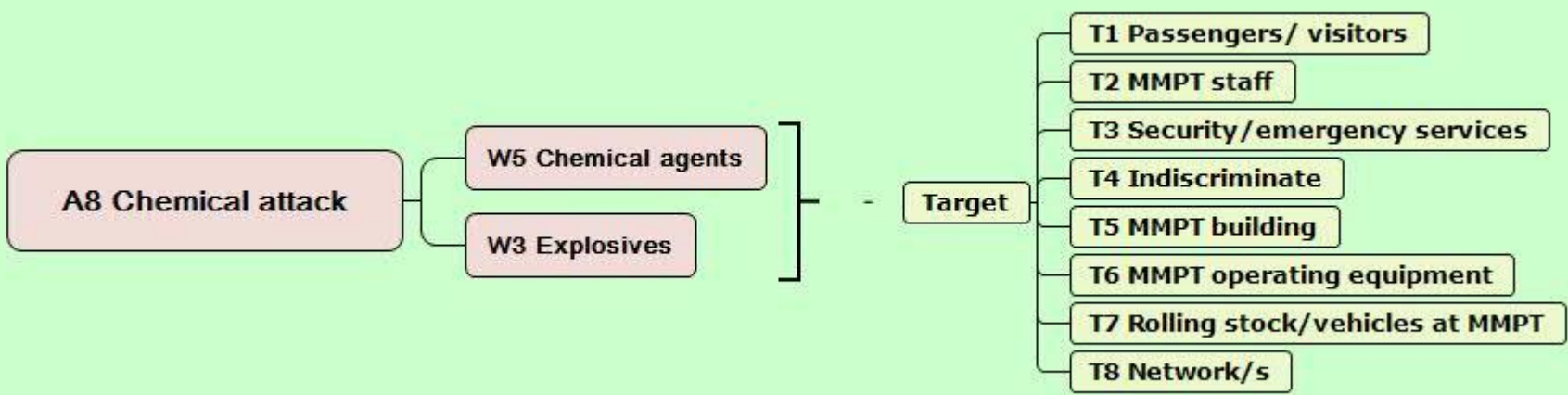






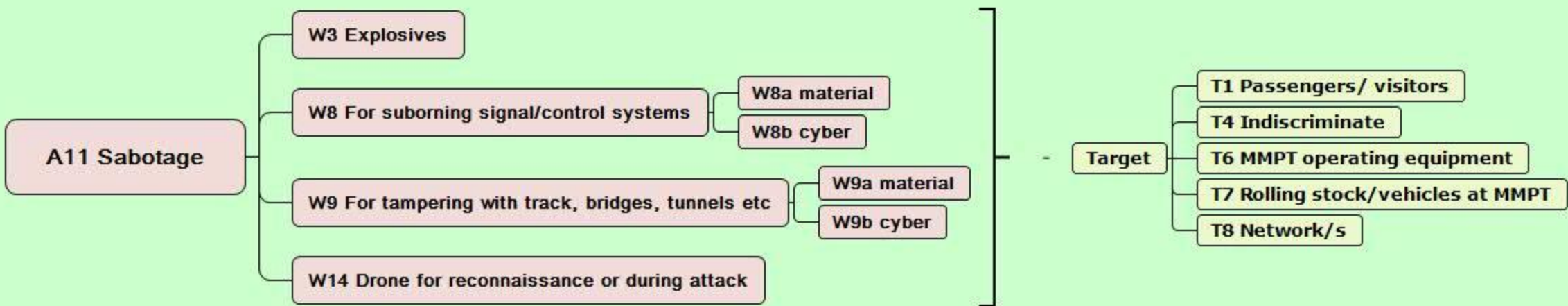


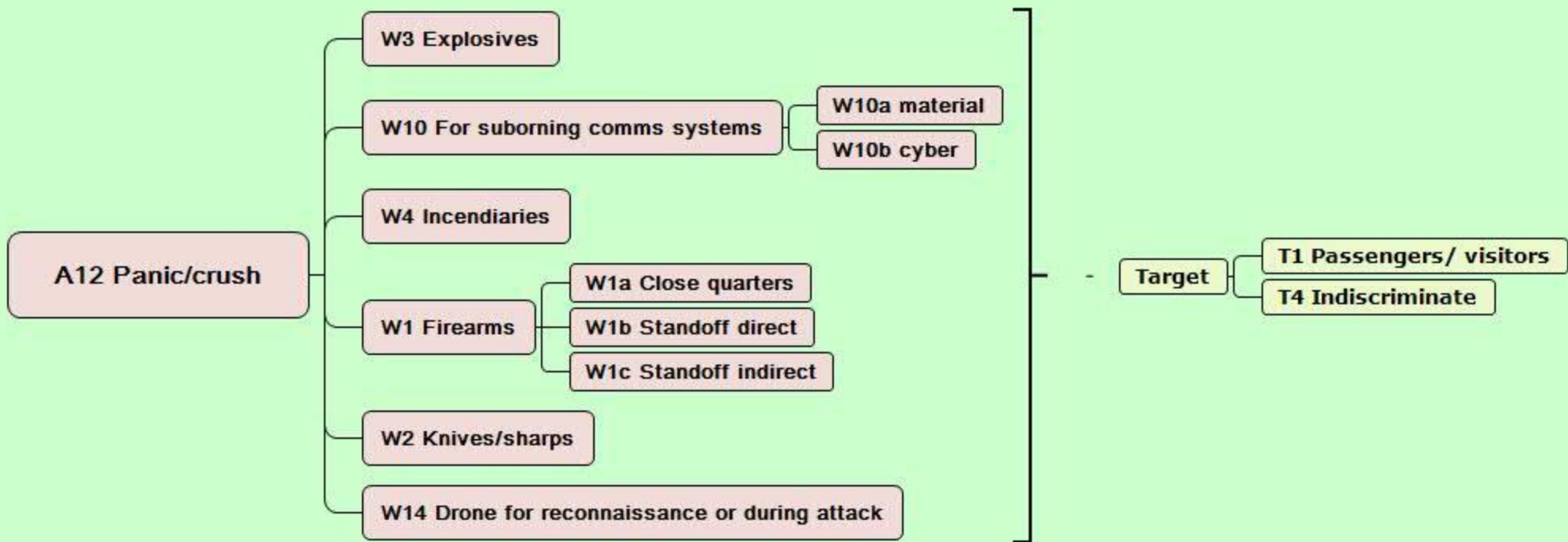






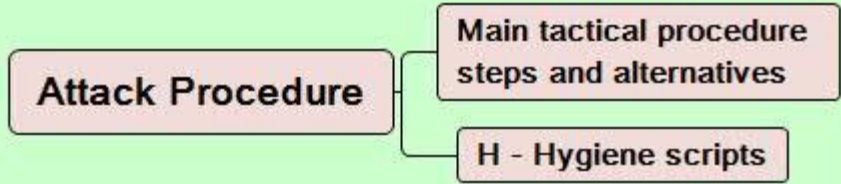


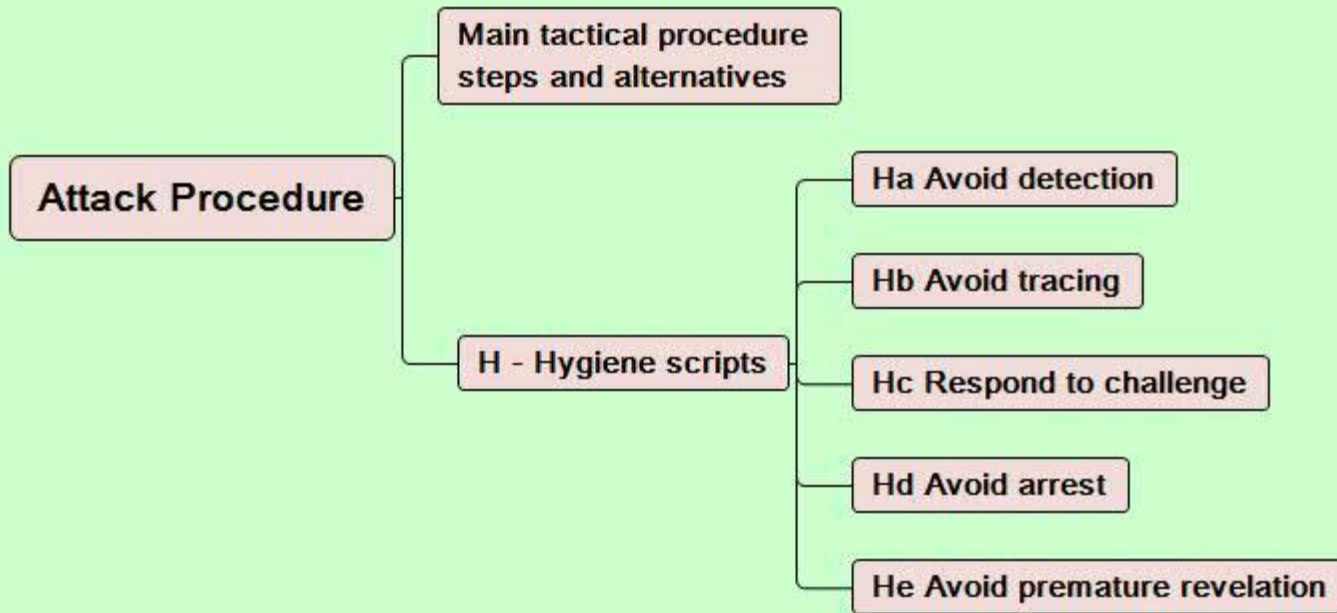


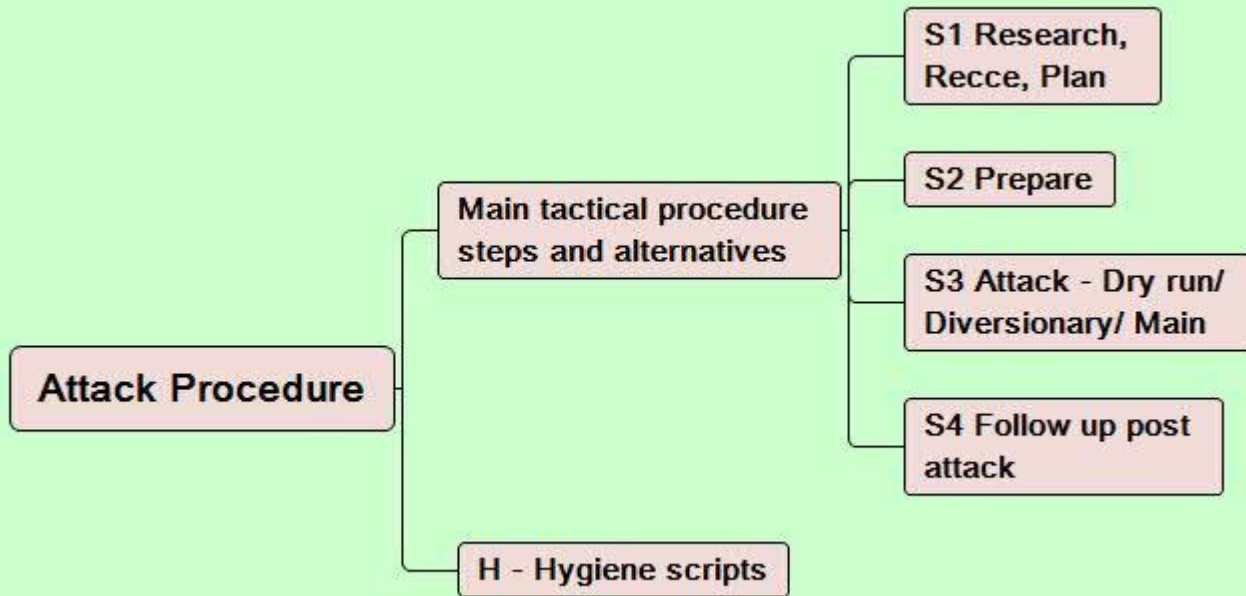


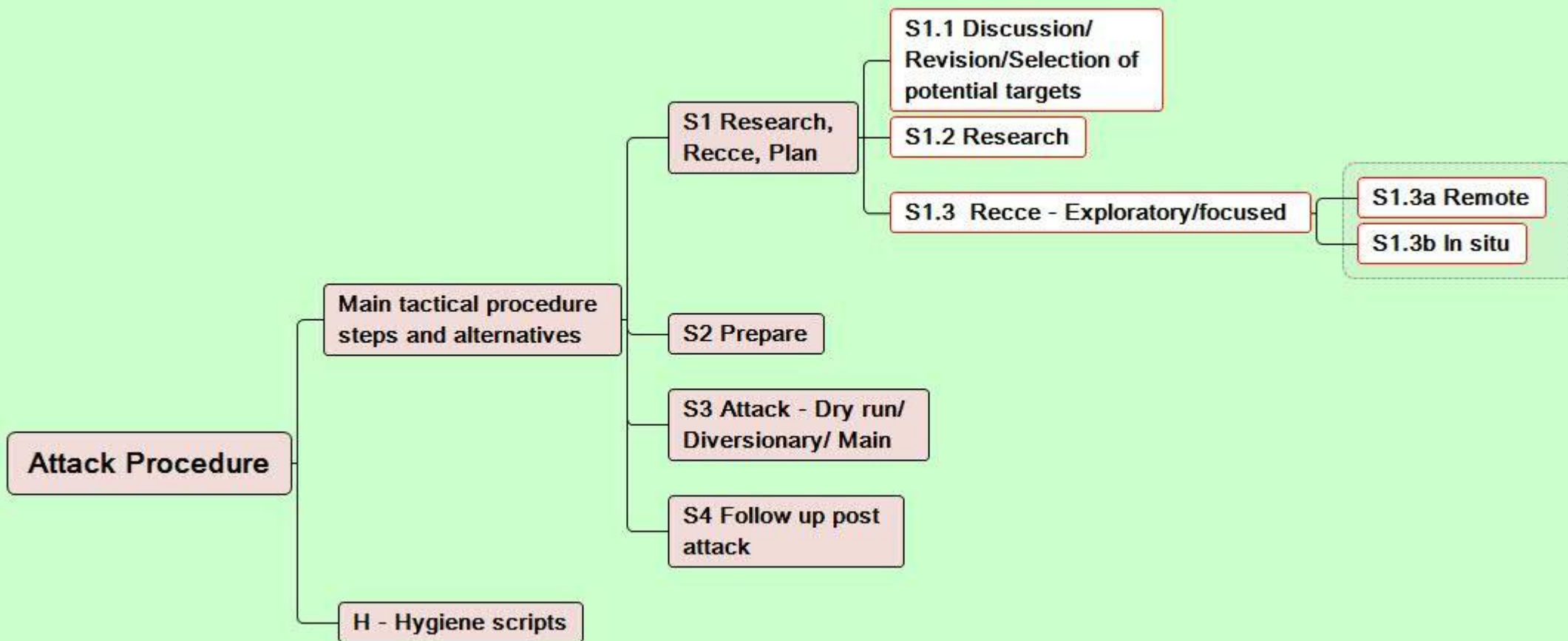
Developed from Project Griffin and the concept of crime scripts

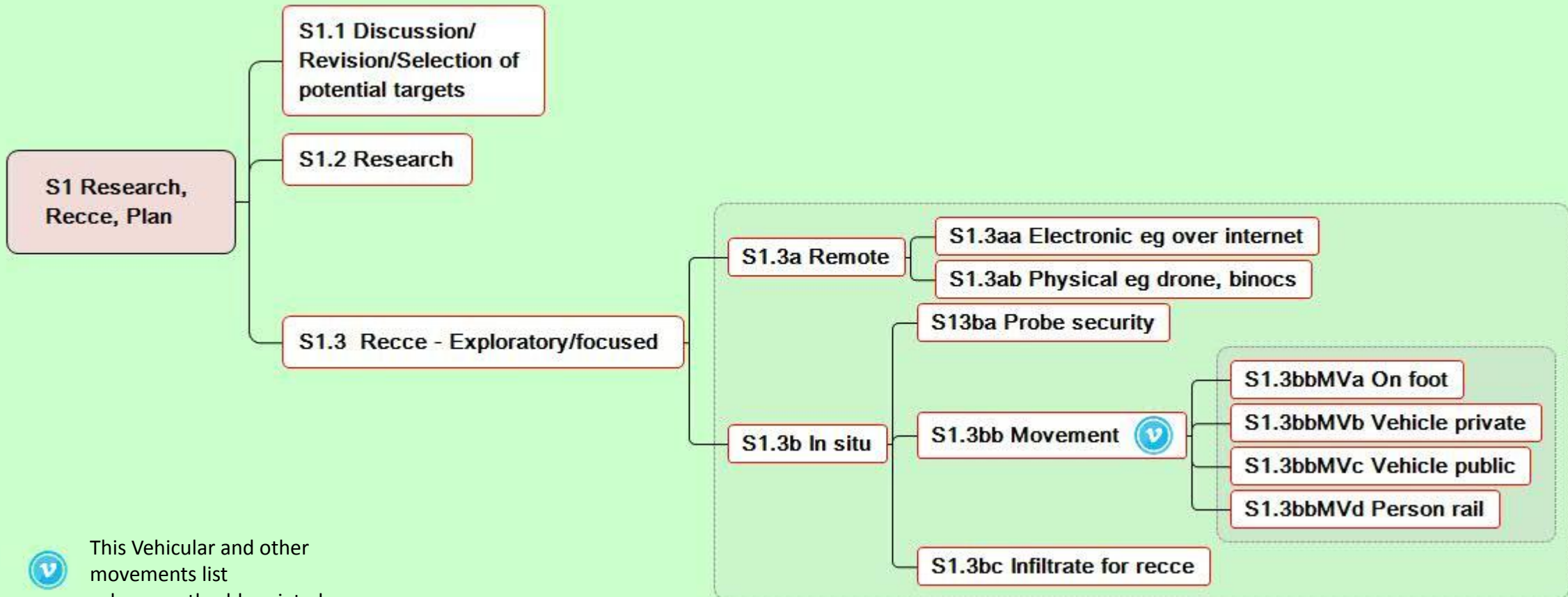
Think Perpetrator, Threat



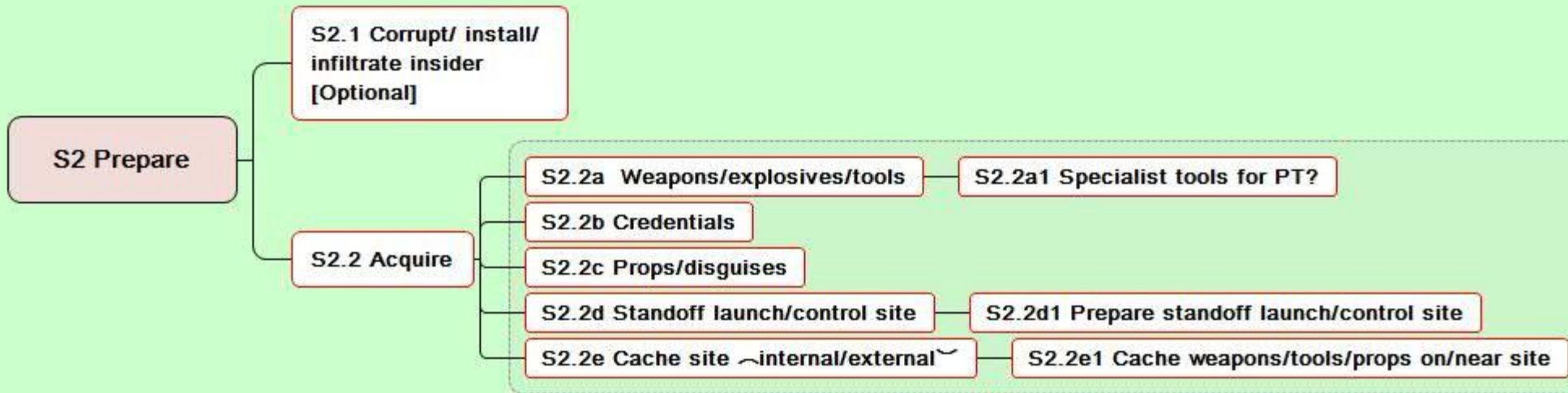




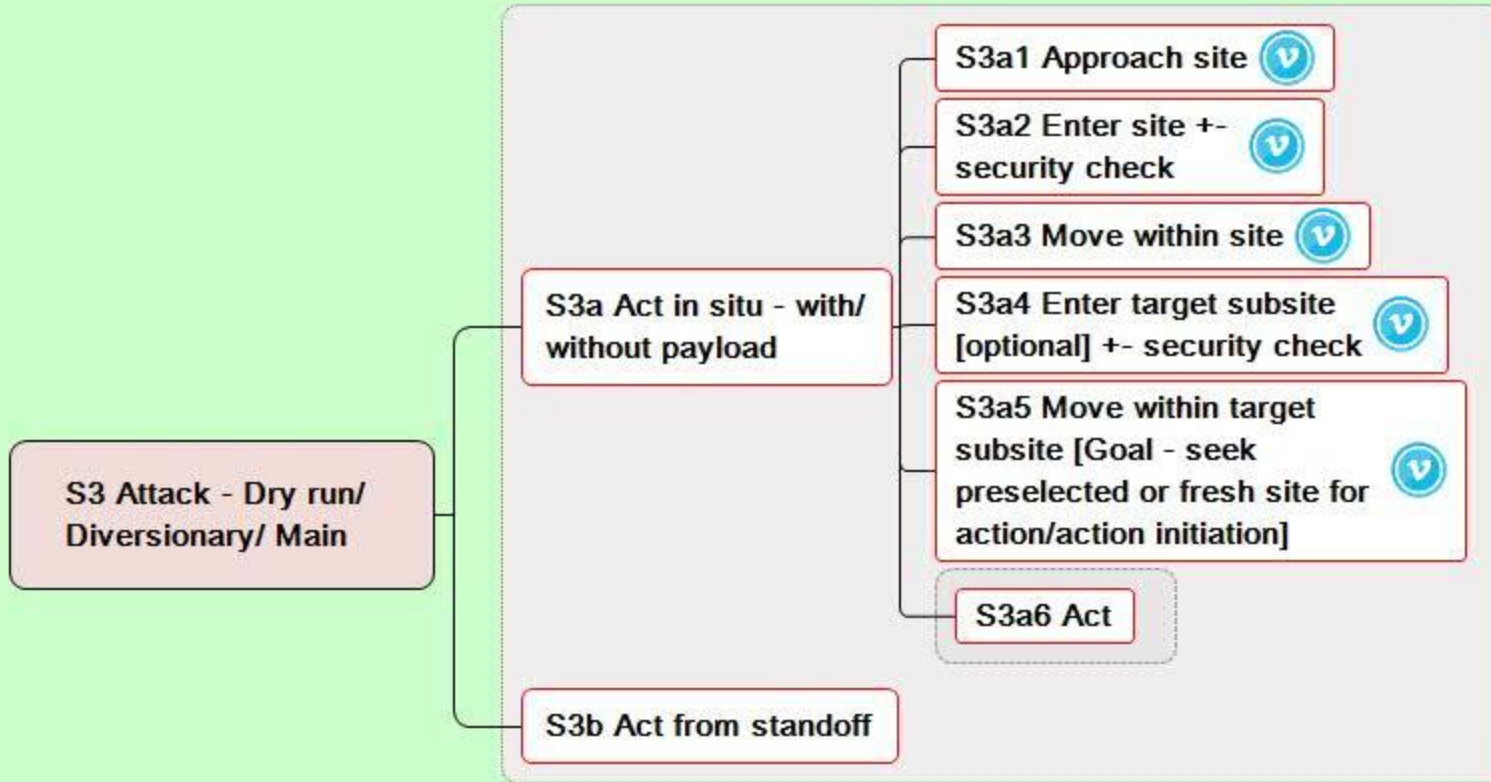


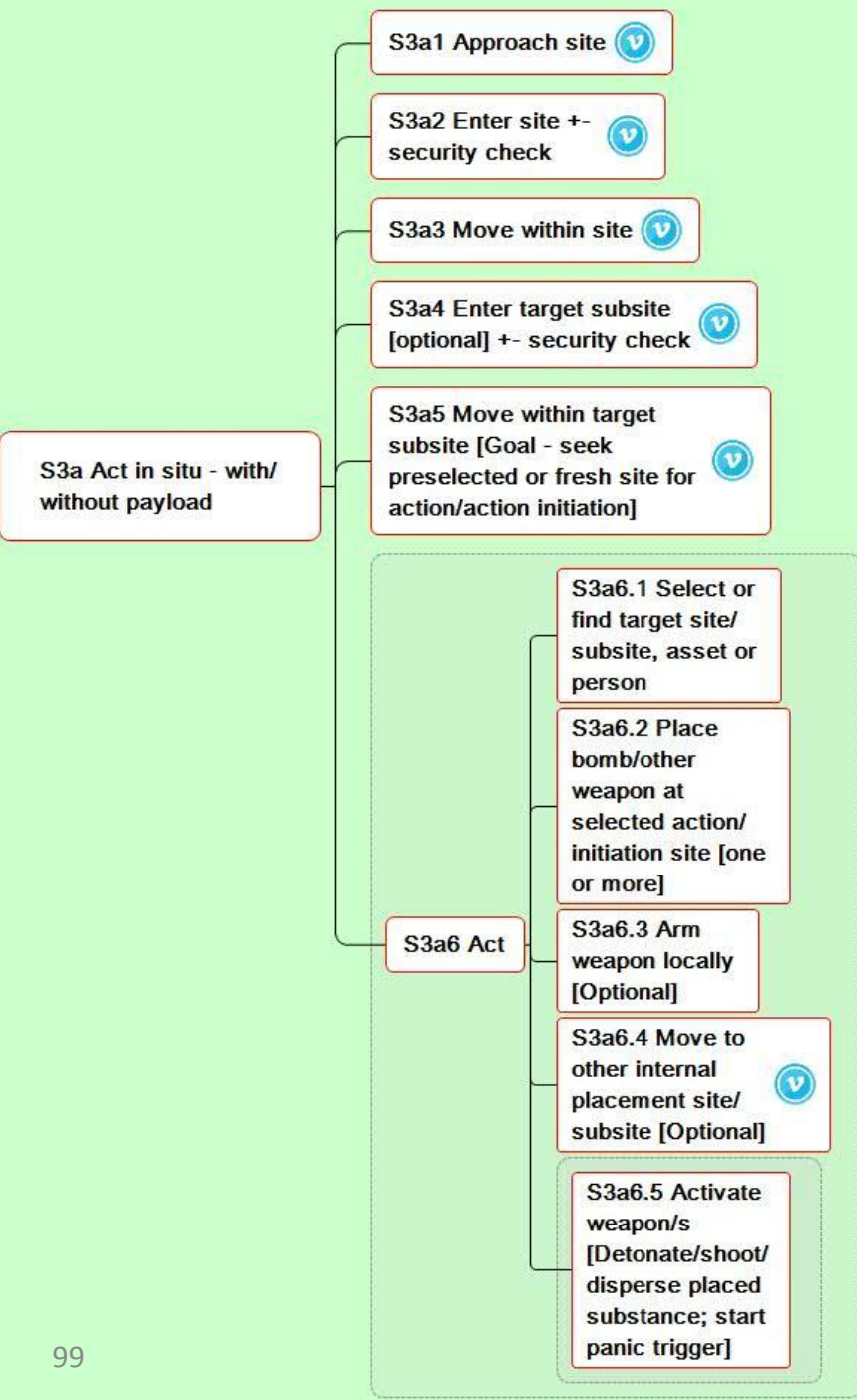


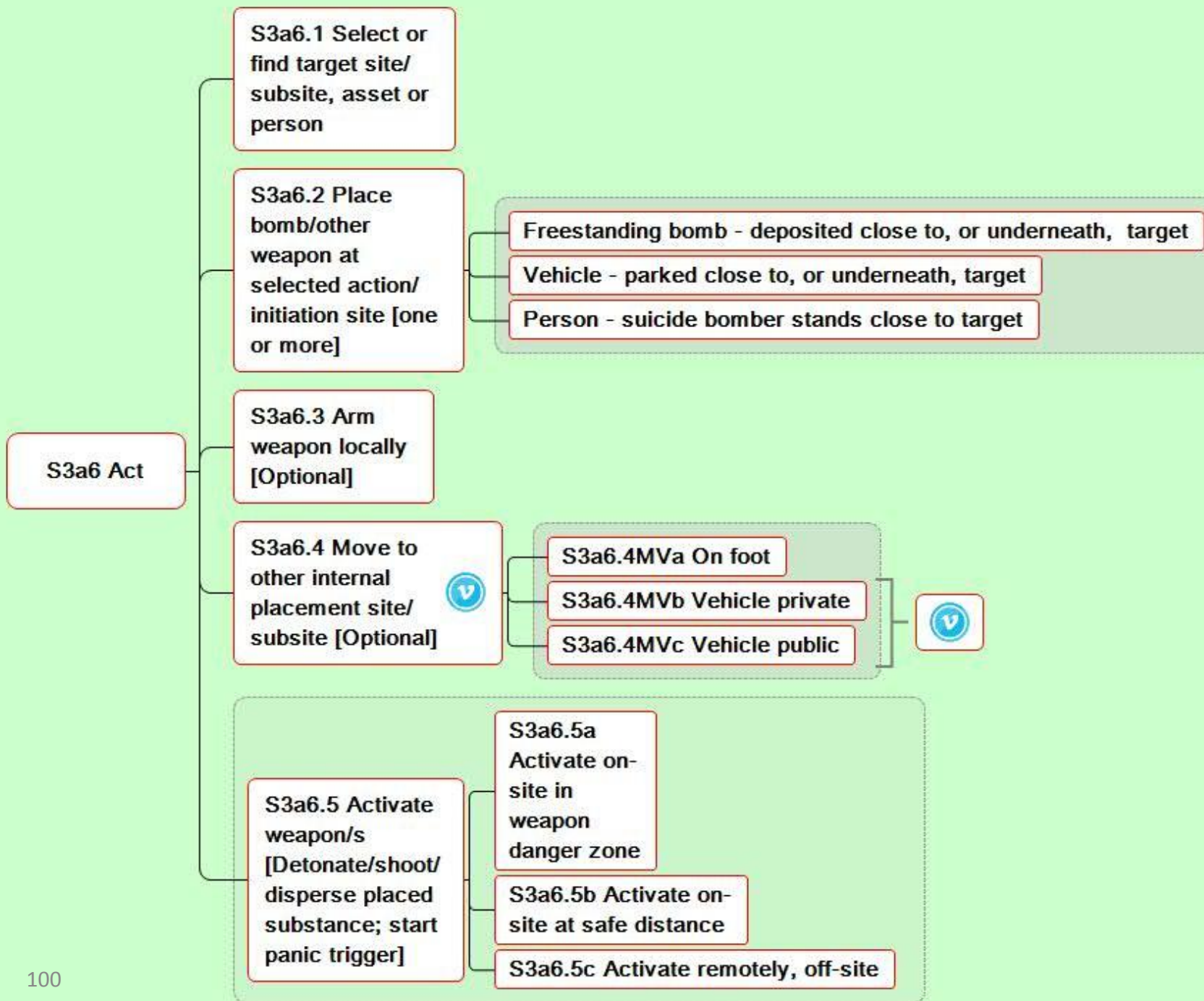
This Vehicular and other movements list subsequently abbreviated



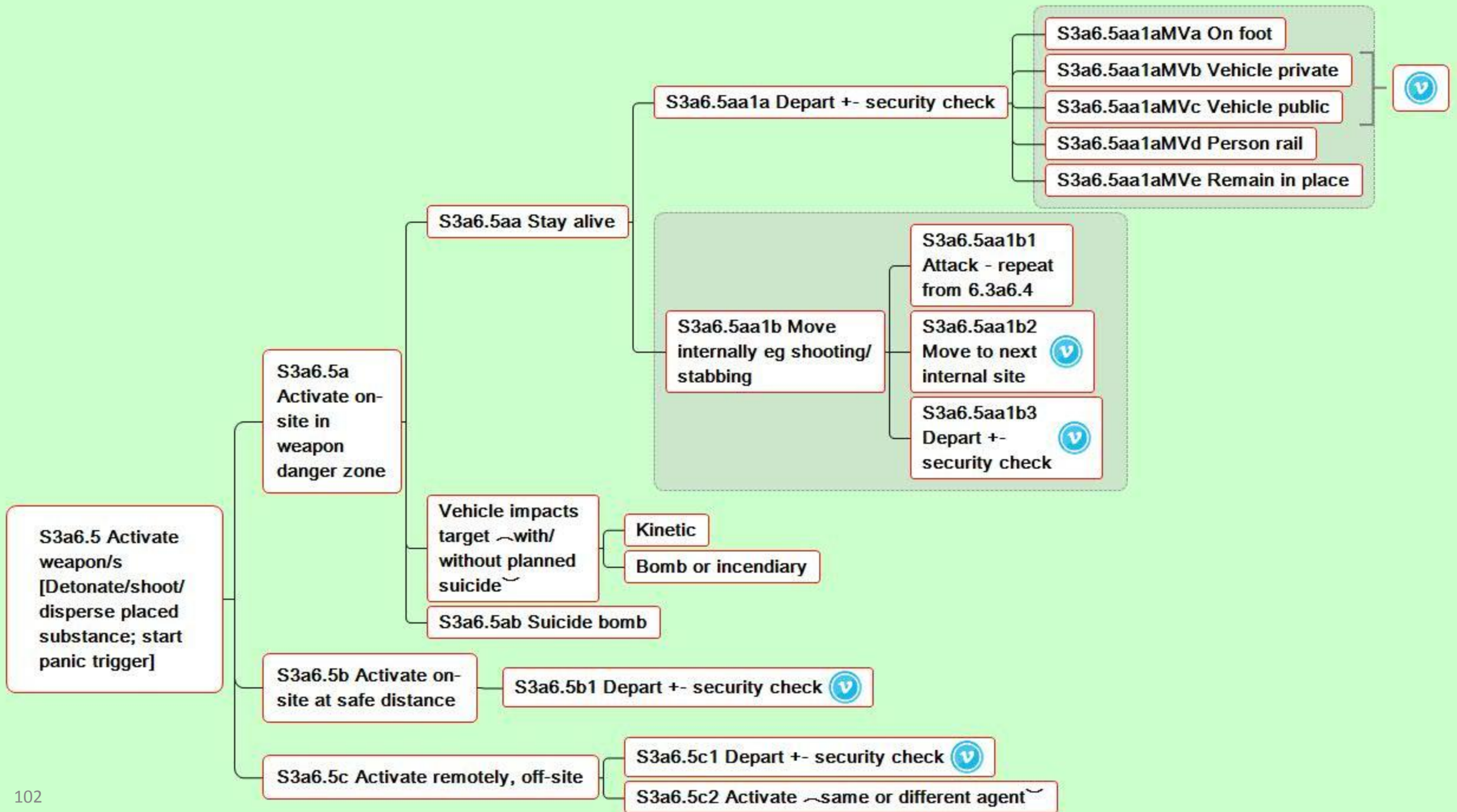


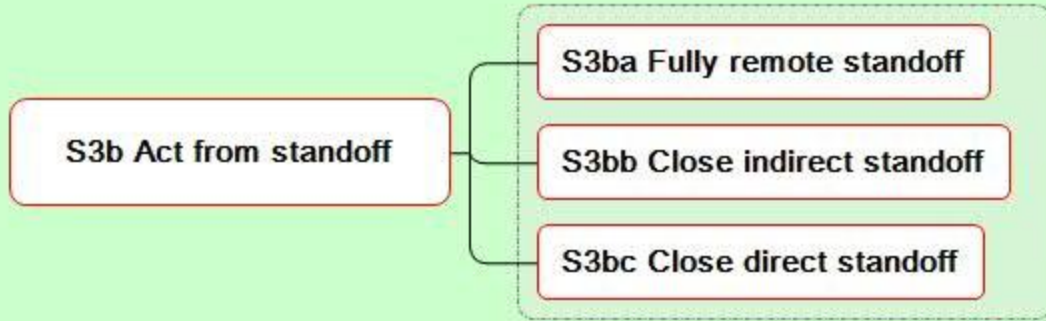


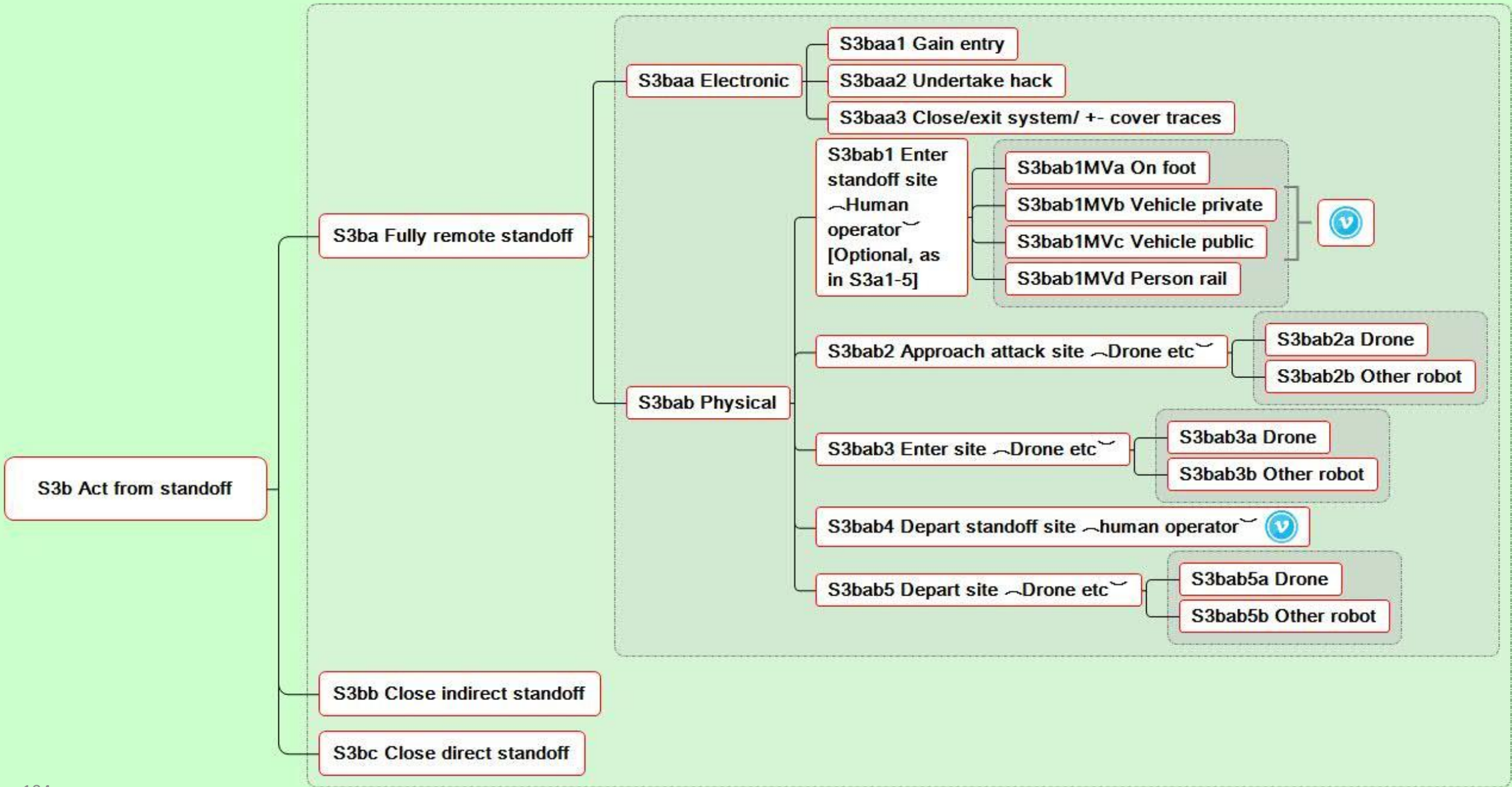


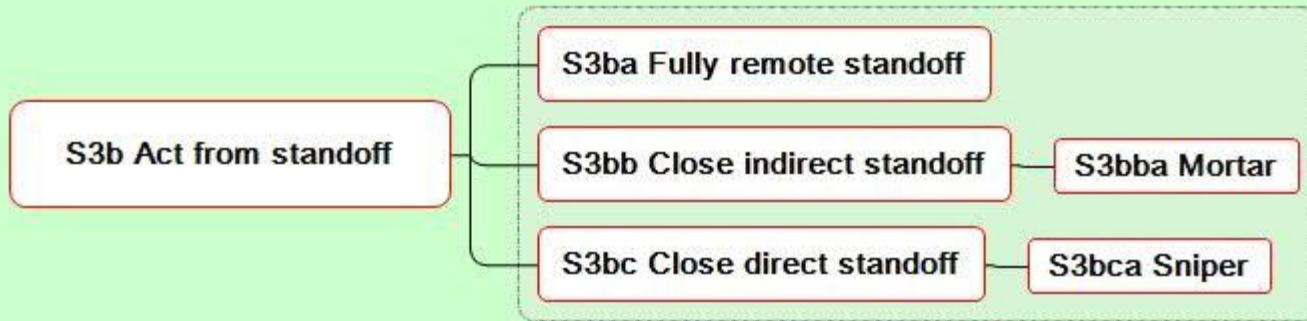


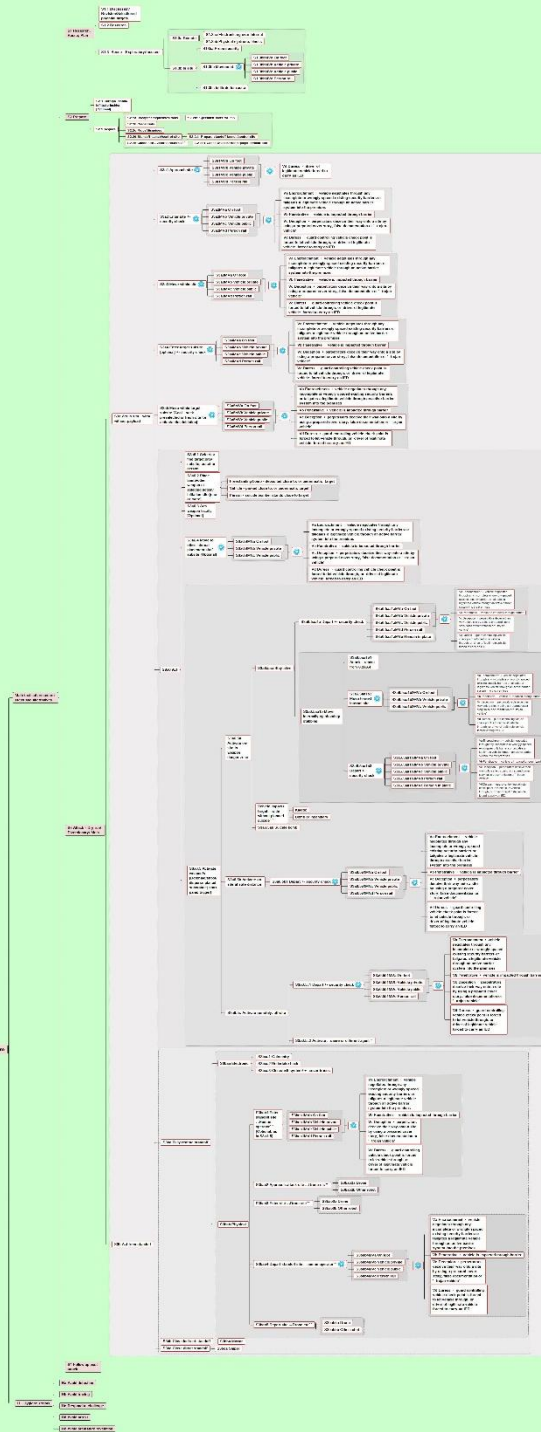










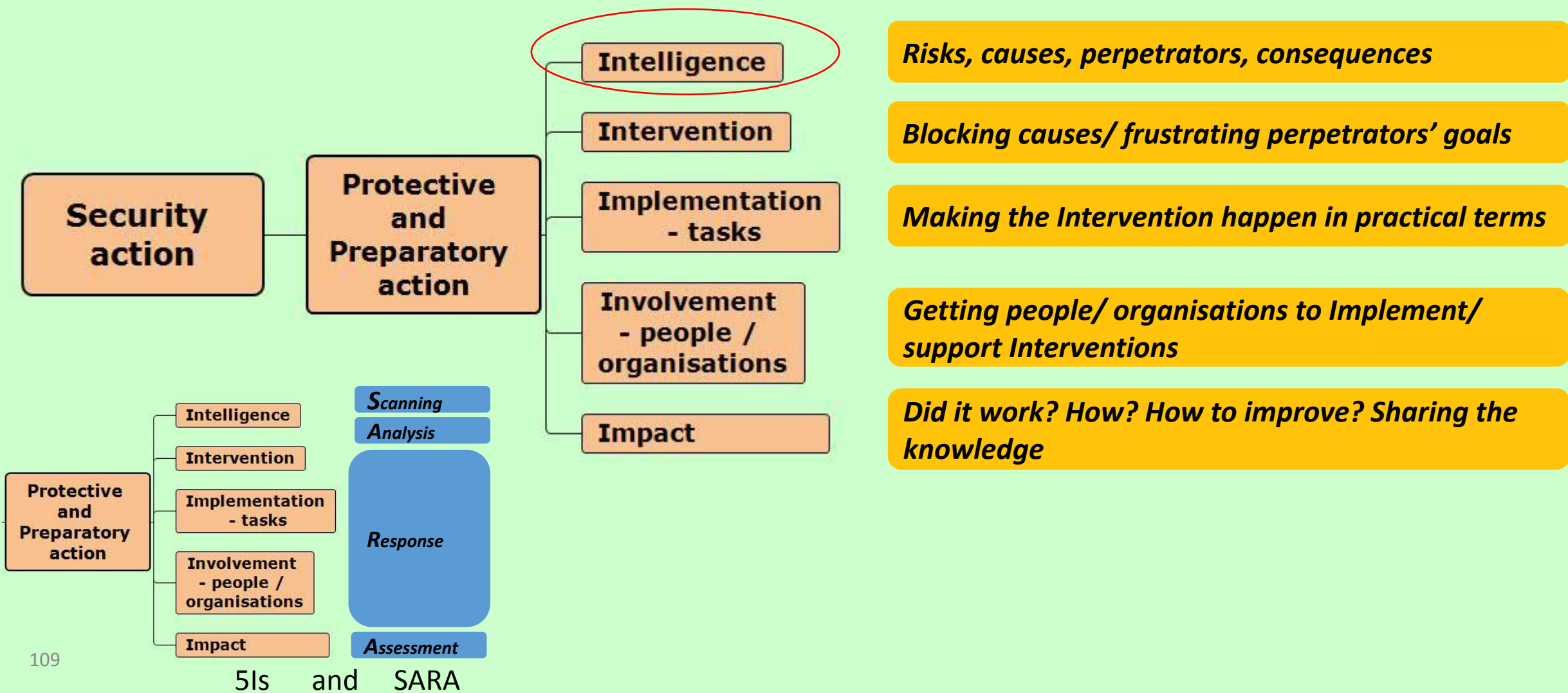


Security Action – framework and findings

Based on the 5Is, CTO, CPTED and a range of other crime science frameworks

**Security
action**

**Protective
and
Preparatory
action**



Intelligence

**General social/geographical
context of the terrorism problem**

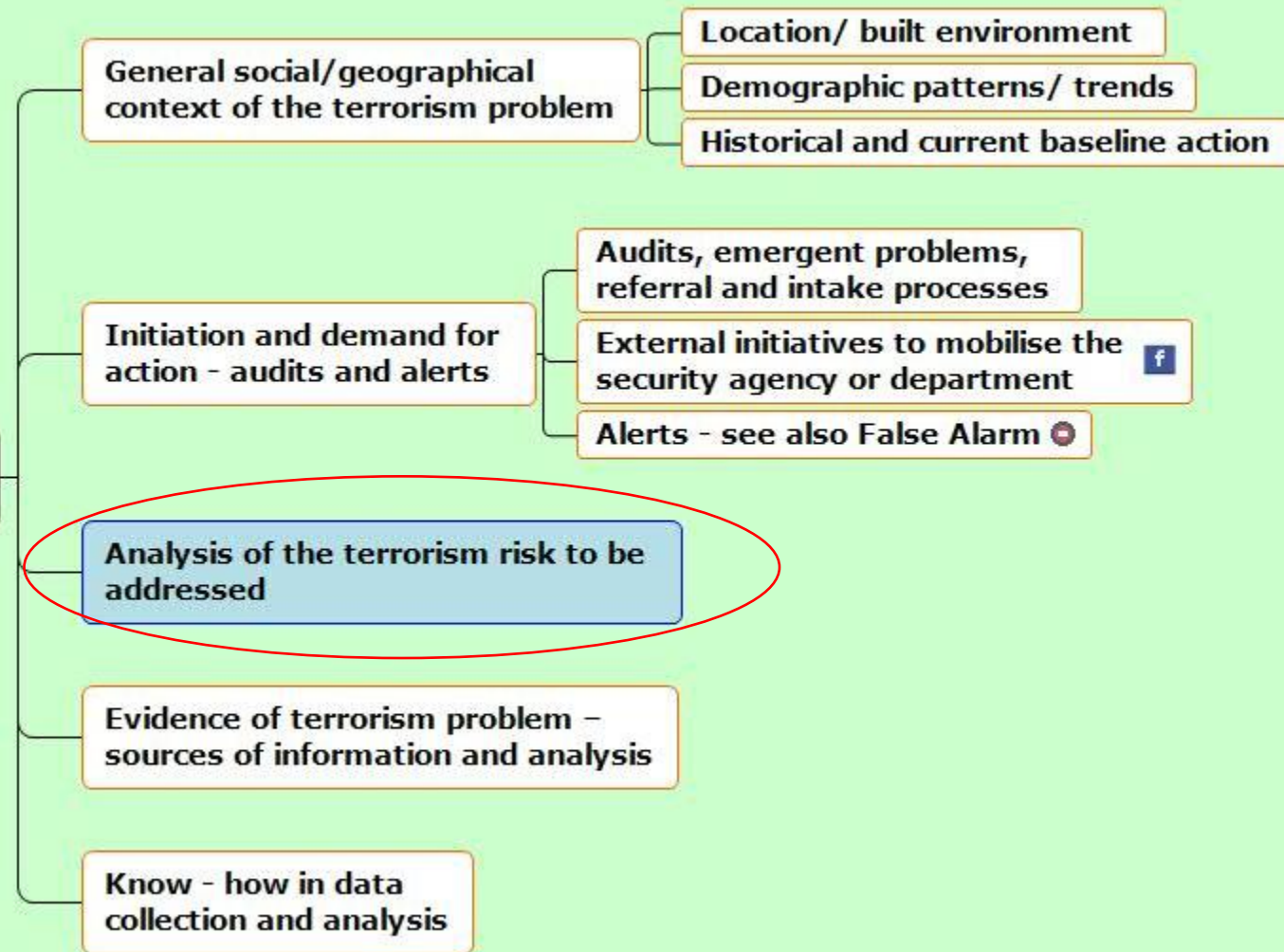
**Initiation and demand for
action - audits and alerts**

**Analysis of the terrorism risk to be
addressed**

**Evidence of terrorism problem –
sources of information and analysis**

**Know - how in data
collection and analysis**

Intelligence



Analysis of the terrorism risk to be addressed

Aspects of terrorist problem, pattern of risk and its context

Types of perpetrators

Modus Operandi - see Tactical Attack Methods & Attack Procedures

Target property damaged - see Tactical Attack Methods

Target premises - see Tactical Attack Methods

Target persons/ organisations - see Tactical Attack Methods

Owners/ managers of property/ premises - see role analysis

Immediate physical and social context of event/s

Wider physical and social context of event/s

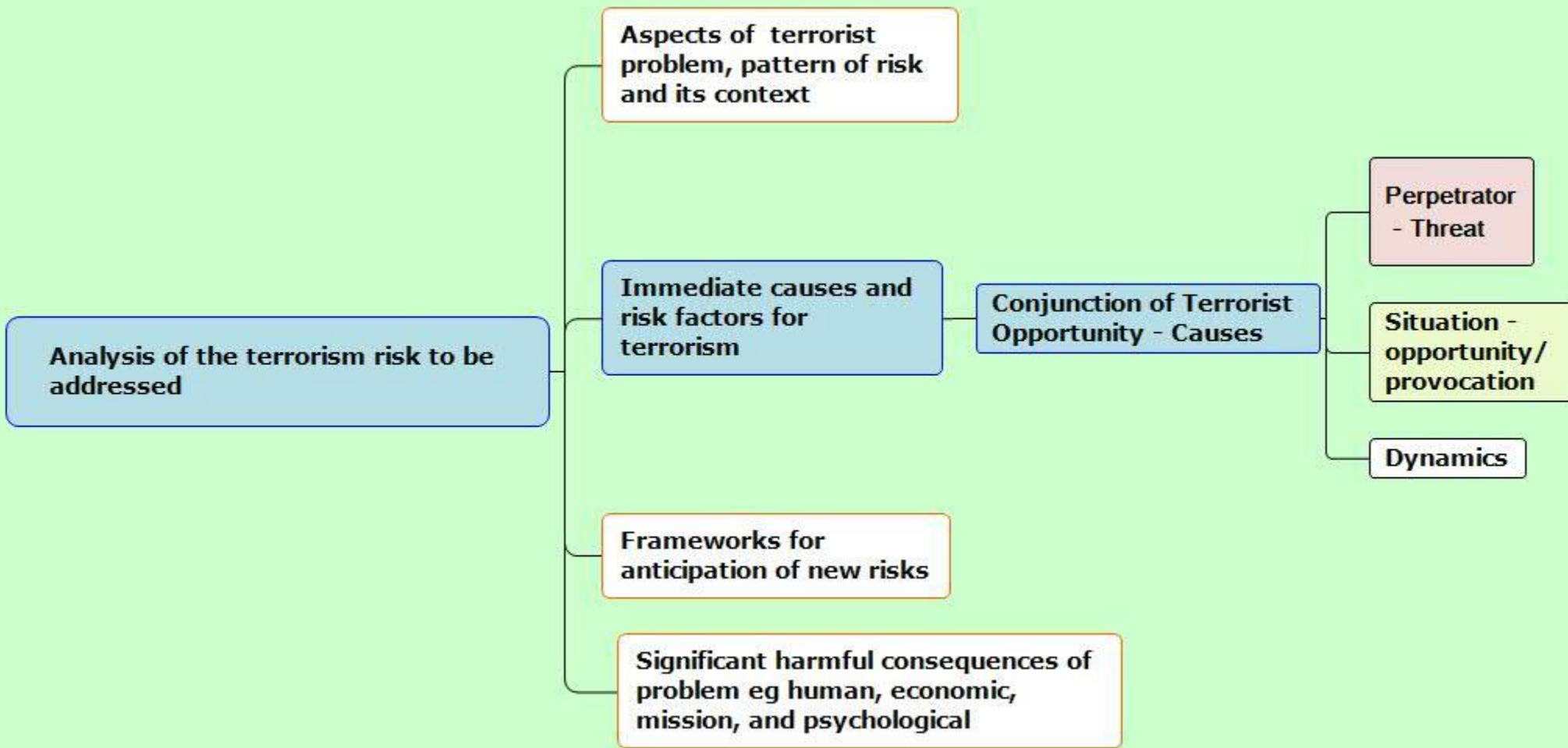
Timing of events during day, week or year

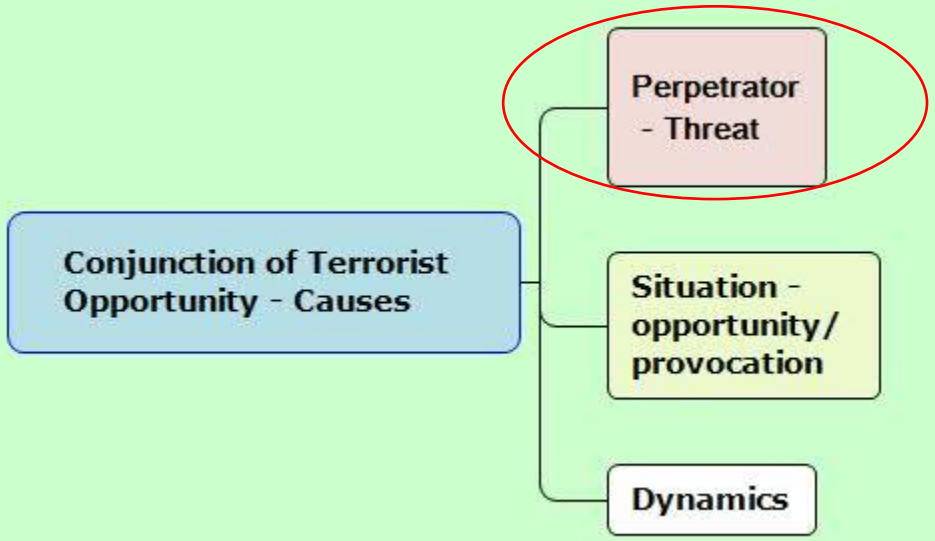
Whether crime problem recent or of long-standing

Immediate causes and risk factors for terrorism

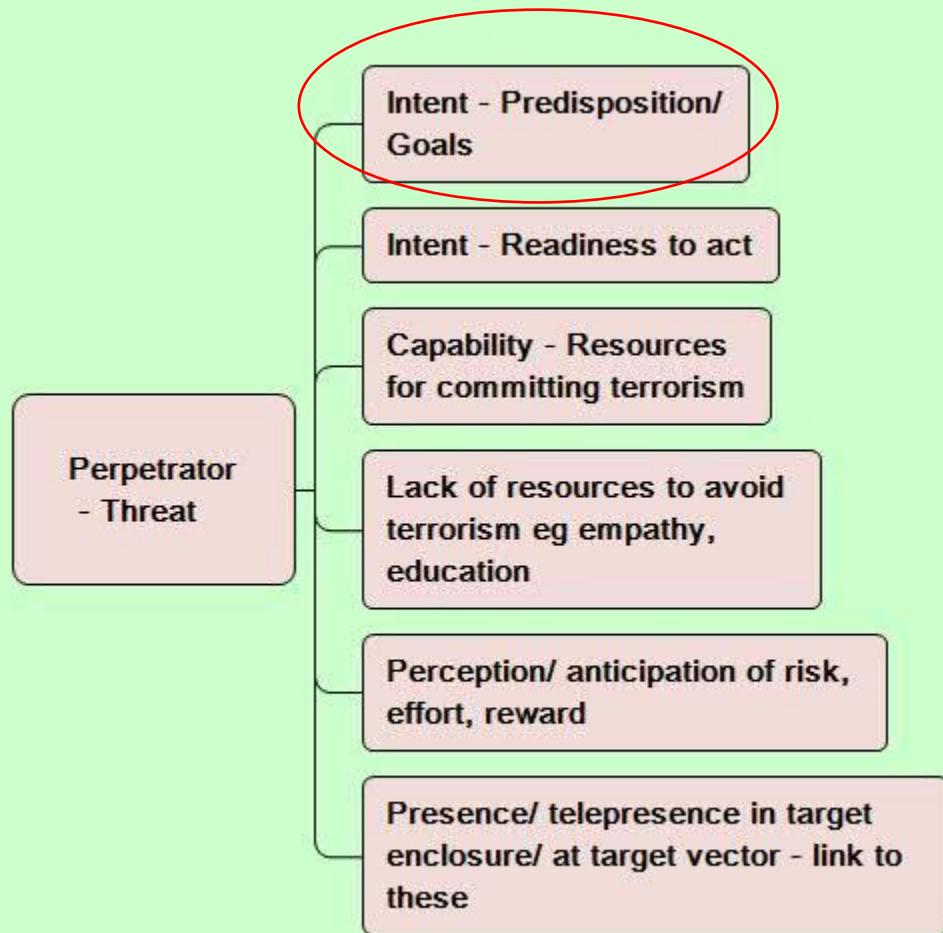
Frameworks for anticipation of new risks

Significant harmful consequences of problem eg human, economic, mission, and psychological

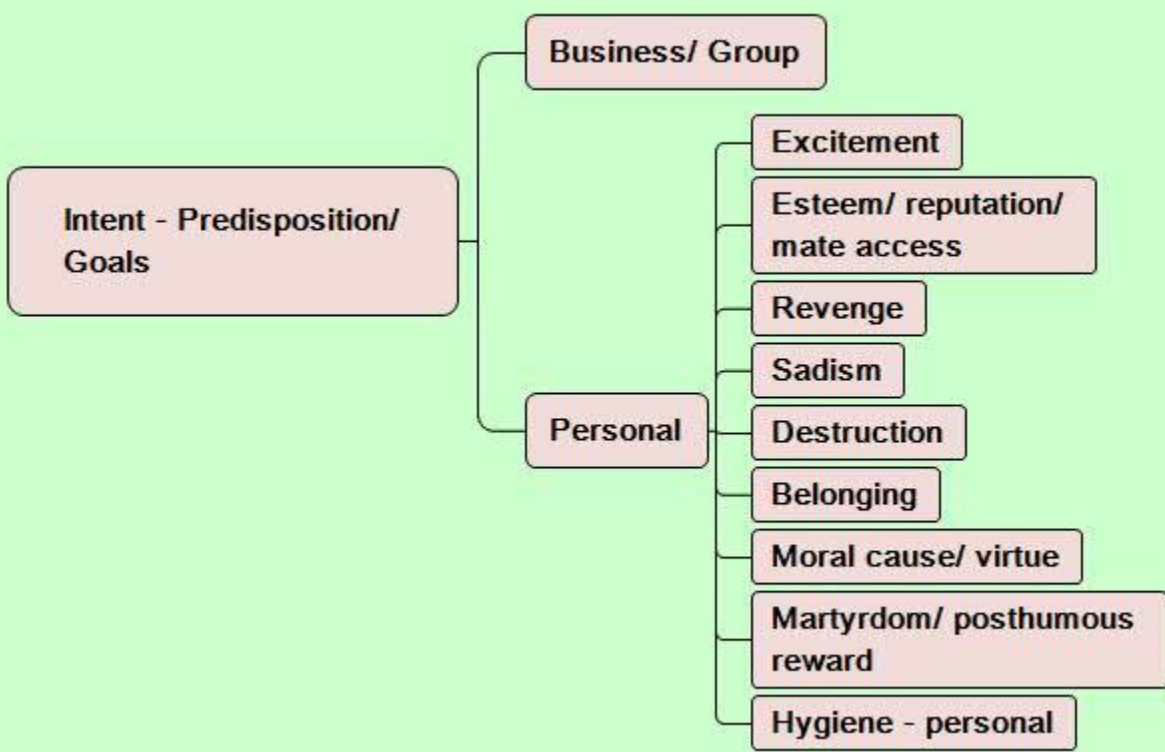




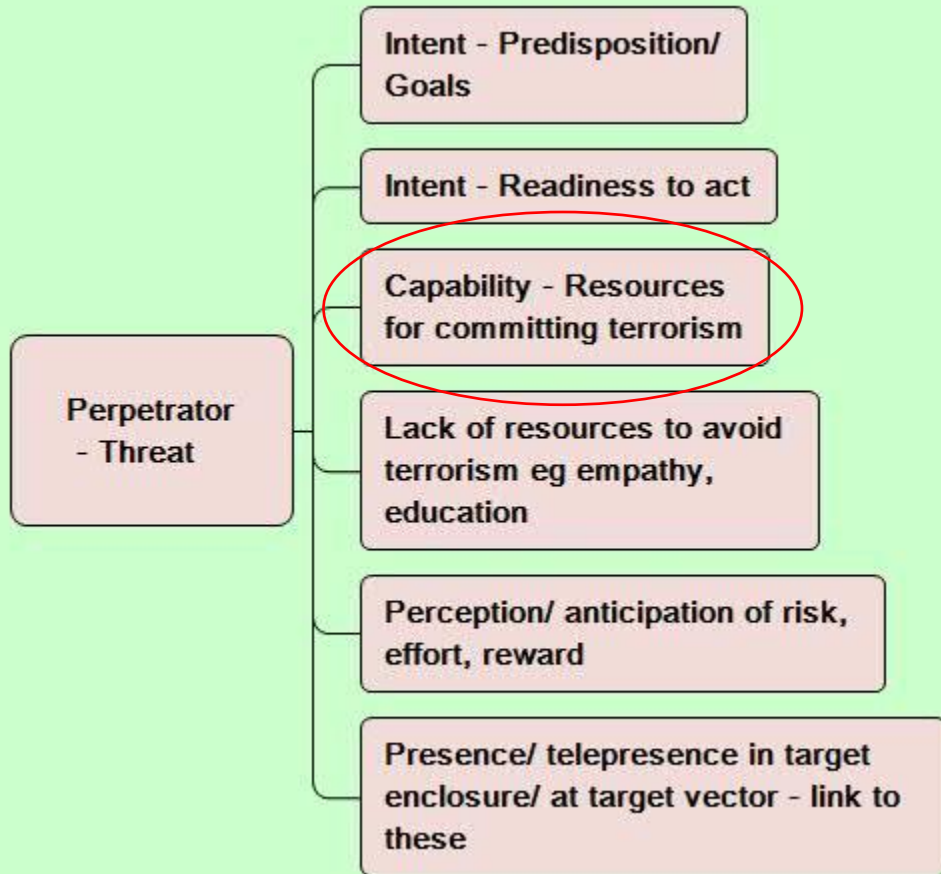
Think Perpetrator

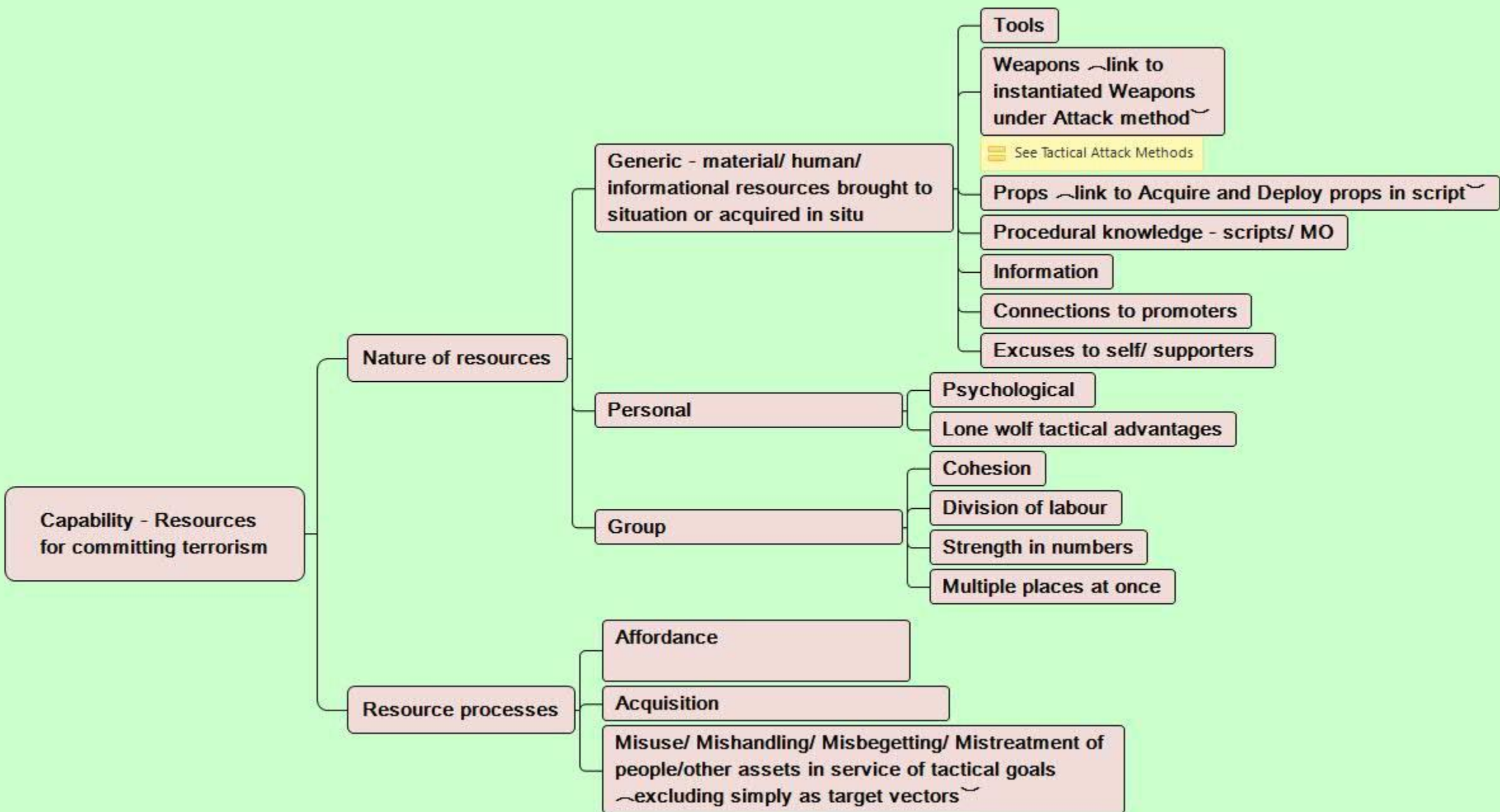


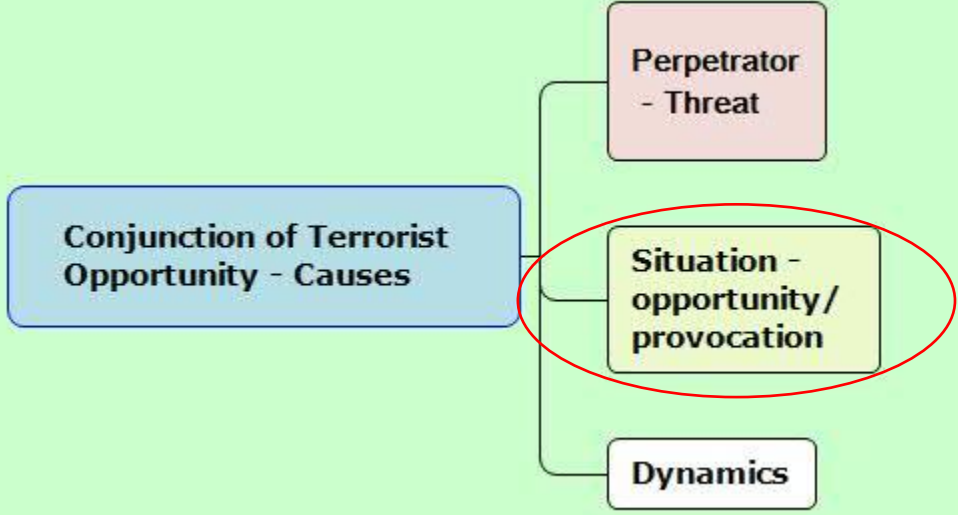




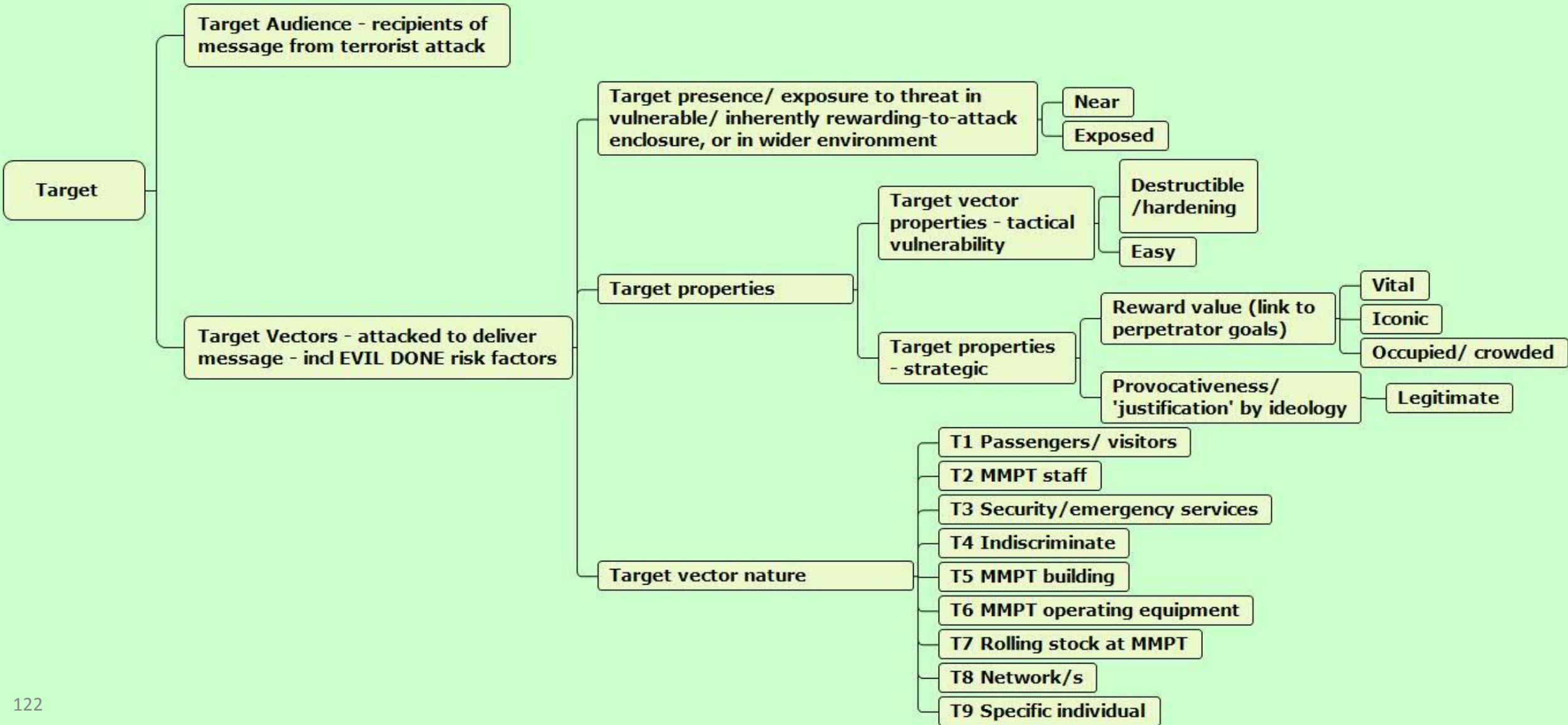
Think Perpetrator



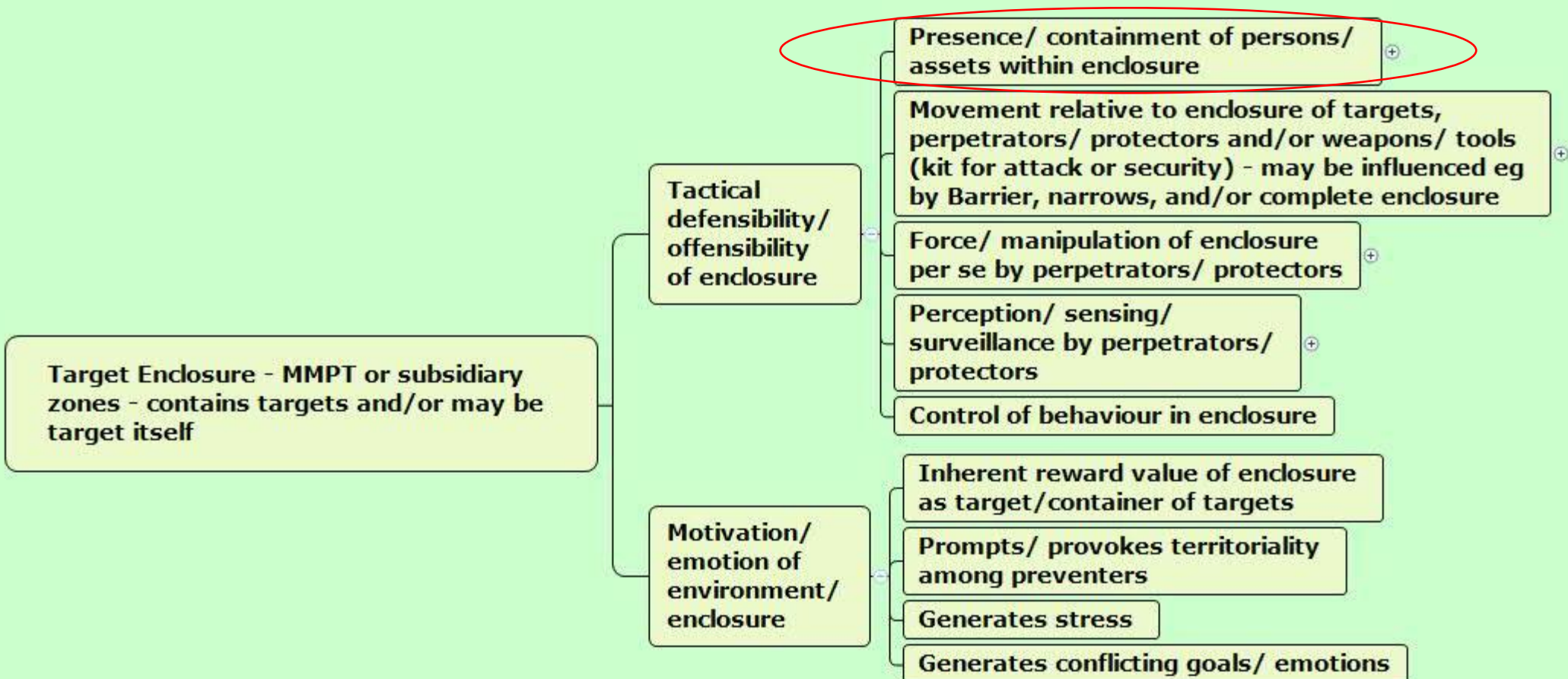


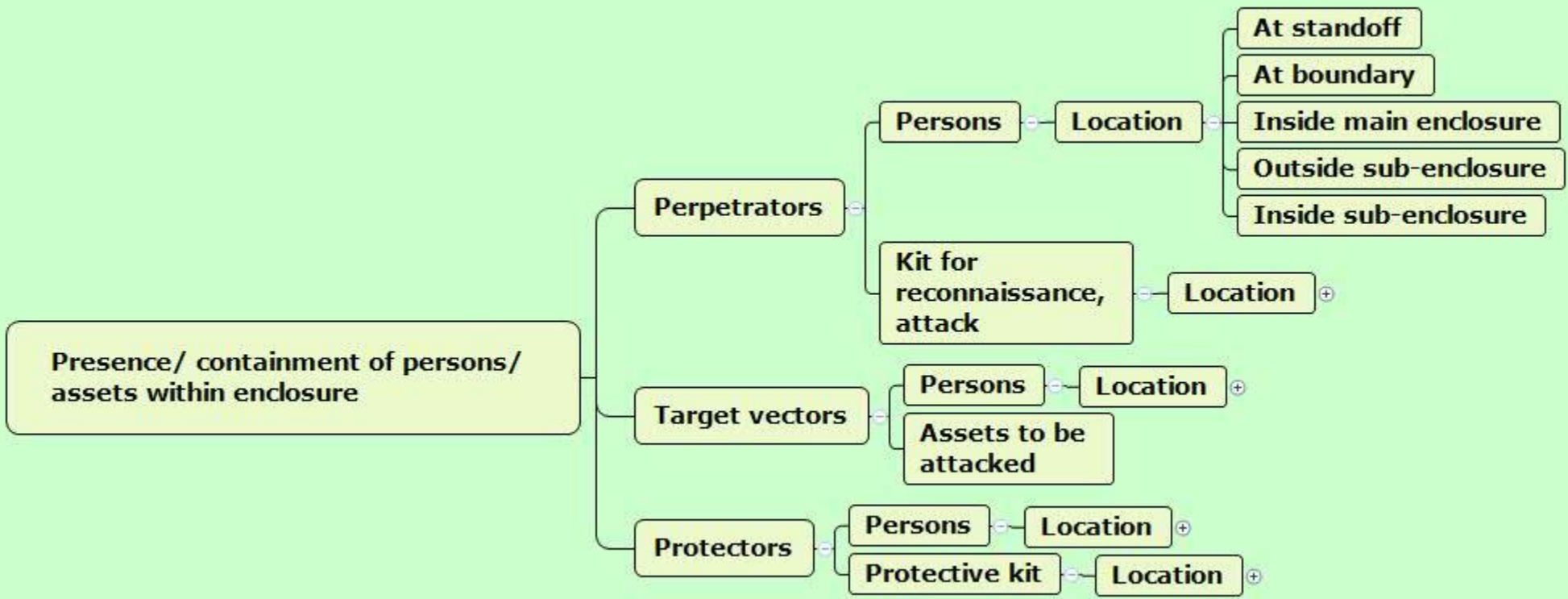


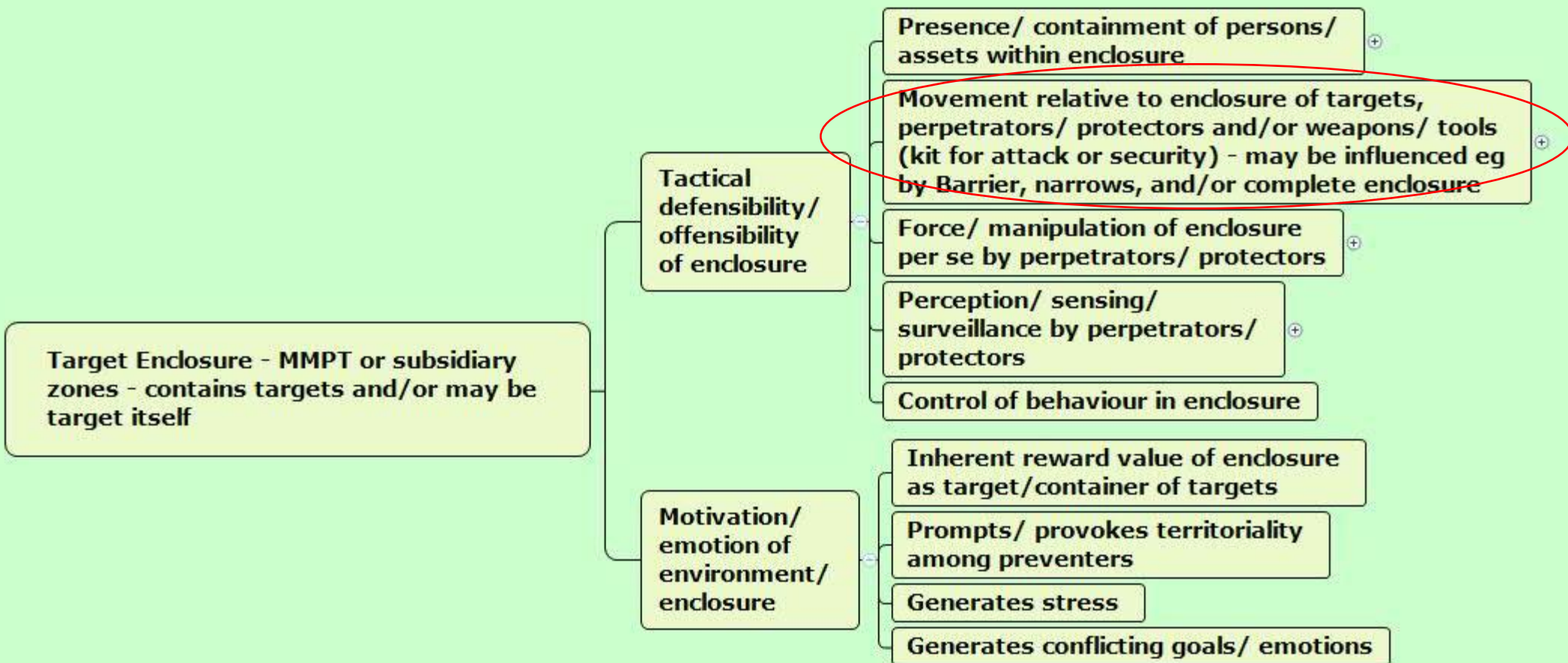


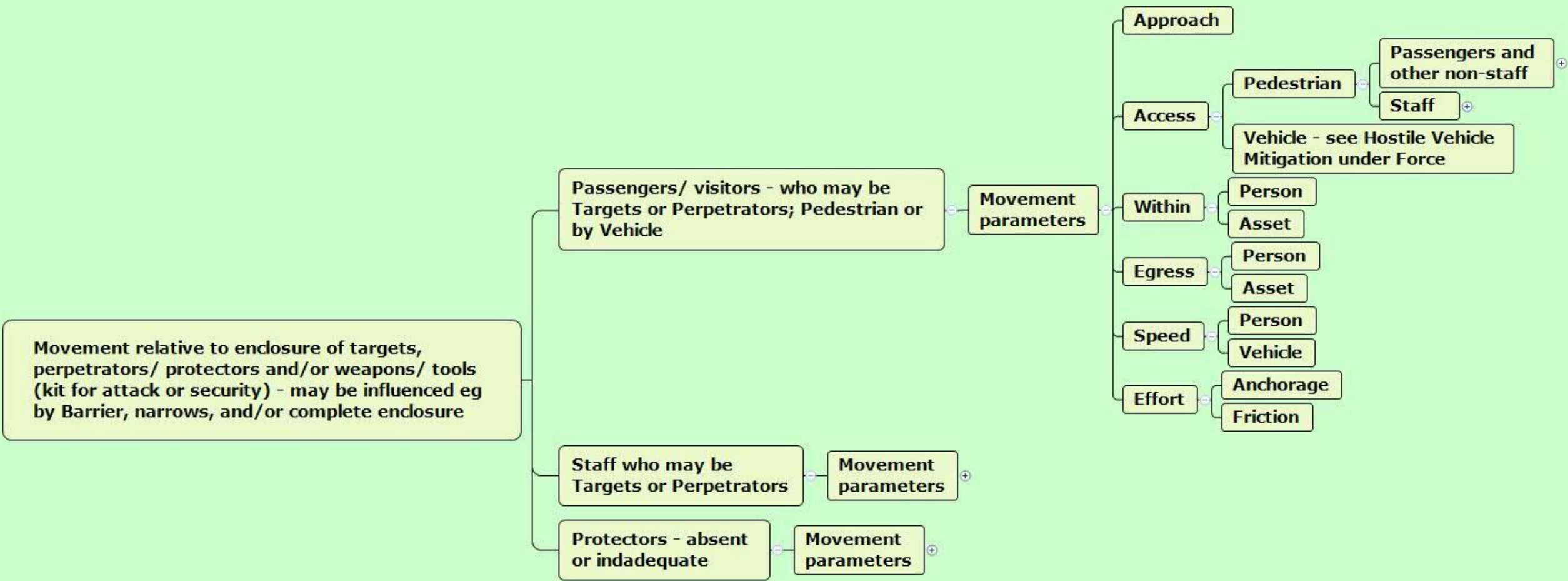


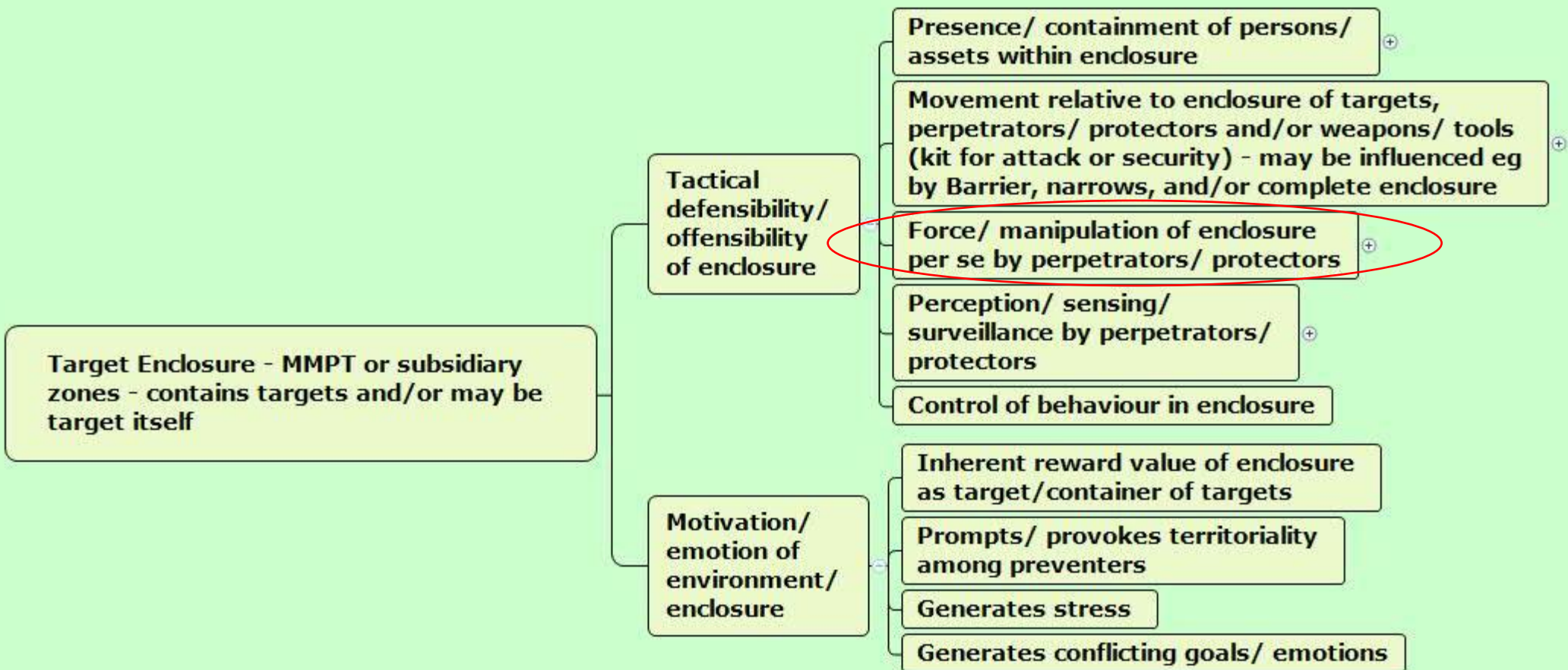


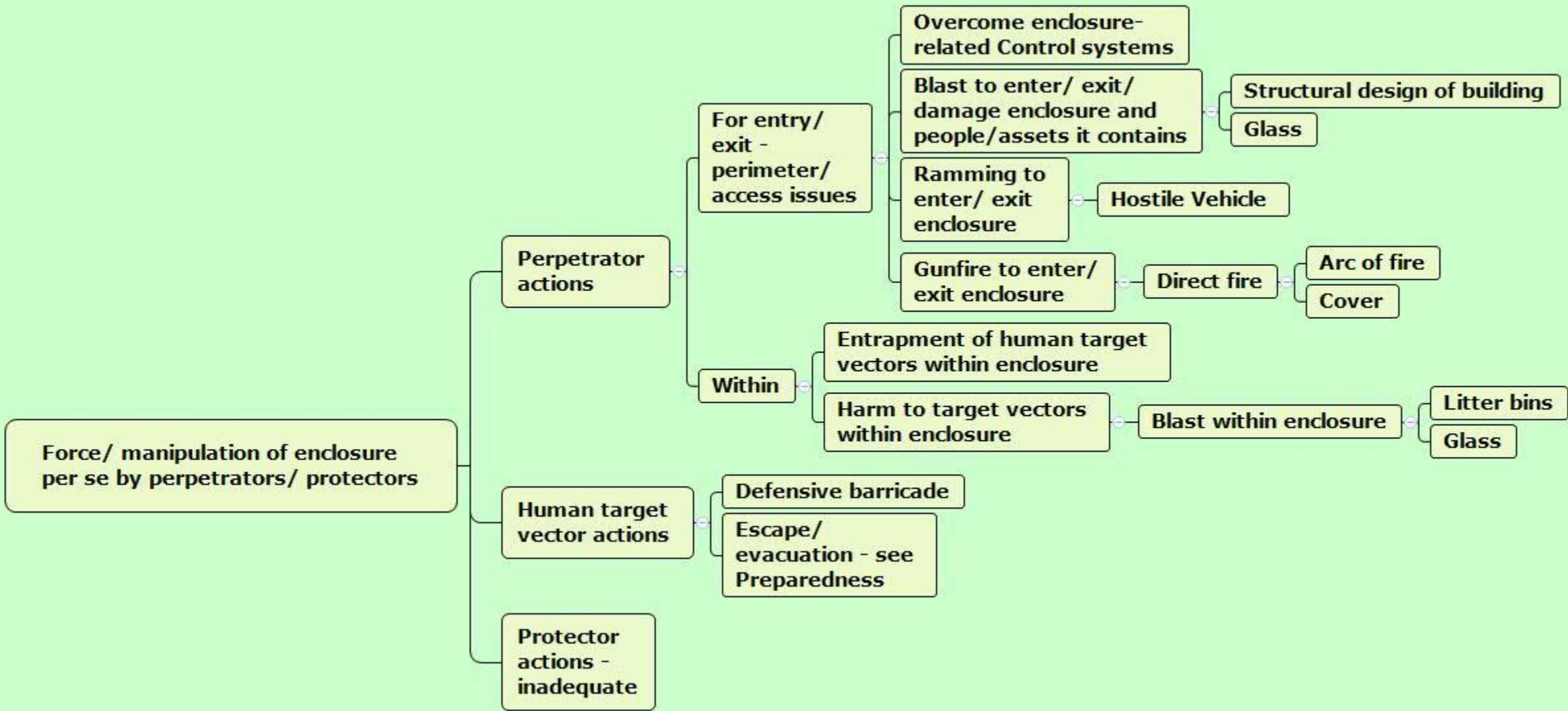


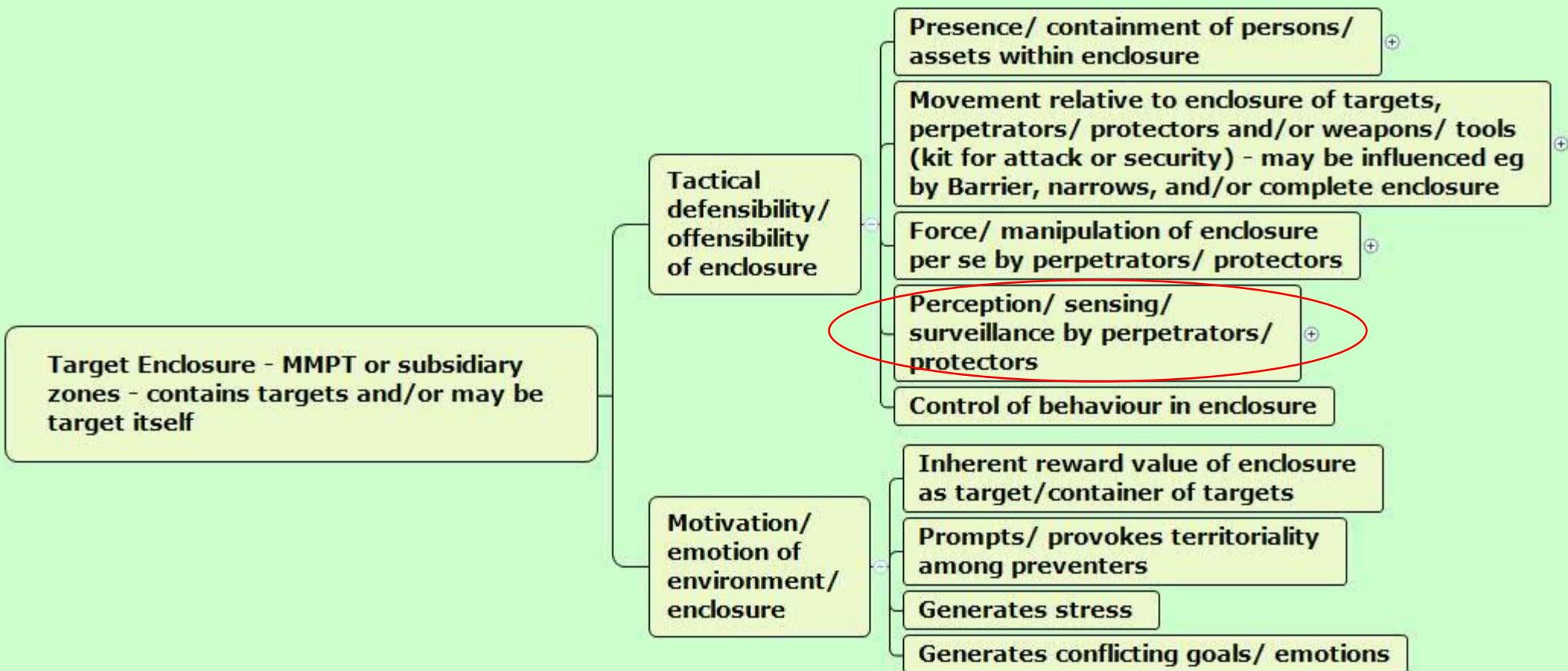












**Perception/ sensing/
surveillance by perpetrators/
protectors**

Sight

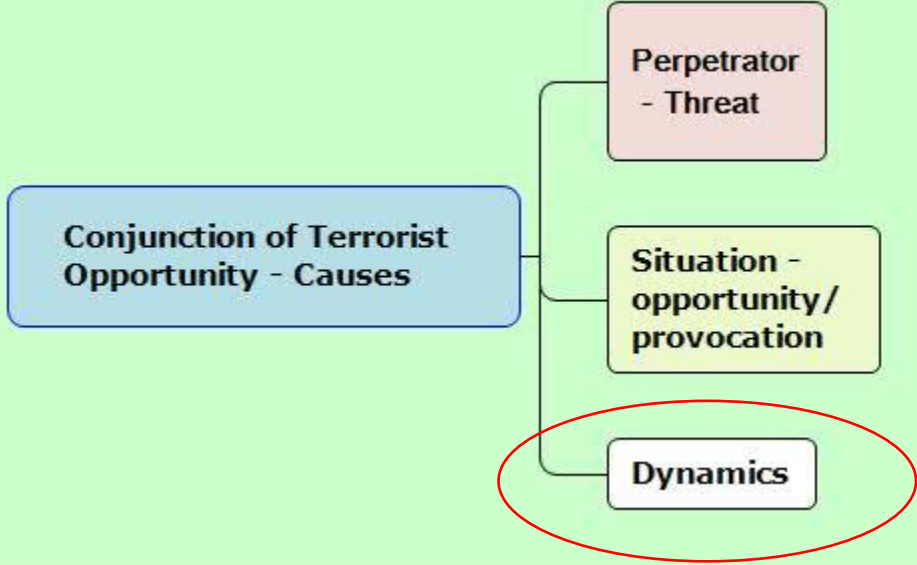
**Transparency of enclosure boundary/
internal walls**

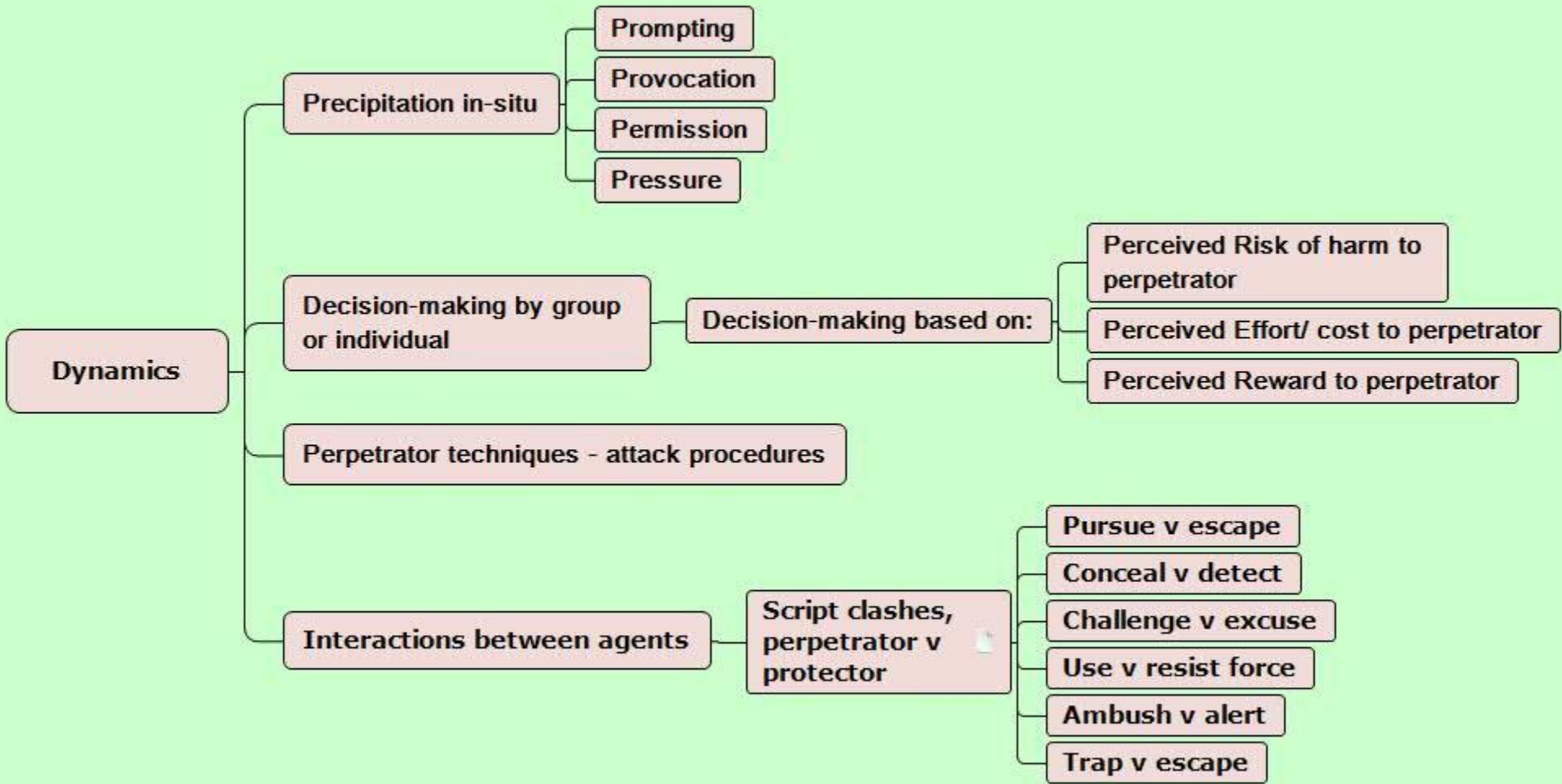
Sound

Audibility outside enclosure from inside

Audibility within enclosure from outside

**Screening technologies/ procedures -
entering/ within/ leaving enclosures**







**Frameworks for
anticipation of new risks**

Generic crime/terrorism risks
- Conjunction of Terrorist
Opportunity can be used to
structure future risks

**Specific risks of
involvement in crime/
terrorism of new
products, procedures,
places, systems -
Misdeeds & Security**

Misappropriation - theft

**Mistreatment - harm -
damage or or injury**

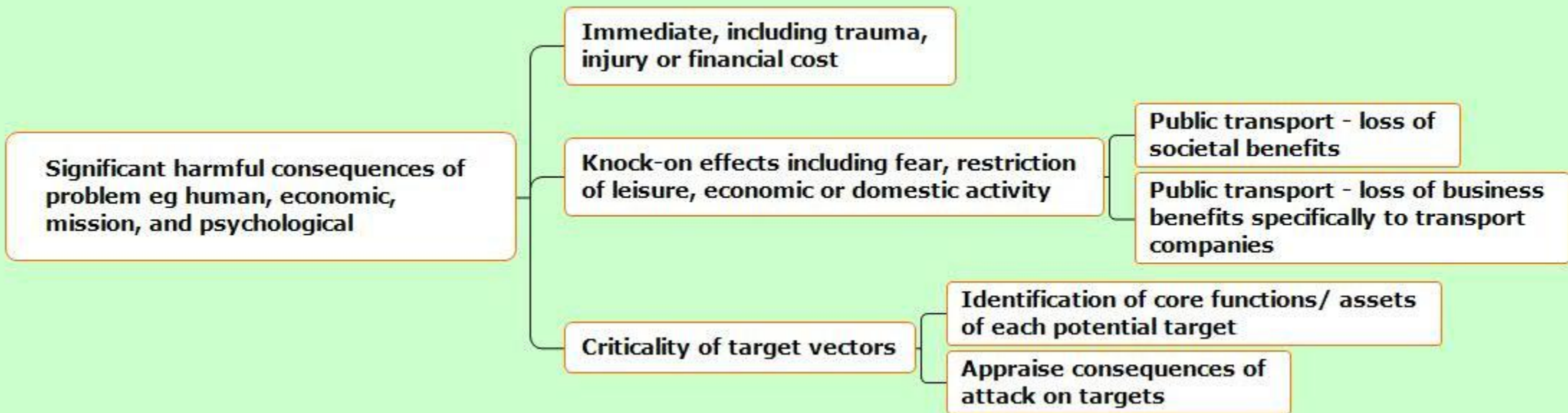
Misbegetting - counterfeit

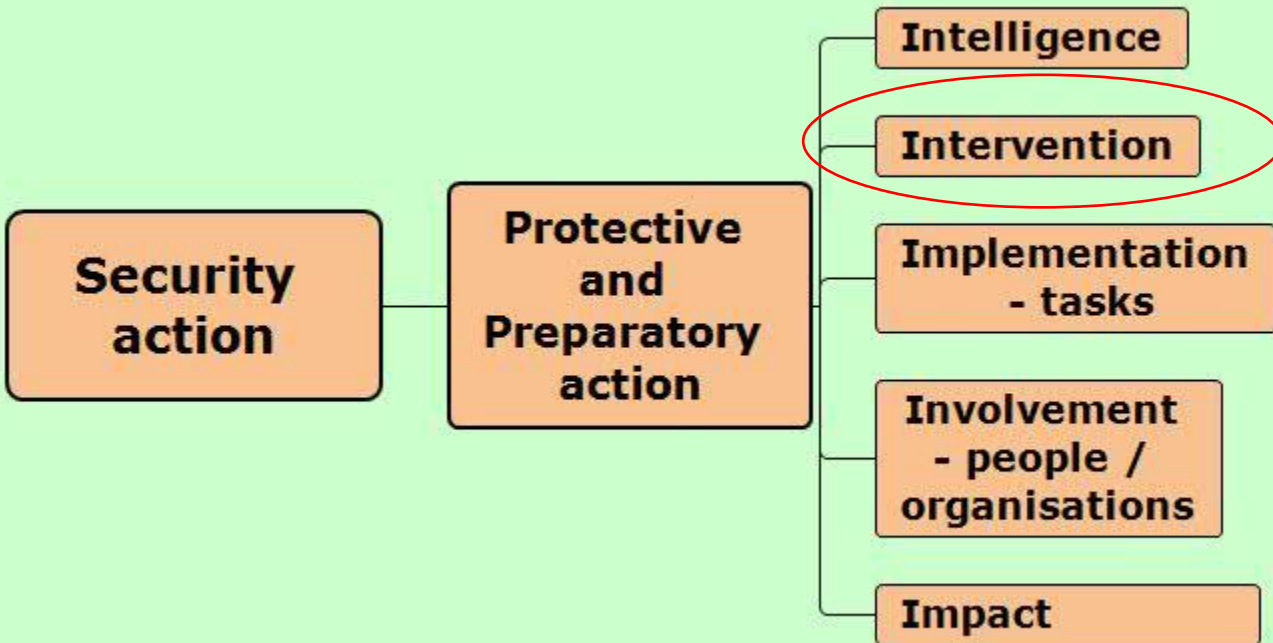
**Mishandling - smuggling, ID
alteration**

Misuse - as tool or weapon

Misbehaviour - disorder

**Mistake - false
alarm, false arrest**



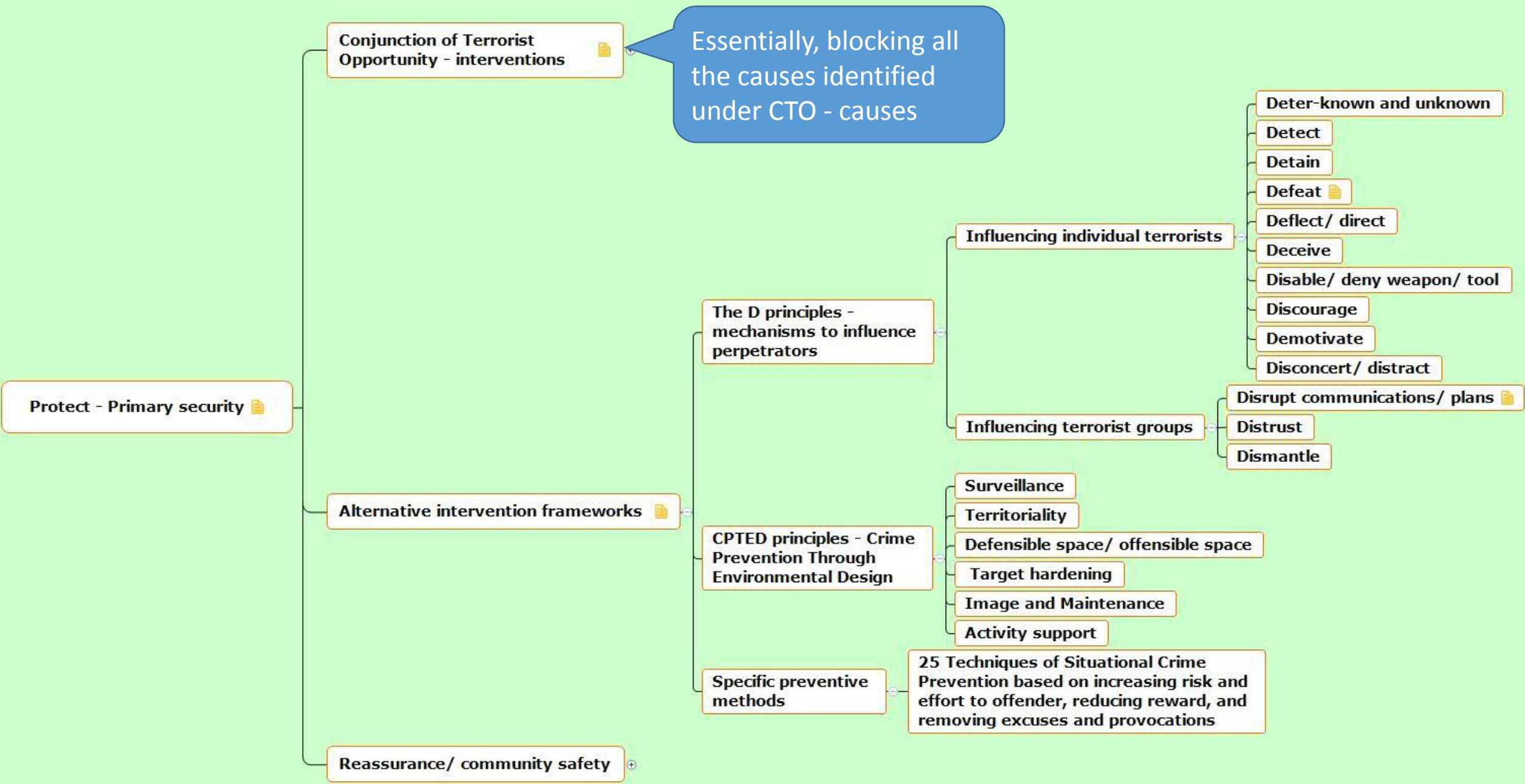


Intervention

Protect - Primary security 📄

Prepare in advance of attack 📄

Prepare for recovery (not covered here)



Intervention

Protect - Primary security 📄

Prepare in advance of attack 📄

Prepare for recovery (not covered here)

Prepare in advance of attack 📄

Secondary security - Prepare for response during attack or suspected hostile reconnaissance/ dry run

Tertiary security - Prepare for response immediately after attack

Prepare for response - general - must be robust to survive attacks

Secondary security - Prepare for response during attack or suspected hostile reconnaissance/ dry run

**Prepare for detection/
reporting of incident - also
relevant to Protection**

Detect by unusual movements

**Address false
alarms - see also
Alerts**

Prepare to resist incident

Lockdown full/partial

Structural design of building 

**Prepare to limit immediate
harm from attack**

Fire alarm/response 

Prepare in advance of attack 📄

Secondary security - Prepare for response during attack or suspected hostile reconnaissance/ dry run

Tertiary security - Prepare for response immediately after attack

Prepare for response - general - must be robust to survive attacks

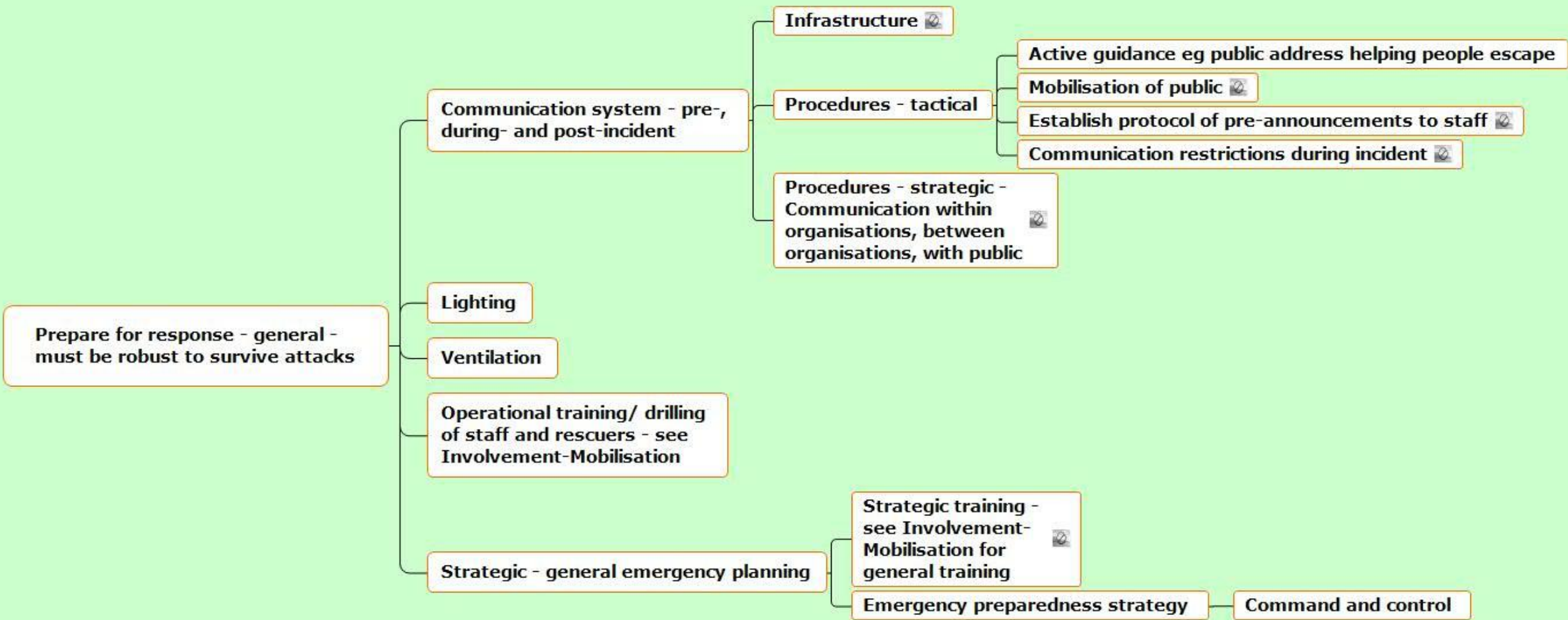


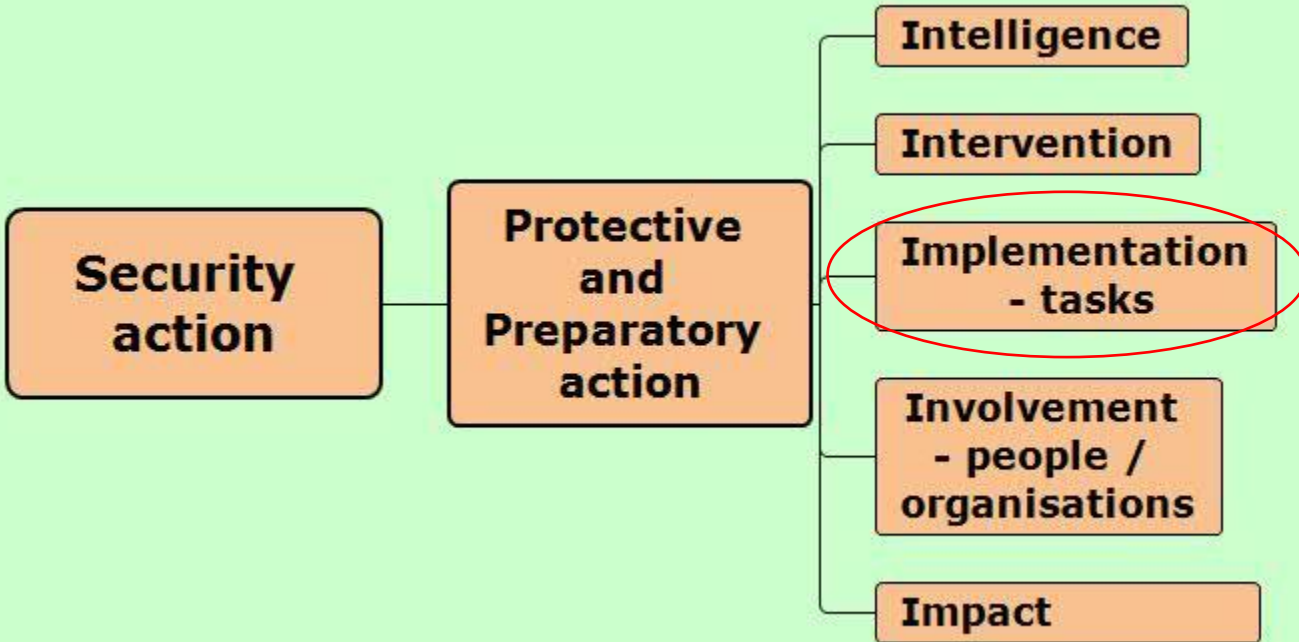
Prepare in advance of attack 📄

Secondary security - Prepare for response during attack or suspected hostile reconnaissance/ dry run

Tertiary security - Prepare for response immediately after attack

Prepare for response - general - must be robust to survive attacks





Implementation - tasks

Institutional/ organisational contexts

Mode of delivery of action

Targeting of action

Selection of interventions for identified threat/risk

Tailoring of action to context

Lifecycle/s of action

Basic execution process

**Management, planning,
organisational and governance issues**

Implementation - tasks


Institutional/ organisational contexts

Mode of delivery of action

Project

Service

Capacity-building only


Large/ special event 

Targeting of action

The problem, behaviour or condition tackled (see Objective under Intelligence)

Ecological level of action - whether it acts on individual people, places, communities

Targeting strategy

Basis of selection including risk & protective factors, known causes, risk patterns (of people, hot-spots etc), or needs - see also Intelligence 

Principle of selection - Universal, Selective (e.g. at risk) or Indicated (e.g. convicted offenders, repeat victims)

Coverage

Targeting issues

Selection of interventions for identified threat/risk

What works in this context

Cost - capital and running cost 

Implementability

Constraints/enablers

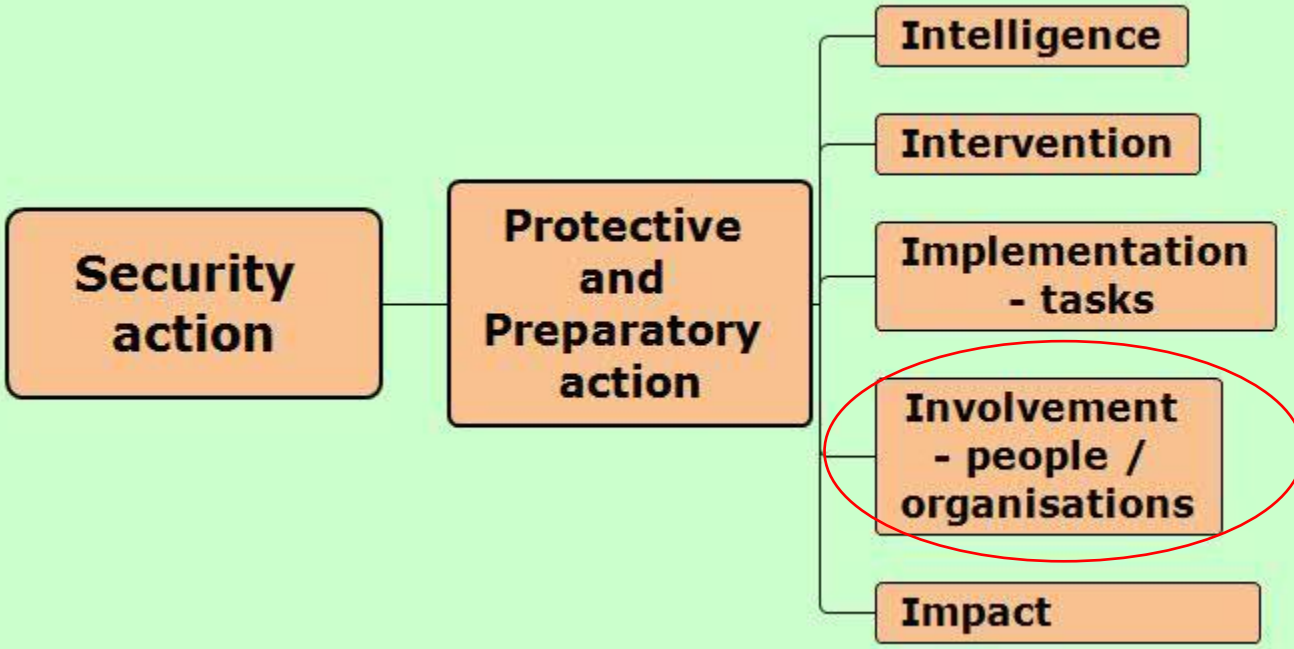
Robustness/ delicacy

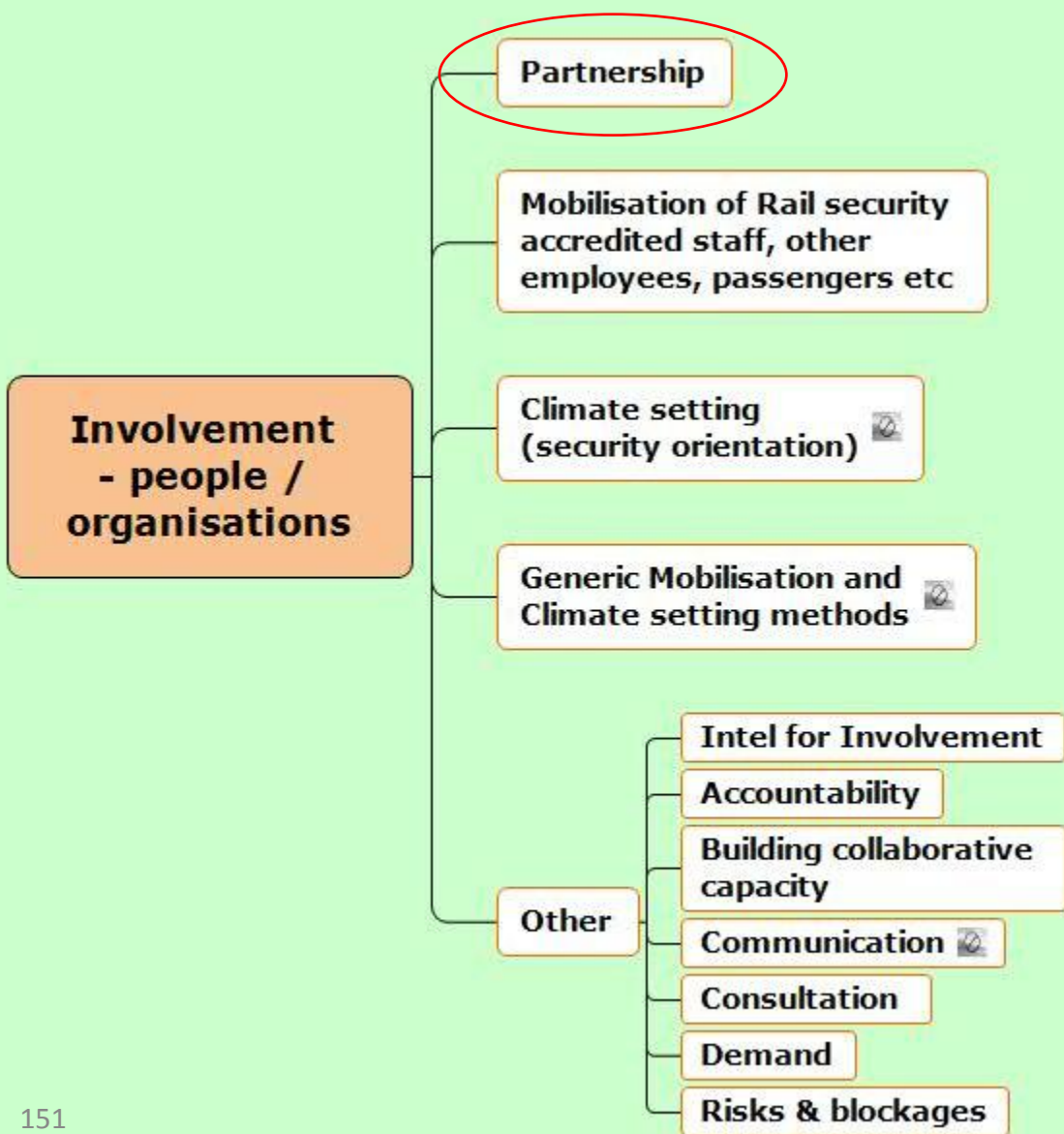
Tailoring of action to context

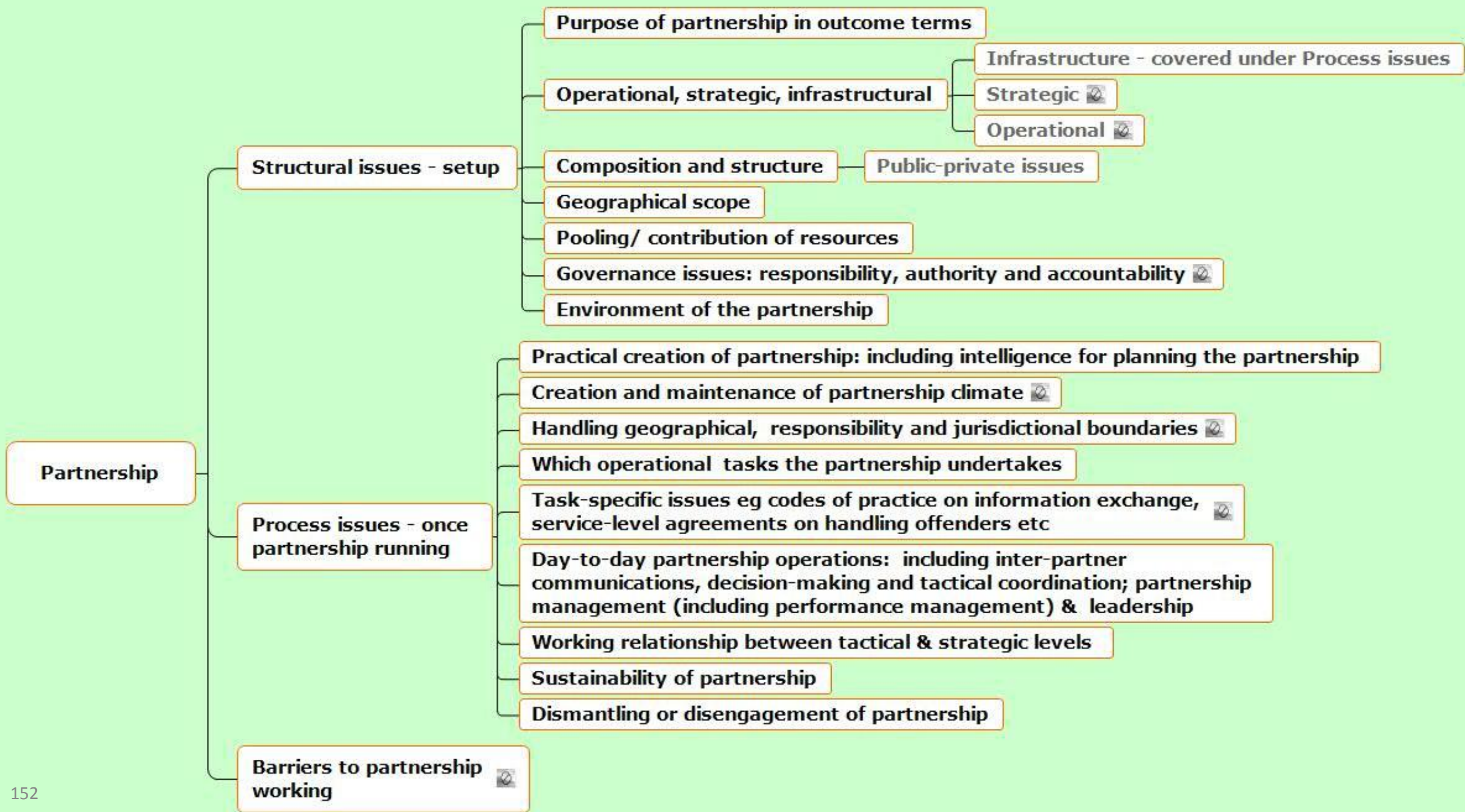
Lifecycle/s of action

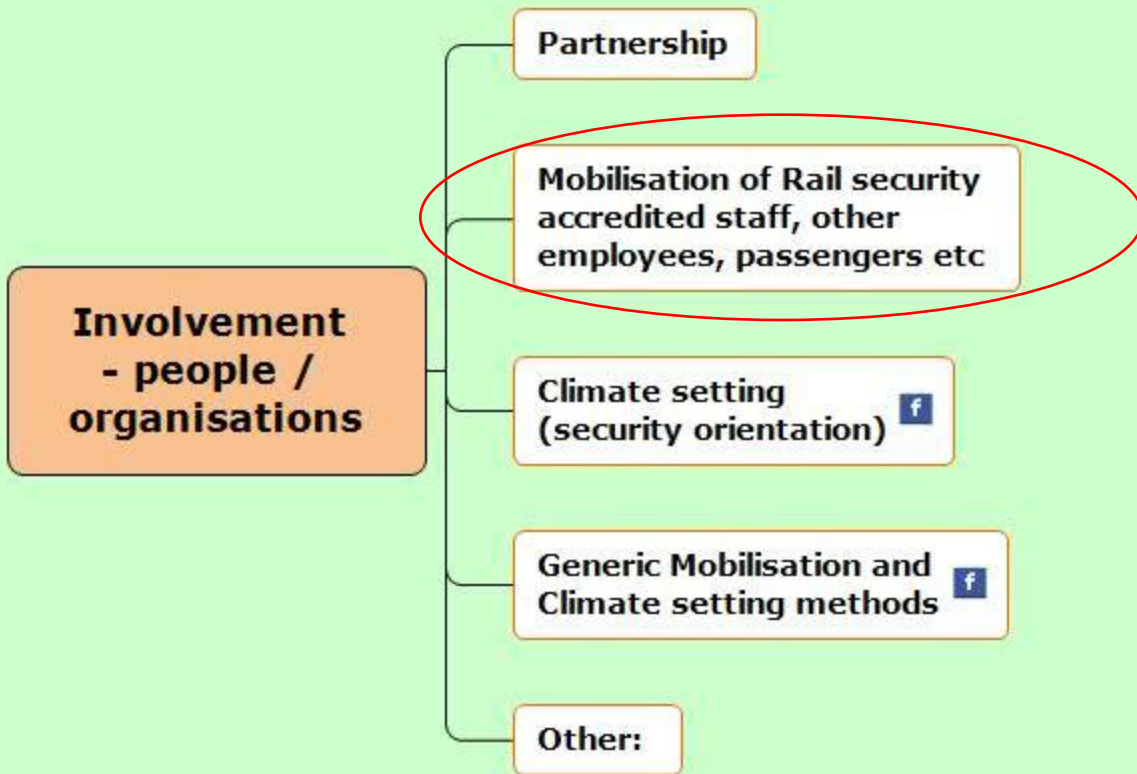
Basic execution process

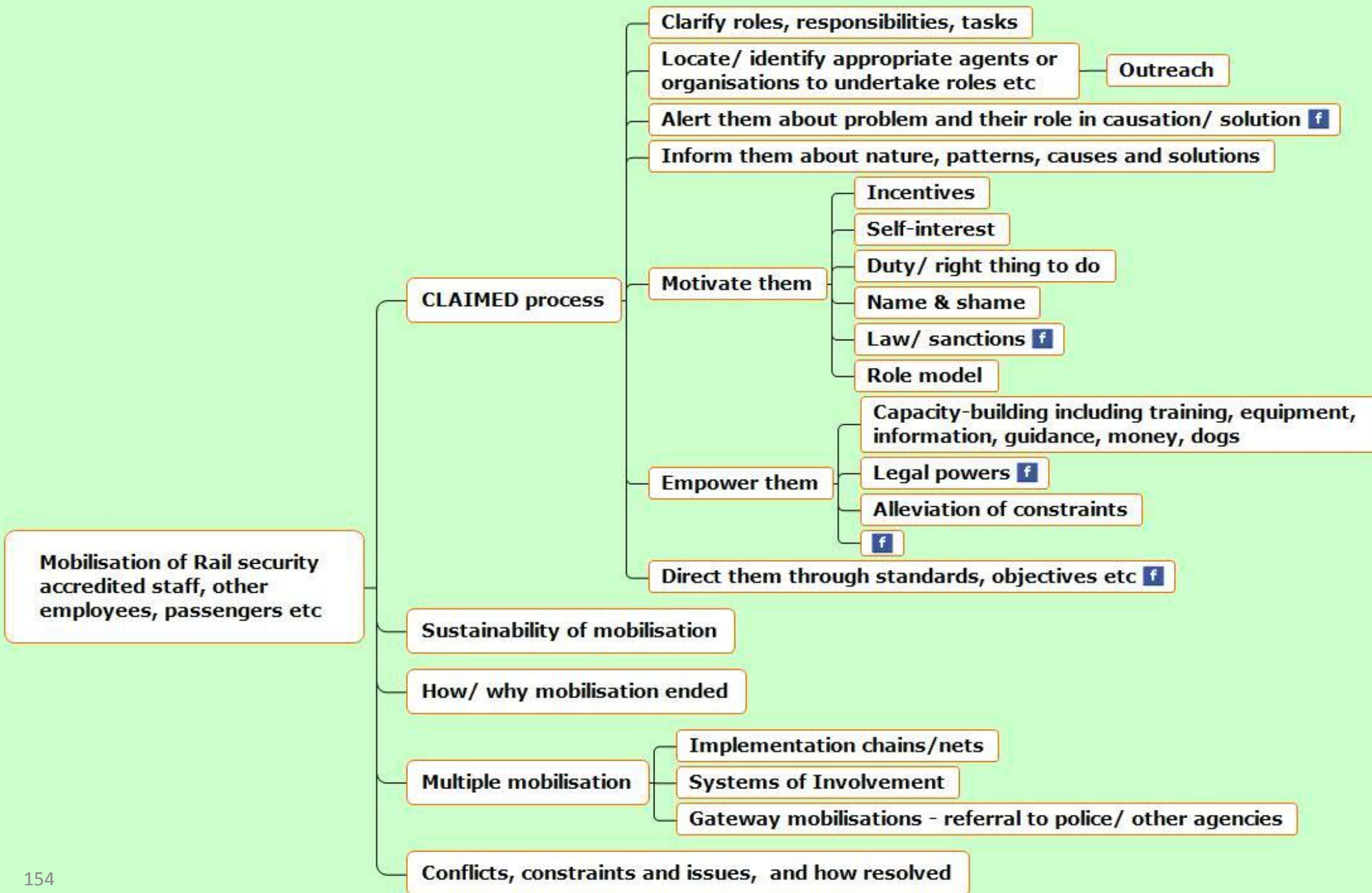
Management, planning, organisational and governance issues

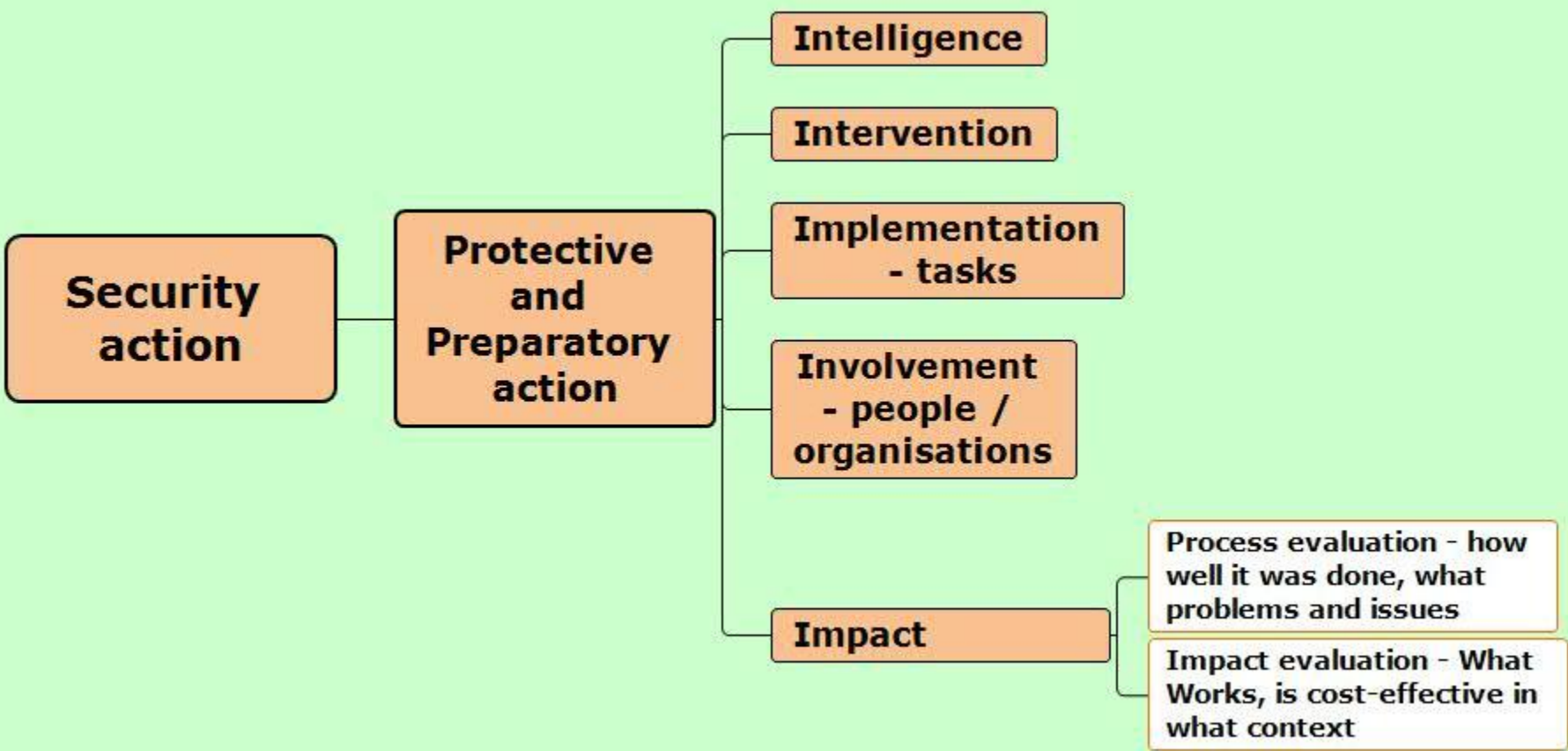






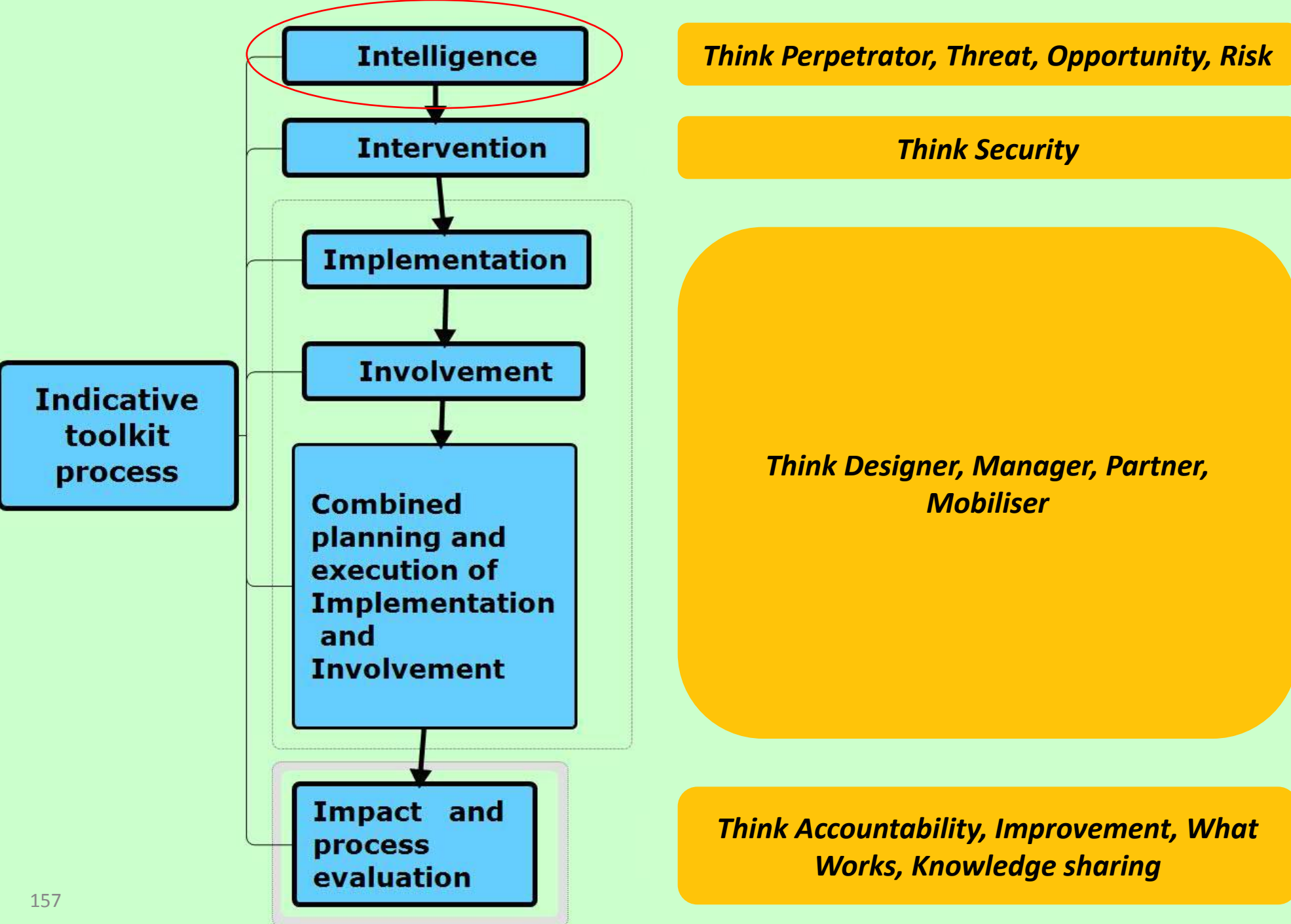


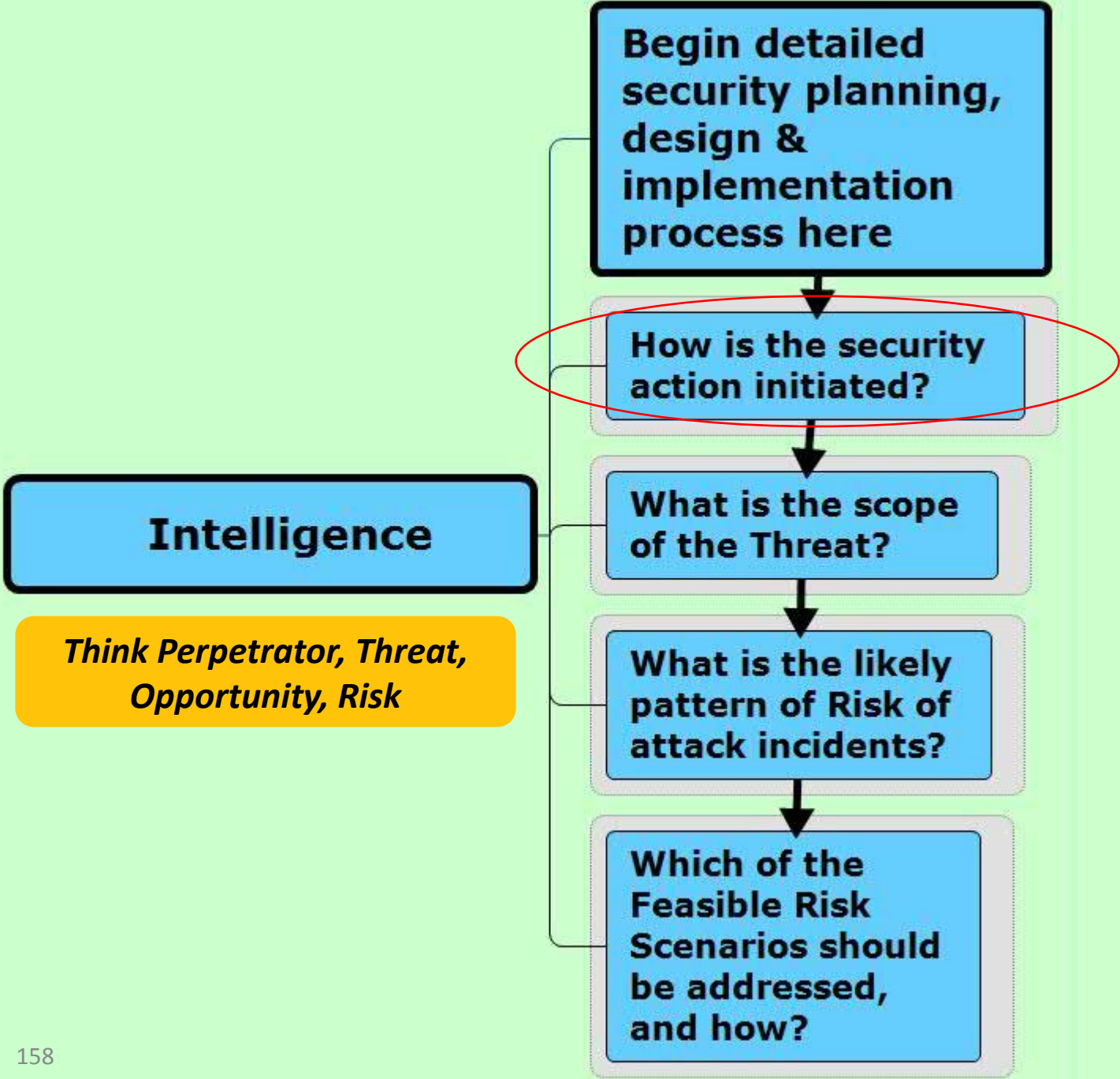


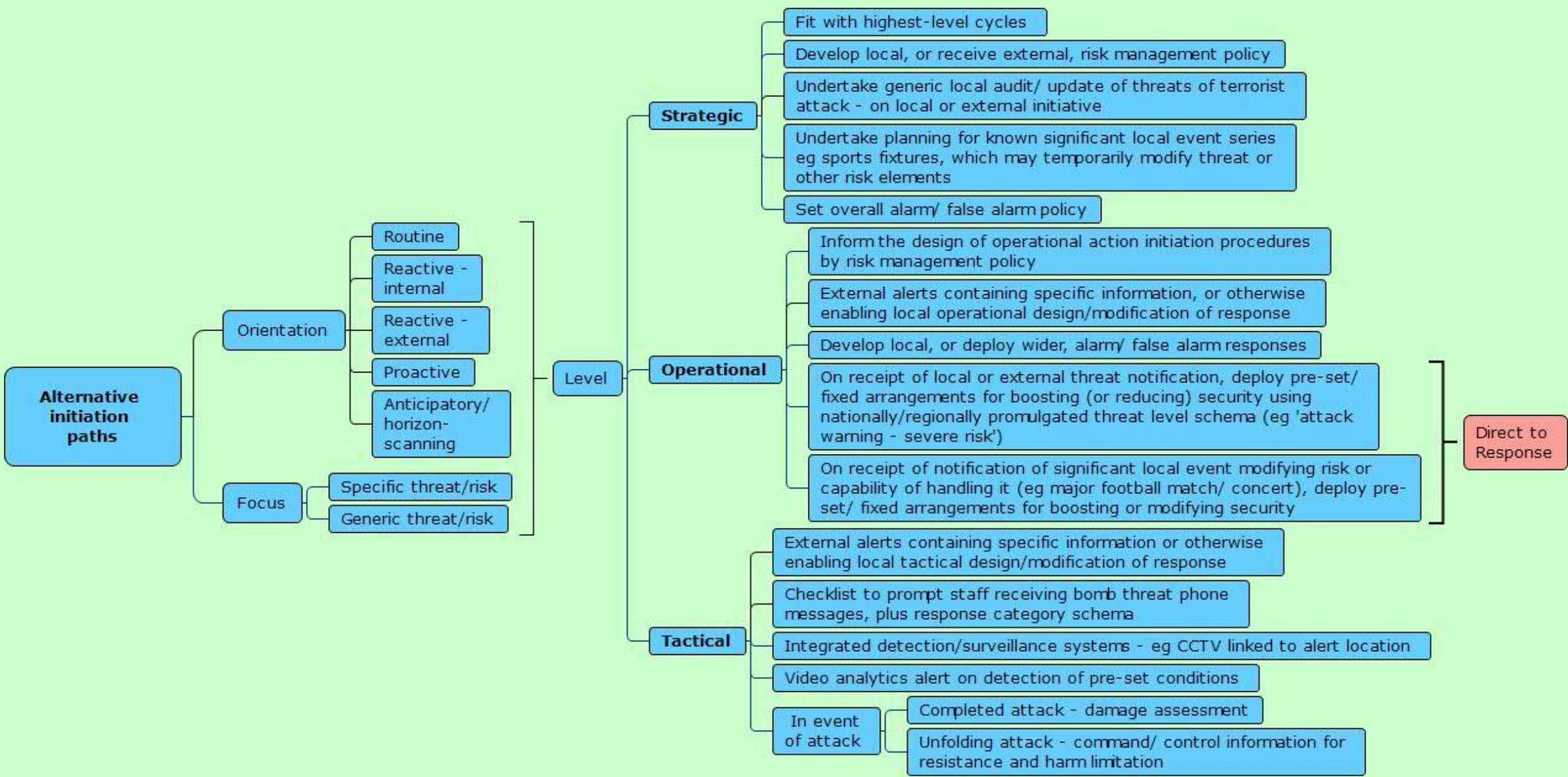


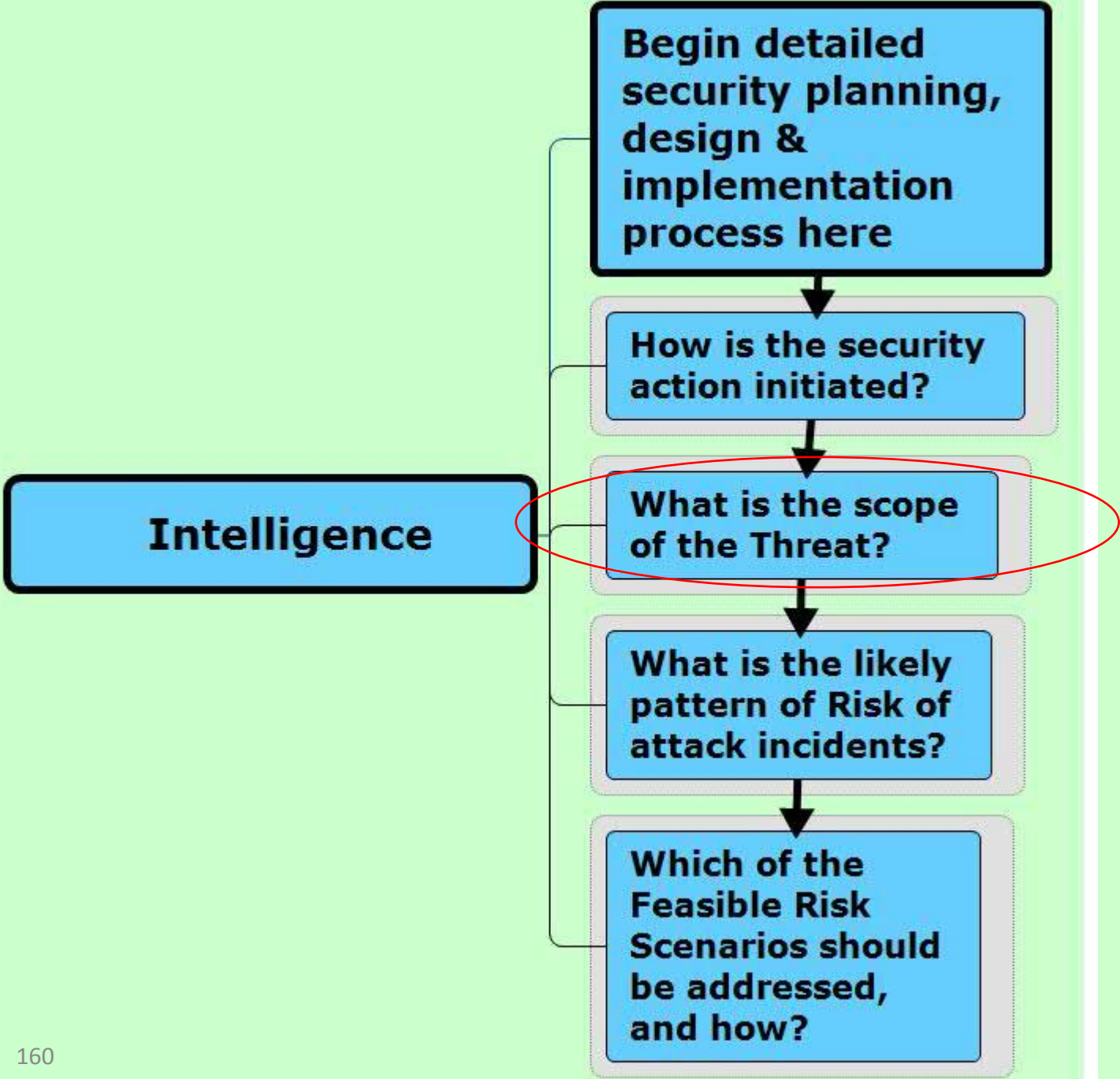
Security Action – Outline toolkit

- What follows is an outline toolkit based on 5Is, Conjunction of Terrorist Opportunity and other frameworks introduced above
- It is planned to develop this into a fully-interactive working toolkit and tutorial









What is the scope of the Threat?

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

What is the scope of the Threat?

What do the Perpetrators want to do? - Intent

Perpetrators' strategic, operational and tactical goals relating to their overall strategy, Target Audiences and Target Vectors

Perpetrators' level of motivation/ determination/ callousness

Could they do it? - Capability

Tactical Attack Method possibilities

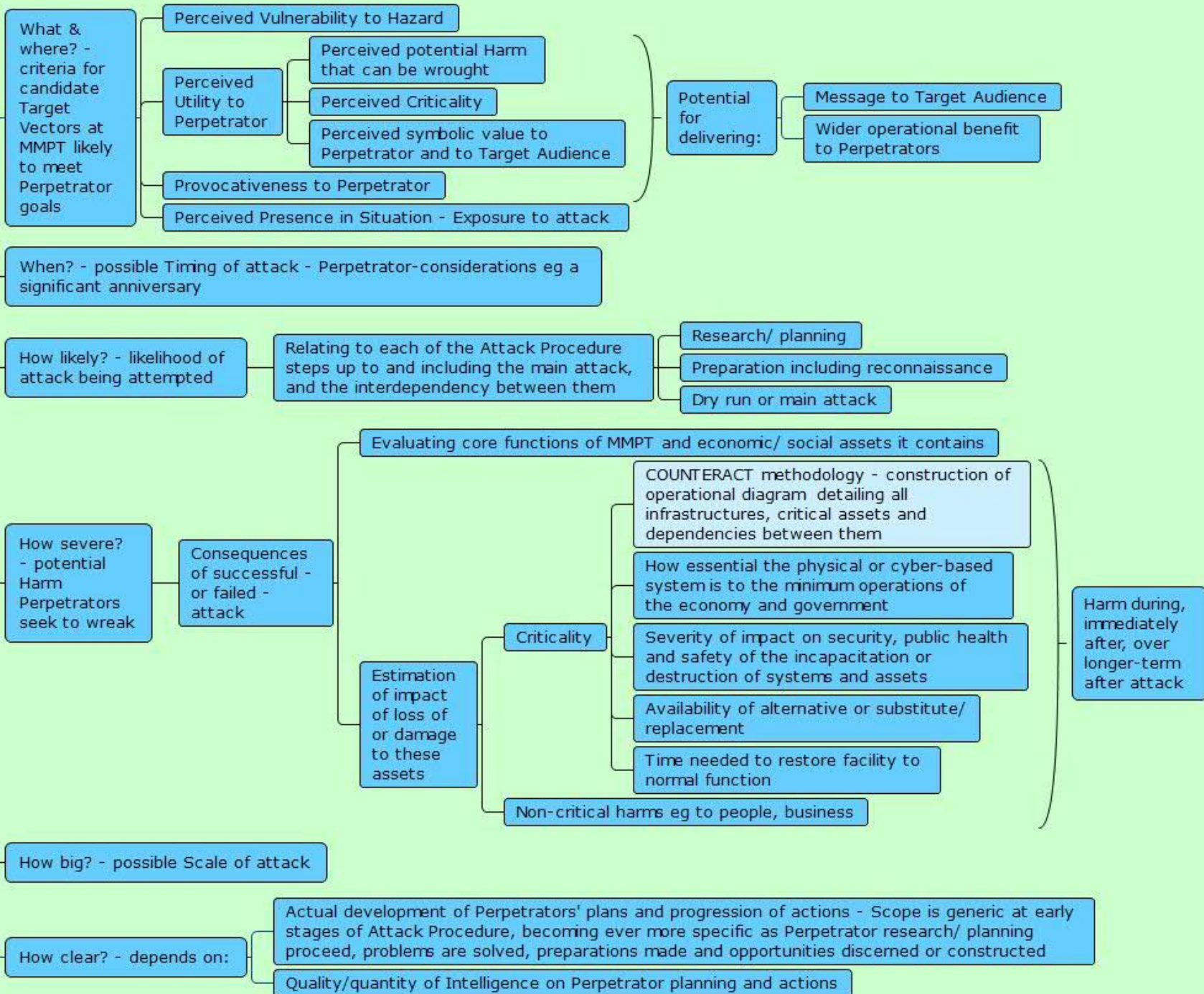
Weapons, tools, Exploitable External Hazards

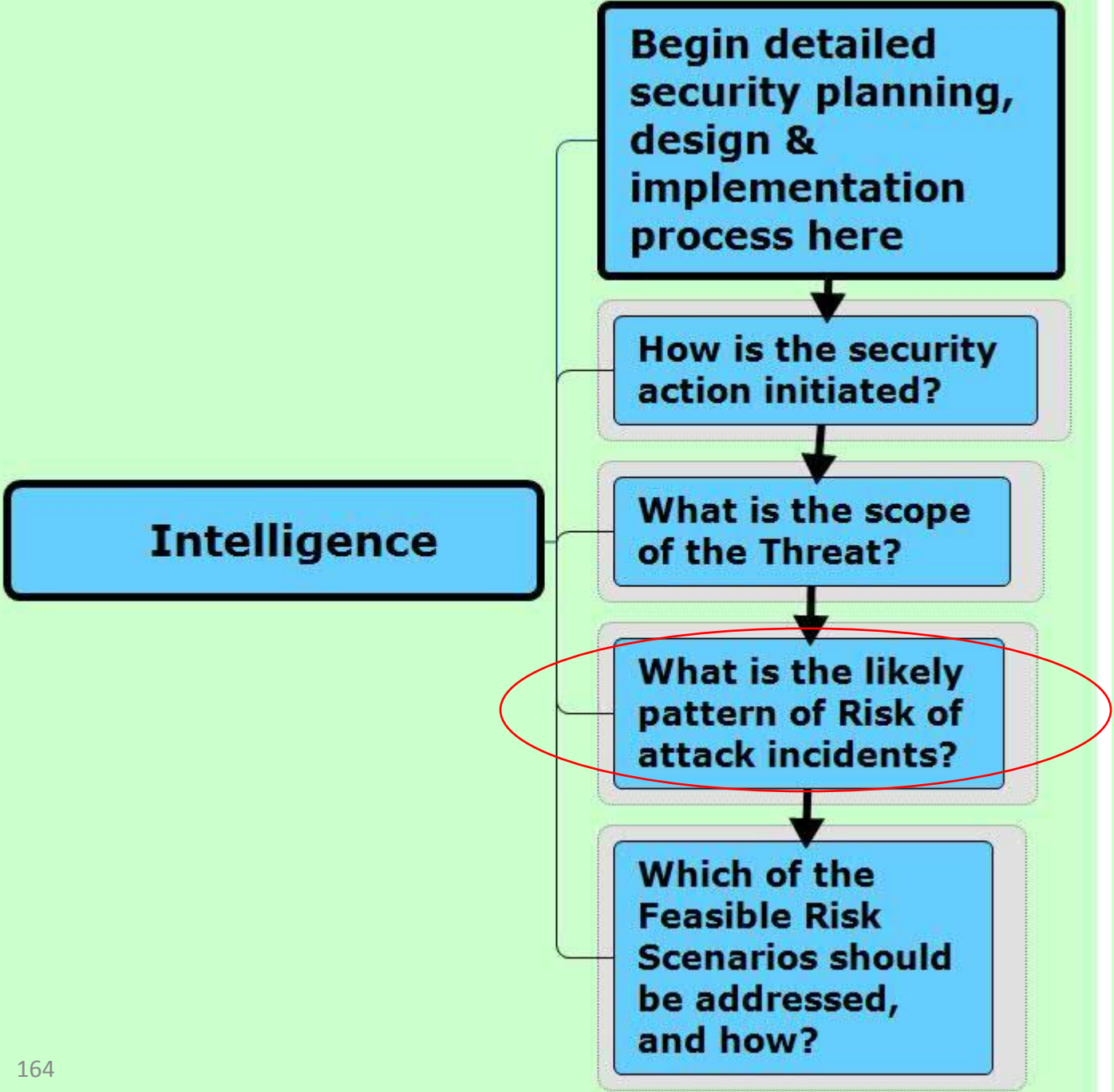
Exploitable Internal Hazards

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





**What is the likely
pattern of Risk of
attack incidents?**

**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**

What is the likely pattern of Risk of attack incidents?

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

Intent, Capability and Scope of threat relative to MMPT

The set of Tactical Attack Method combinations likely to be available to the Perpetrators associated with this Threat

The Weapons, Tools & External Hazards Perpetrators may bring to MMPT

How each available Method might be instantiated as a particular Attack Script Permutation, or set of Permutations on alternative Tracks, of the Attack Procedure tree, in this particular MMPT

Each such Permutation constitutes an Attack Threat Scenario

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

What is the likely pattern of Risk of attack incidents?

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

Situational
Opportunity
factors
remaining
in MMPT,
under the
Baseline
Security
condition

Enclosure - MMPT itself or internal enclosures within it

Wider Environment of MMPT

Accessibility to MMPT (remote access/
viewing or physical presence of Perpetrator)

Preventers - limitations of Police, Security, Employees, Contractors, Public

Promoters - Inadvertent, careless or deliberate

The likely kinds of
Target Vector

Present at MMPT

Vulnerable to Threat

Rewarding for Perpetrator to
injure, damage or destroy

Internal Hazards within MMPT, accessible and
susceptible to exploitation by Perpetrators

What is the likely pattern of Risk of attack incidents?

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

Do the Opportunity factors in the current Baseline Security condition all line up sufficiently well such that a Feasible Opportunity Path extends for the entire sequence of the attack procedure, step-by-step?

Are there problems with one or more steps that the Perpetrators are judged unlikely to be willing or able to solve or circumvent using alternative methods, ie Opportunity Paths are Blocked?

This yields a set of feasible Risk Scenarios

Likelihood

Consider the parameters of each Feasible Risk Scenario as they relate to this MMPT

Immediate & consequential Harm if incident happens

Estimation of impact of loss of or damage to these assets

Criticality - national

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

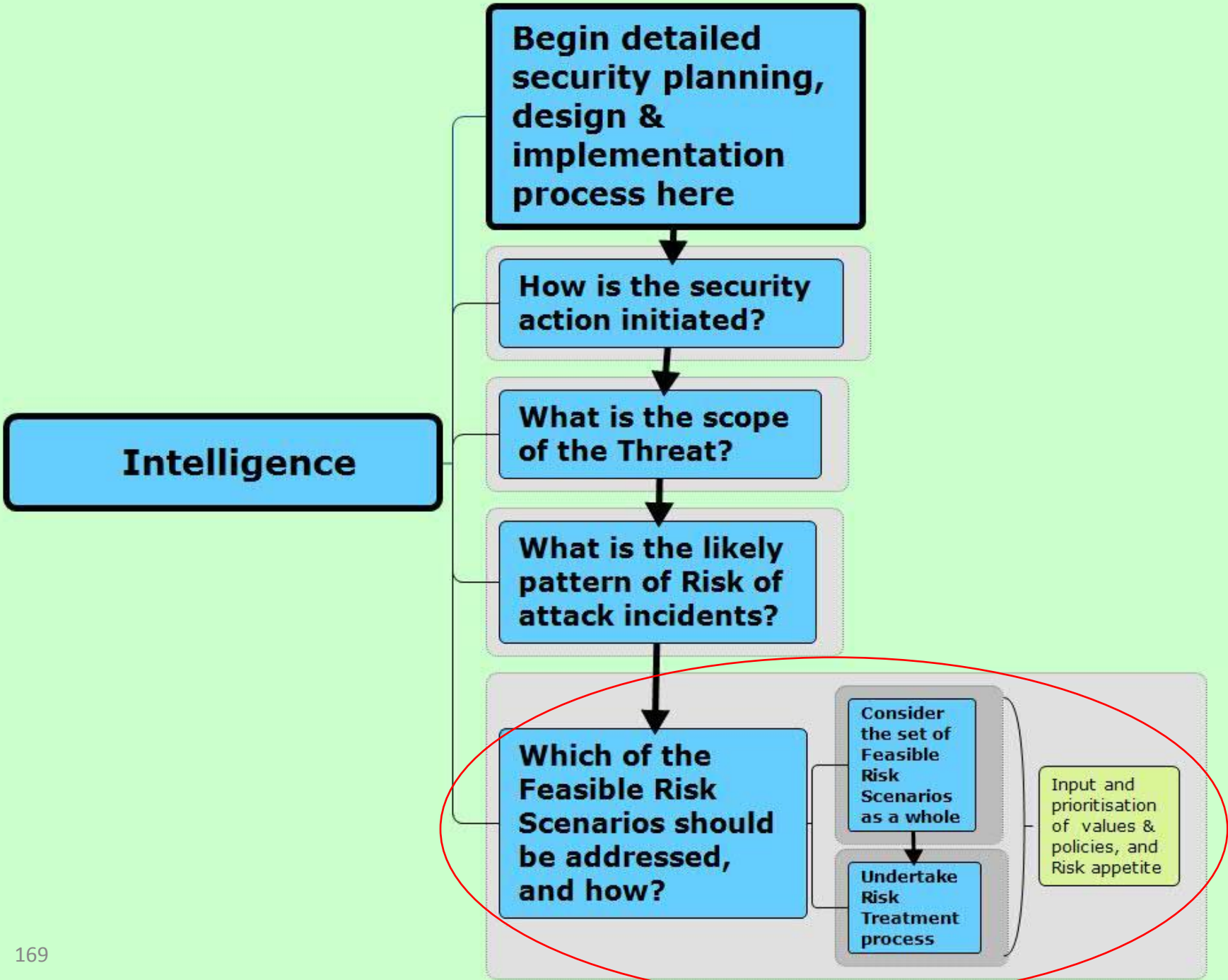
Non-critical harms eg to people, core assets of business

Timing

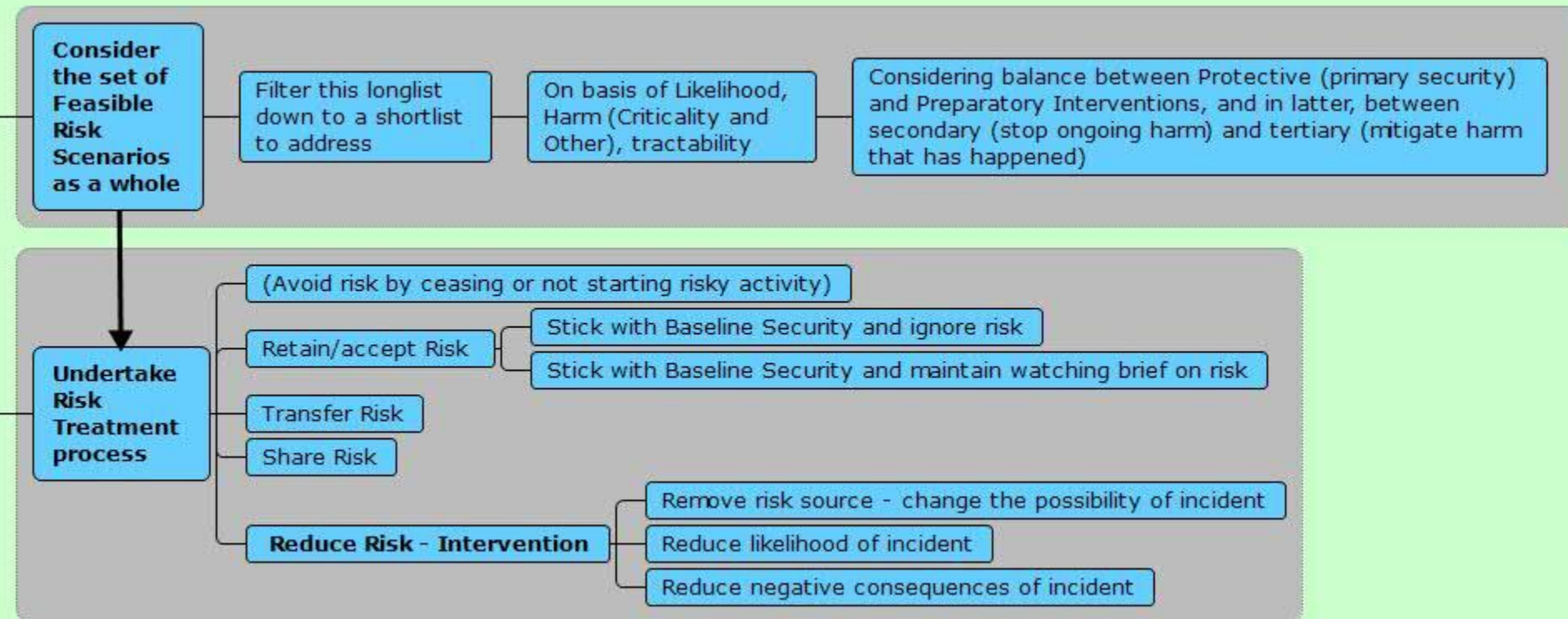
Consider variations in each Feasible Risk Scenario

Horizon-scanning eg for technological, procedural or social change can identify which currently Blocked Opportunity Paths may become Feasible in future

And consider multiple Risks together



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



Intervention

Think Security

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?

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

Look across all Feasible Paths of Opportunity identified, against which it has been decided to intervene

Assemble an array of Feasible Opportunity factors, individual or in configurations, which together make up these paths

Identify the smallest set of Opportunity factors to reduce in order to yield greatest prima facie impact/ cost-effectiveness/ implementability over appropriate timescale

Look for critical 'pinch points' in Opportunity Paths; and synergies, beneficial redundancy etc to guide which paths, and which individual steps on them, to block

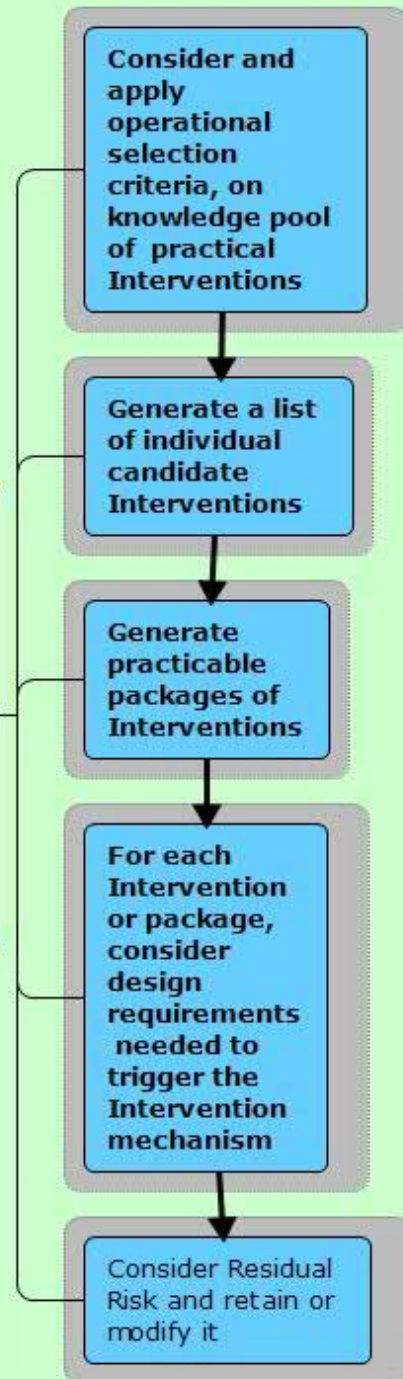
Informed by practical operational/ tactical experience

Intervention

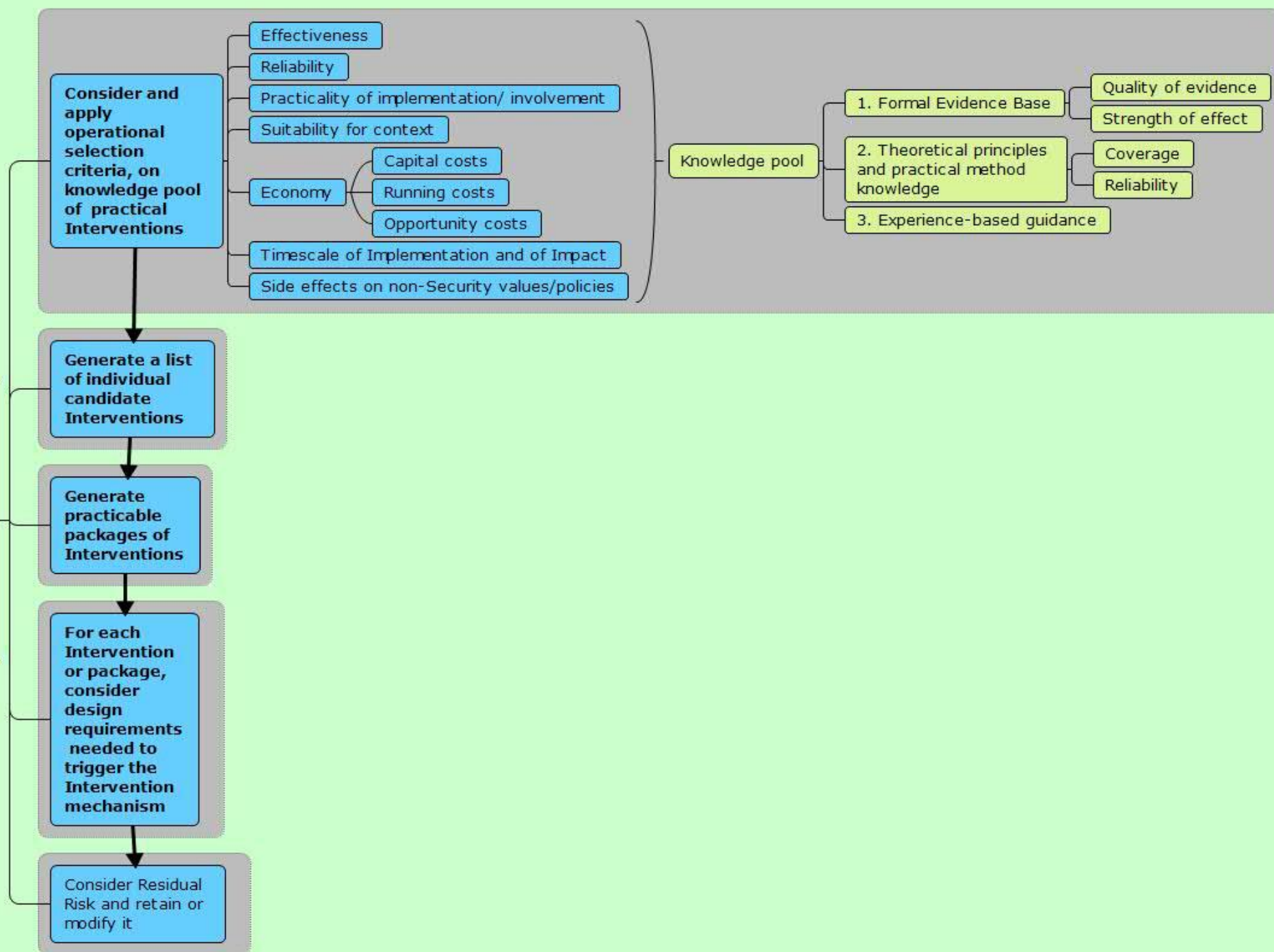
Which set of Opportunity factors should be addressed at the MMPT, to reduce likelihood of/harm from the selected Risk Scenarios?

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

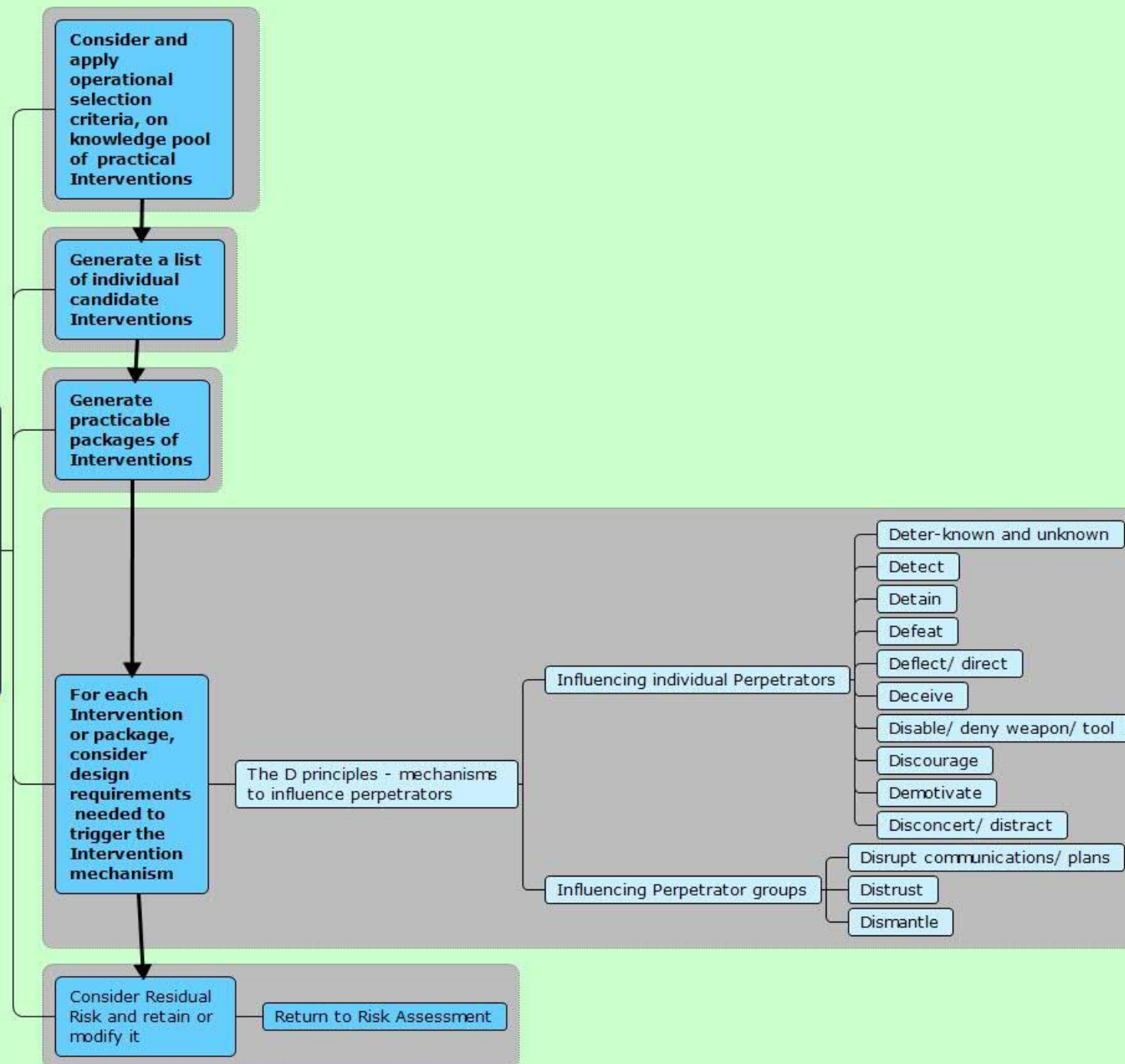
**What Intervention
Methods and/or
Principles work to
block the
Opportunities in
the selected Risk
Scenarios, for this
MMPT?**

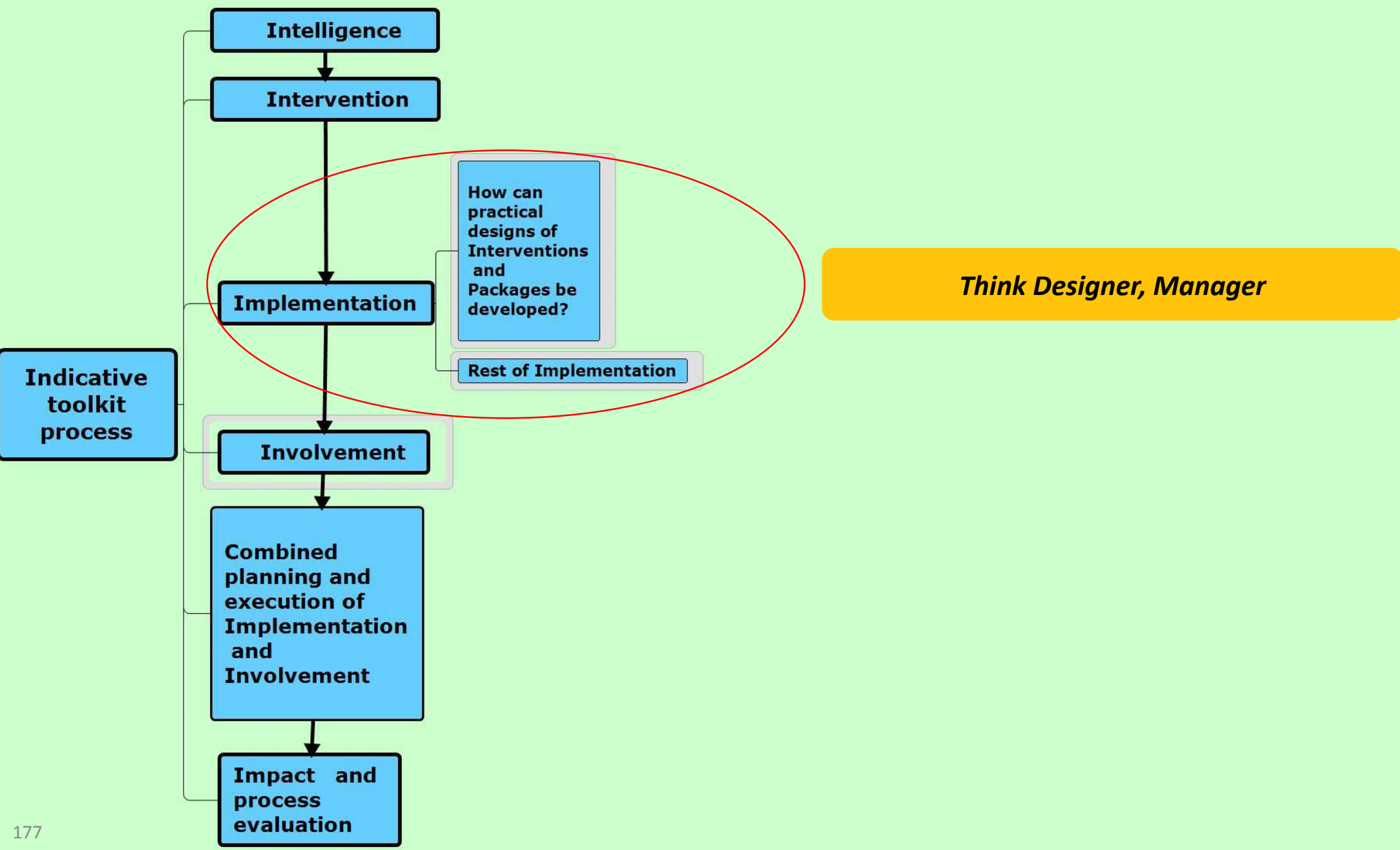


What Intervention Methods and/or Principles work to block the Opportunities in the selected Risk Scenarios, for this MMPT?



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



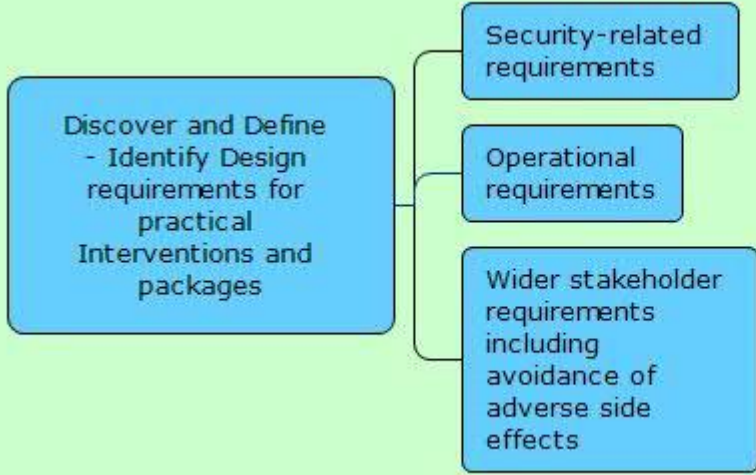


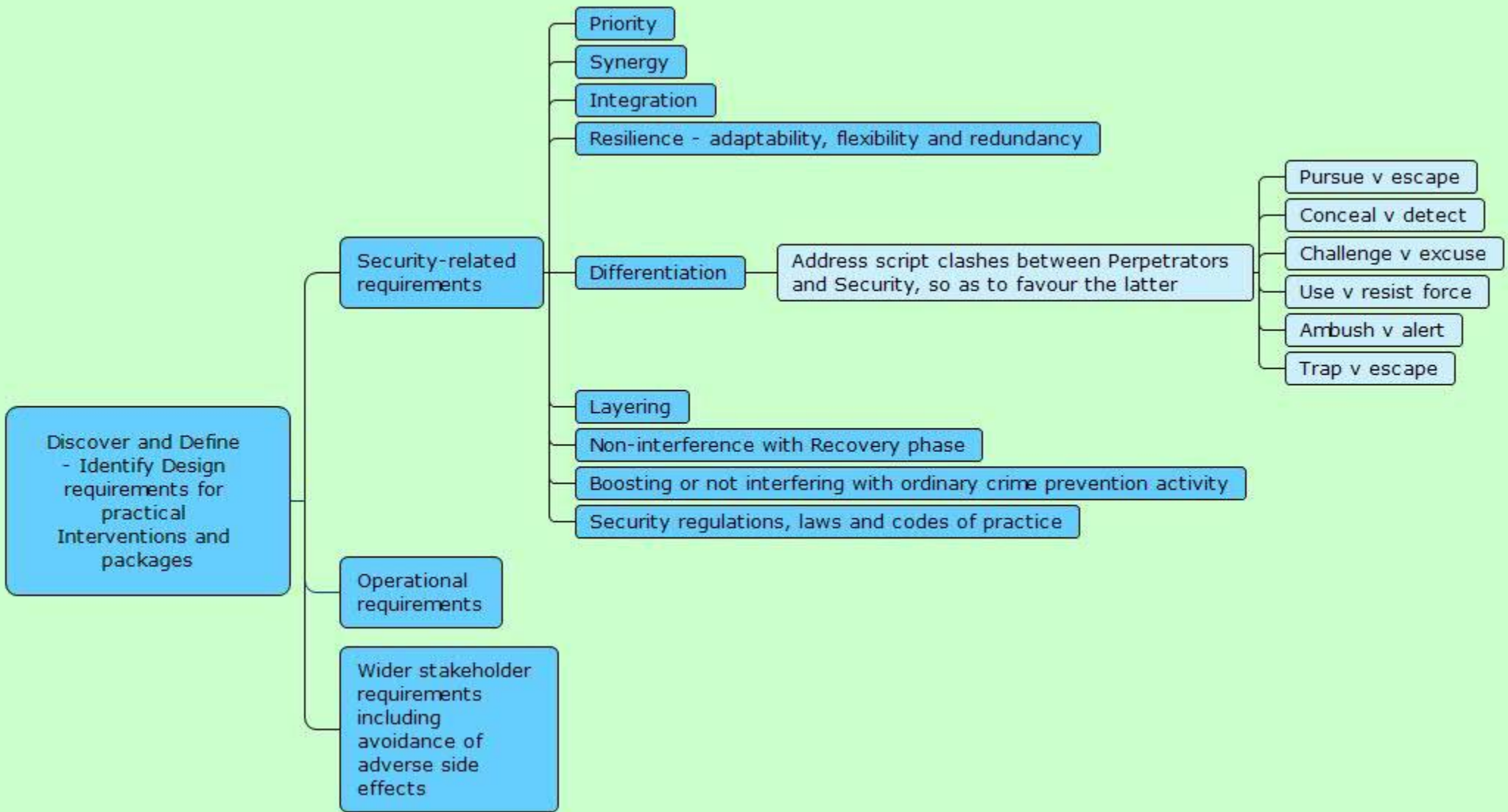
How can practical designs of Interventions and Packages be developed?

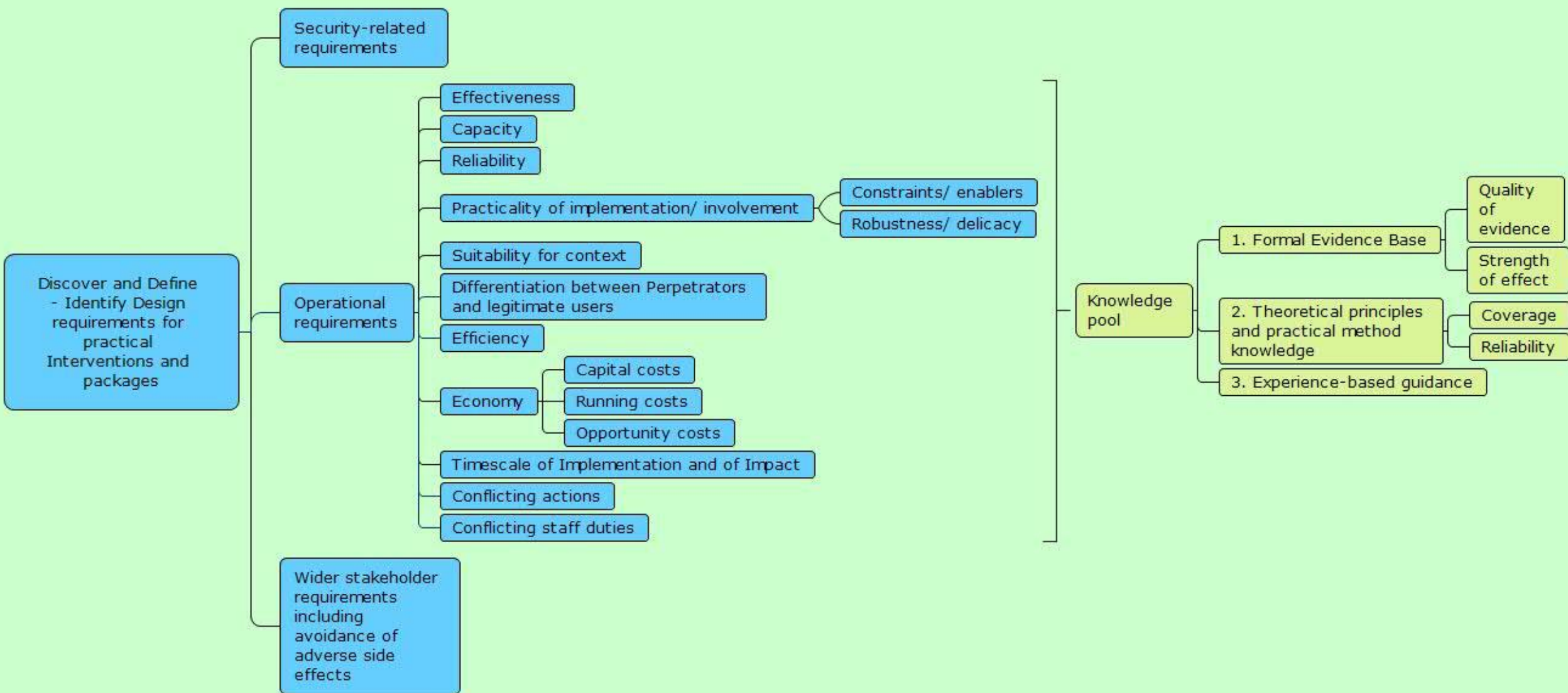
Discover and Define
- Identify Design requirements for practical Interventions and packages

Develop and Deliver
- Conduct iterative design process to generate practical Interventions/ Packages

Involve police, security, transport staff and other stakeholders in co-design process to draw on their expertise and site-specific knowledge

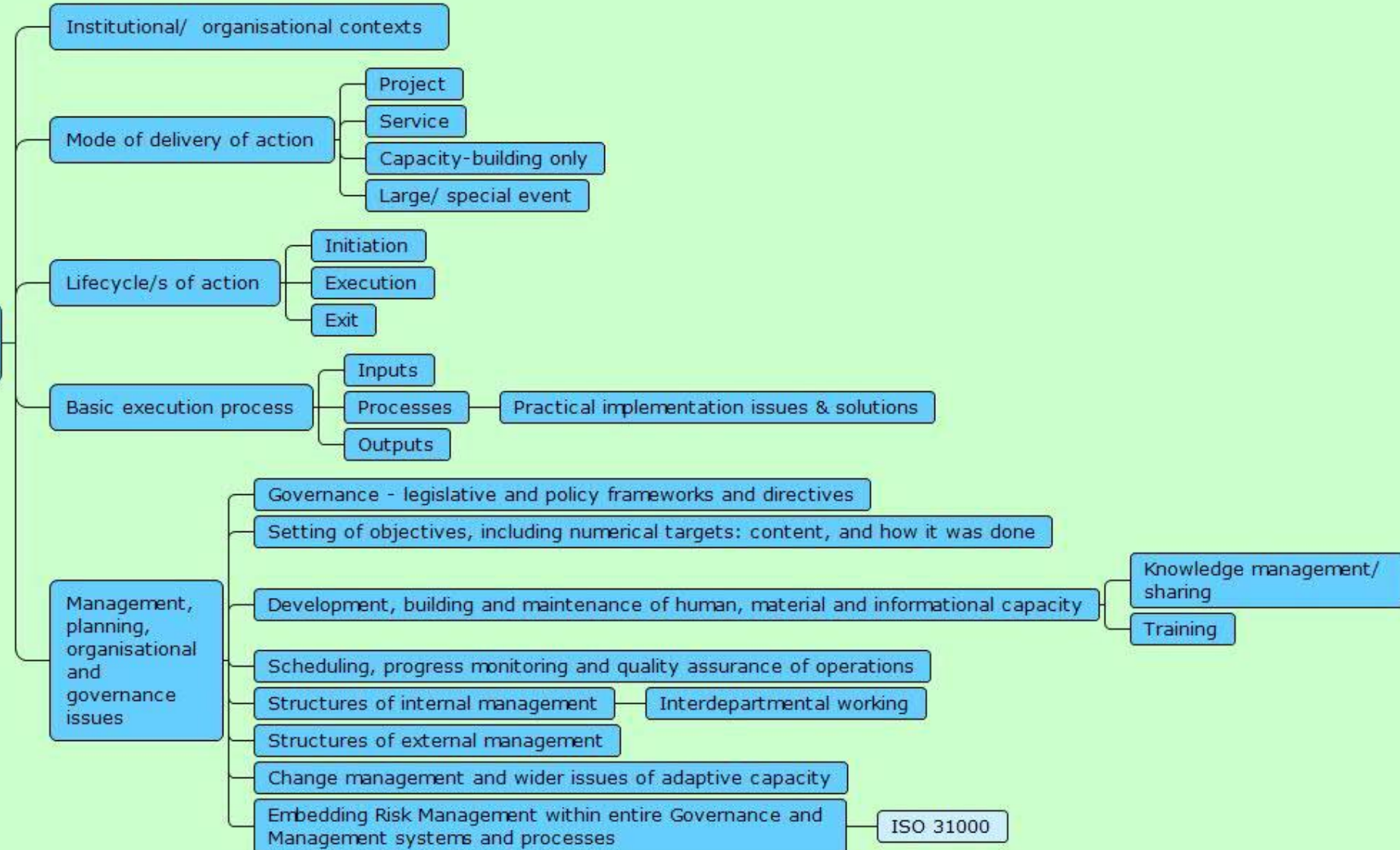








Rest of Implementation



Involvement

Partnership

Mobilisation

Climate setting

Generic Mobilisation and
Climate setting methods

Other:

Intel for Involvement

Accountability

Building collaborative capacity

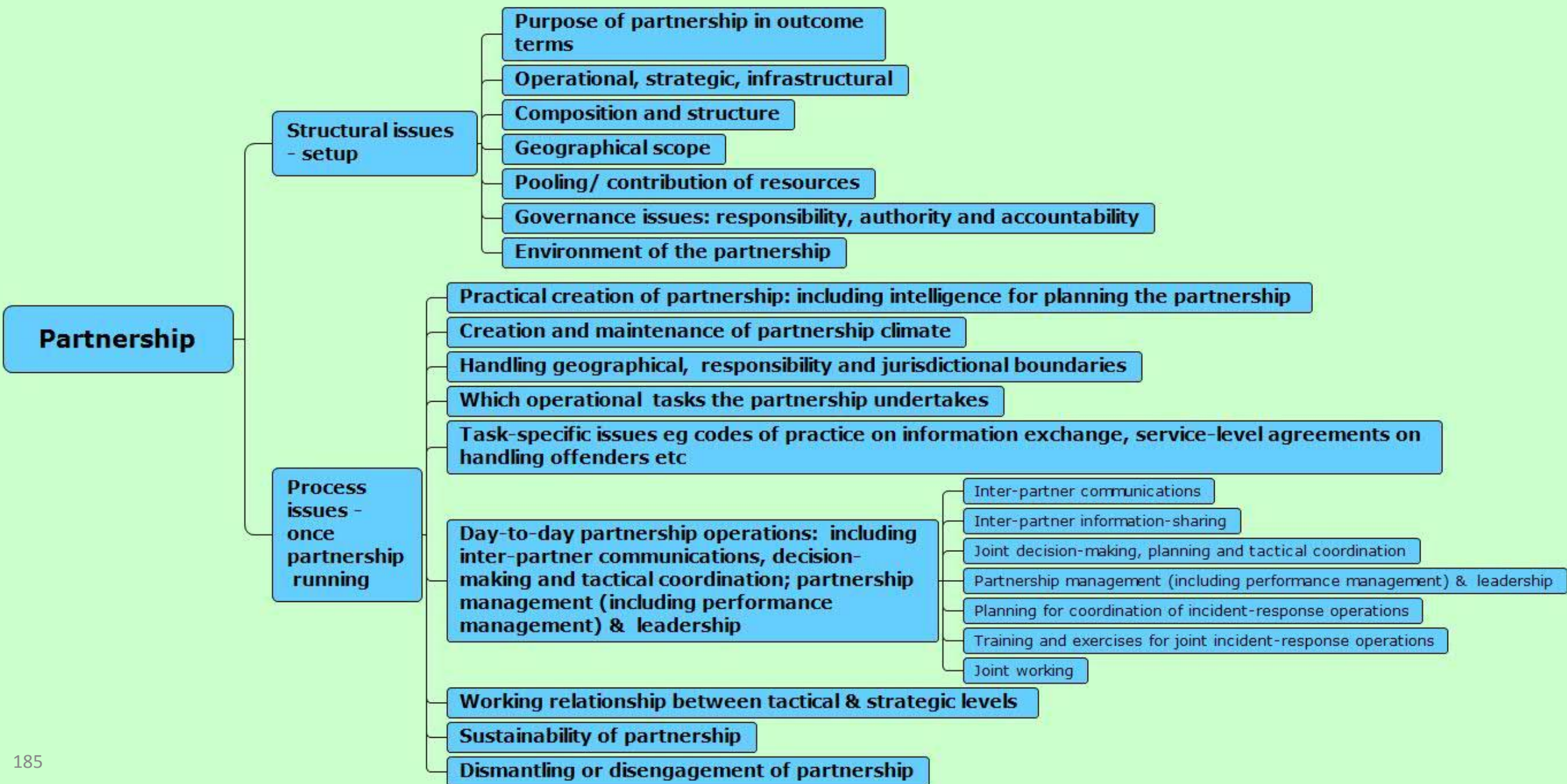
Communication

Consultation

Demand

Risks & blockages

Think Designer, Partner, Mobiliser



Mobilisation

By professionals, of rail security accredited staff, other employees, passengers etc

CLAIMED process

Clarify roles, responsibilities, tasks

Locate/ identify appropriate agents or organisations to undertake roles etc

Outreach

Alert them about problem and their role in causation/ solution

Inform them about nature, patterns, causes and solutions

Motivate them

Incentives

Self-interest

Duty/ right thing to do

Name & shame

Law/ sanctions

Role model

Empower them

Capacity-building including training, equipment, information, guidance, money, dogs

Legal powers

Alleviation of constraints

Direct them through standards, objectives etc

Sustainability of mobilisation

How/ why mobilisation ended

Multiple mobilisation

Implementation chains/nets

Systems of Involvement

Gateway mobilisations - referral to police/ other agencies

Conflicts, constraints and issues, and how resolved

Involvement

Partnership

Mobilisation

Climate setting

Public and stakeholder acceptability of security arrangements

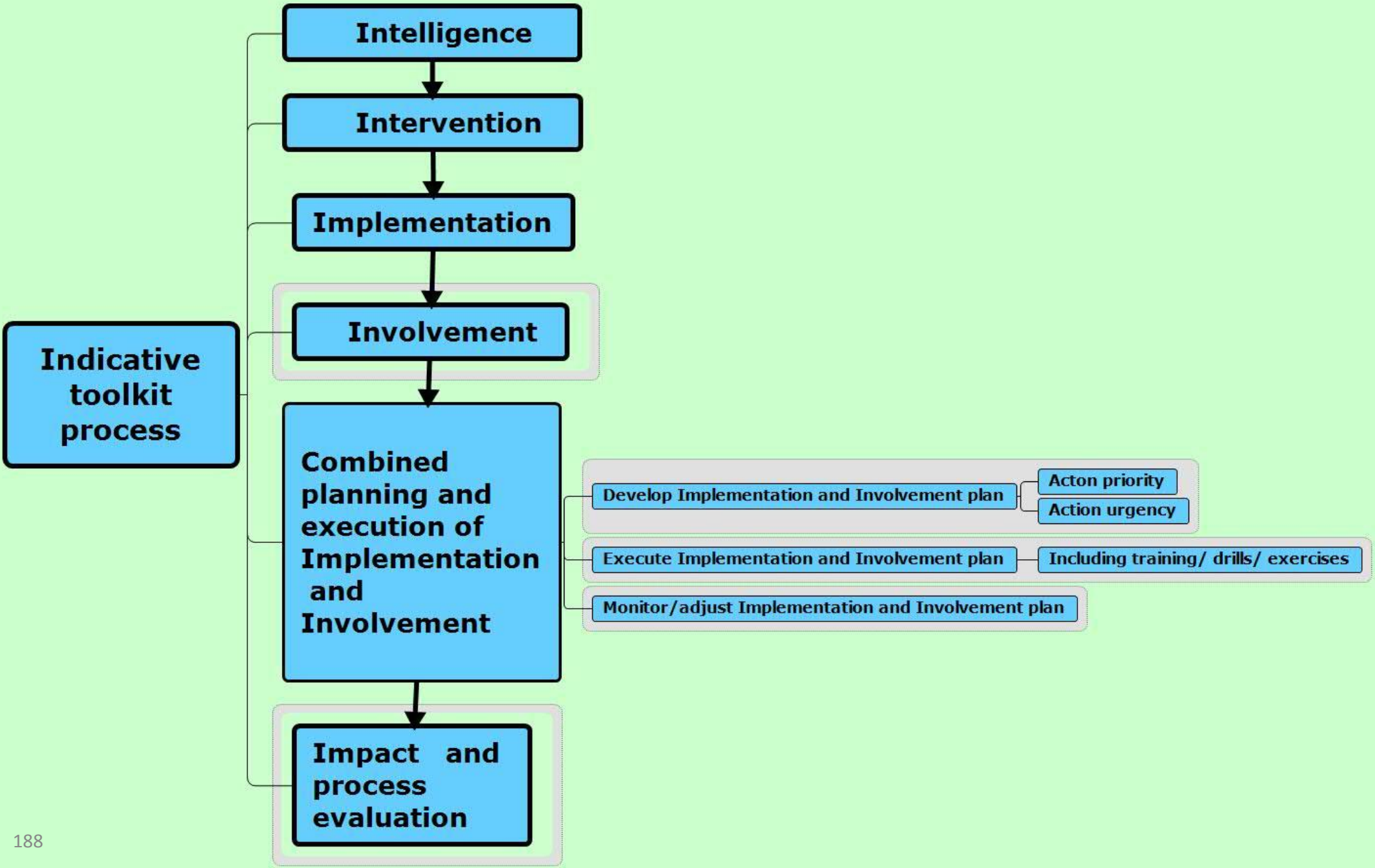
Generic Mobilisation and Climate setting methods

Public involvement in drills/simulations of emergencies

Security awareness campaigns

Combined mobilisation programmes eg Projects Griffin and Argus

Other:



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

*Think Accountability,
Improvement, What
Works, Knowledge sharing*



**AUSTRALIAN
CRIMINAL
INTELLIGENCE
COMMISSION**



Australian Government

Australian Institute of Criminology

Understanding and Reducing the Risk of Terrorist Attacks at Passenger Terminals: Workshop Policy section

**Paul Ekblom
Huddersfield**

**University of

November 2016**

Policy: Eight General Principles for a Pan-EU Land Transportation Security Strategy for MMPTs

Principle 1

Common language: Standardise definitions of all terms relating to MMPT security throughout EU

CAF includes a Glossary

Principle 2

Establish holistic governance structures and partnership working at MMPTs

Recommended Practice	Practices/ Areas of concern
<ul style="list-style-type: none">❖ Data sharing between transport networks, police and MMPT businesses❖ Compatible voice communication systems between different agencies❖ Regular multi-agency meetings between MMPT stakeholders❖ Co-location of security personnel❖ One company responsible for management of both cleaning and security staff	<ul style="list-style-type: none">❖ Organisations(police, business, transportation)each with their own security procedures and policy❖ Fragmentation of responsibility for security across boundaries within/ proximate to MMPTs❖ Lack of coordination between different operators on security matters (e.g. between over-ground rail & Metro systems)❖ Restricting partnership working to dealing with emergencies only

Recommended Practice

- ❖ **Physical barriers** on MMPT approach roads
- ❖ **Bollards** in front of buildings to prevent vehicles armed with explosives entering site (Glasgow airport attack)
- ❖ Use of **metal shutters** to close off part of the terminal at night
- ❖ **Blast-proof waste bins** to mitigate the effects of an explosive device if placed there
- ❖ **Anti-shatter film** for glass



Practices/ Areas of Concern

- ❖ Leaving MMPT foyers and concourses unprotected by the absence of Hostile Vehicle Mitigation interventions



Principle 4

Manage and control the movement of people using MMPTs

Recommended Practice

- ❖ The presence of barriers can block or deter people from entering certain areas, can provide an opportunity to challenge suspicious behaviour
- ❖ The absence of barriers can create a better flow of movement with an absence of pinch points and overcrowding



Principle 4

Manage and control the movement of people using MMPTs

Practices/ Areas of Concern

- ❖ At certain times of the day if automatic barriers are unmanned this can lead to overcrowding around the barriers, creating an additional target for terrorists

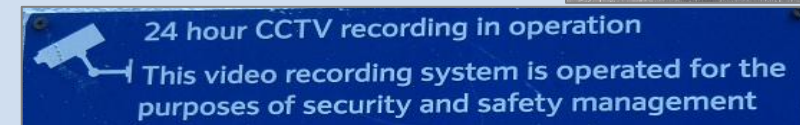


Principle 5

Maximise opportunities to conduct effective surveillance at MMPTs

Recommended Practice

- ❖ MMPT designs and layouts that maximise opportunities for surveillance – clear sightlines and use of glass/ transparent materials
- ❖ The use of transparent plastic bags in waste bins
- ❖ Clearly visible signs to inform passengers that CCTV is in operation & minimum standards for its use
- ❖ Regular patrolling by staff but varying the routes they take

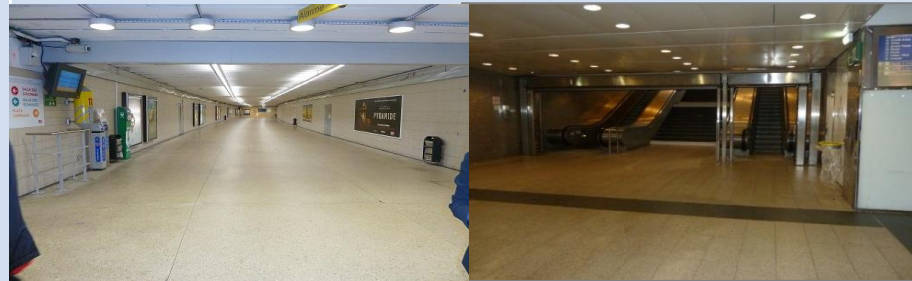


Principle 5

Maximise opportunities to conduct effective surveillance at MMPTs

Practices/ Areas of Concern

- ❖ Variations in levels of lighting
- ❖ Designs that compromise opportunities for surveillance
- ❖ Having a multitude of CCTV systems managed by different operators and to different standards
- ❖ Not viewing CCTV in real time



Principle 6

Ensure security approaches & interventions are appropriate for MMPT site and context



Principle 7

Provide Training of staff working at MMPTs

Recommended Practice	Practices/ Areas of Concern
<p>Training in:</p> <ul style="list-style-type: none">❖ 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 <p>Plus:</p> <ul style="list-style-type: none">❖ Consistency in content and quality of training for all staff (security, cleaners, retail)❖ Regular assessments of staff competence	<ul style="list-style-type: none">❖ Failure to provide customer service training where required – ensure staff are ‘approachable’ by passengers

Principle 8

Strike a balance between the need for security & other priorities at MMPTs

Recommended Practice	Practices/ Areas of Concern
<ul style="list-style-type: none">❖ 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	<ul style="list-style-type: none">❖ 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 at the EU level: Defining the baseline

Our research suggested that each MMPT should consider

- **Developing and implementing** a baseline security plan comprising:
 - Communications policy
 - Physical security strategy
 - Movement control plan
 - Site surveillance protocol
 - Essential security awareness training programme for all staff catering for different levels (strategic, operational, tactical)

And that efforts should be made to

- **Produce guidance** at an across-EU level on how to bring the above to fruition

- 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

Thank You!

CAF was developed from the Conjunction of Terrorist Opportunity framework
<https://5isframework.files.wordpress.com/2013/12/cto-security-journal-july05.pdf>

and its more generic forbear, the Conjunction of Criminal Opportunity
<https://5isframework.wordpress.com/conjunction-of-criminal-opportunity/>

Also the 5Is process model of doing crime prevention and security <http://5isframework.wordpress.com>

Other sources:

- Rand classification of terrorist attacks 1968-2009 www.rand.org/nsrd/projects/terrorism-incidents.html
- Project Griffin <https://www.gov.uk/government/publications/project-griffin/project-griffin>
<http://www.met.police.uk/projectgriffin/>
- Crime scripts <http://link.springer.com/article/10.1007/s10610-015-9291-9>
- 11Ds <http://link.springer.com/article/10.1186/s40163-014-0002-5>
- Misdeeds and security
www.designagainstcrime.com/lists/the-misdeeds-and-security-framework-know-about-and-know-what/
- Design Council Design out Crime guide www.designcouncil.org.uk/resources/guide/designing-out-crime-designers-guide
- UK College of Policing What Works <http://whatworks.college.police.uk/toolkit/Pages/Toolkit.aspx>
- UK CONTEST <https://www.gov.uk/government/publications/counter-terrorism-strategy-contest>