Opportunity extended – via development of an interactive counterterrorism toolkit

Prepub version – final may slightly differ.

Ekblom, P. and Newton, A. Opportunity extended — via development of an interactive counterterrorism toolkit. *Crime Sci* **15**, 15(2026) . https://doi.org/10.1186/s40163-026-00280-2

Abstract

From its origins in *Crime as Opportunity* and related papers, through to its current incorporation within crime science, the concept of opportunity has played an important role in research and practice. Yet much of the thinking behind the concept has remained implicit, intuitive and static. A chance to take the concept forward in a practical, yet rigorous way arose when developing a detailed interactive toolkit to guide security managers of large and complex stations to prevent, and prepare responses to, terrorist attacks and other crimes more typical of such places.

We describe the requirement for the toolkit; the conceptual architecture we developed, with particular reference to opportunity and how it meshes with other crime science concepts such as crime precipitation, and with broader concepts from traditional security practice such as threat and risk management; and the practical realisation through a process that matches security actions to the threat posed by terrorists/criminals and the risk generated in the particular environment of complex stations. We finish by considering how the development of the toolkit advanced the concept of opportunity.

Keywords: Opportunity, Crime Prevention, Counterterrorism, Toolkit, Security, Risk management

Introduction

For fifty years, the concept of crime as opportunity has been a core element of crime science, underpinning substantial and enduring achievements in crime prevention (Mayhew et al., 1976). Yet opportunity remains conceptually underdeveloped. Retained in a deliberately simple, practitioner-friendly form, it functions as a largely intuitive and vernacular construct, insufficiently integrated with the field's principal theoretical frameworks. Consequently, it often describes processes that could be more rigorously

specified and theorised. The simplicity that facilitated the concept's diffusion into practice has also constrained its development (Ekblom 2011, Chs. 4–5[1]).

This paper addresses a major challenge for opportunity-based approaches: the provision of practical guidance on terrorism and crime prevention for security managers of large, complex 'multimodal' land transport hubs (hereafter, complex stations). This challenge arises from three interrelated factors: extreme environmental and organisational complexity; the absence of robust 'what works' evidence; and a persistent conceptual and terminological divide between crime science and conventional security practice. Our response seeks both to advance applied security practice and to support the conceptual maturation of opportunity.

We outline below the challenges faced by security managers of complex stations and by researchers in turn; our transfer of situational crime prevention principles to counterterrorism; and our mixed-methods approach to assembling and structuring knowledge on risk, threat, and security action. We then describe the development of an interactive toolkit drawing on that knowledge and integrating crime science with security and risk management concepts; illustrate its operation. We finally discuss implications for evidence-based terrorism and crime reduction, toolkit design, project limitations, and theoretical development within crime science, with emphasis on opportunity.

The challenge

This study was funded by the European Commission (Directorate-General for Mobility and Transport) to develop a toolkit to support security managers of complex stations in preventing and preparing for terrorist and criminal incidents. This entailed significant demand- and supply-side challenges.

Demand-side challenges

Complex stations constitute large, heterogeneous, and dynamic risk environments. Routine travel, retail, leisure and work activities generate crime (Brantingham et al., 2017), while dense concentrations of people, infrastructure, and symbolic assets attract both opportunistic offenders and highly motivated, well-resourced and persistent attackers.

Governance fragmentation further complicates risk management. Stations typically involve multiple operators, transport providers, retail tenants, private security, and police, hindering comprehensive risk assessment and coordinated security action.

[1] And see https://crimeframeworks.com/a-critical-perspective-on-mainstream-crime-science-frameworks/

Security managers, operating under constrained resources, require substantial analytical and practical support to deliver effective prevention and preparedness.

Supply-side challenges

On the supply side, detailed empirical knowledge of terrorist attacks is limited. The RAND database (n.d.) documents attack types between 1968 and 2009, but lacks the granularity for site-specific prevention. More critically, high-quality evaluative evidence on terrorism prevention is scarce. As noted by Silke (2001), empirical research is limited; a major systematic review by Lum et al. (2006–9) identified only seven studies meeting even relaxed evidentiary standards out of approximately 20,000 examined (representing billions of dollars' investment), producing findings that were both highly general and often irrelevant to land transport contexts – for example, 'screening of passengers at airports is cost-effective'.

This evidentiary deficit reflects the rarity of terrorist incidents and the secrecy surrounding counterterrorism measures, which together preclude robust experimental evaluation. The security literature also suffers from inconsistent terminology, with key concepts such as 'vulnerability' used ambiguously (Ekblom and Sidebottom, 2008).

Finally, existing toolkits provide limited support for the detailed, systematic, and site-specific processes required for effective risk analysis and intervention selection. While aids such as the UK College of Policing's EMMIE toolkit[2] synthesise crime prevention evidence, they function primarily as searchable catalogues of interventions rather than as process-oriented 'how-to' guidance for practitioners.

Responding to the evidentiary challenge

The most serious challenge was to develop a counterterrorism toolkit grounded in sufficiently reliable knowledge despite the absence of directly relevant, rigorous evaluations. Before assembling available evidence, a strategic approach was required. We therefore sought to draw on transferable knowledge from Situational Crime Prevention (SCP) and wider crime science, combining this with insights from conventional security and risk management. SCP focuses on modifying immediate environments 'upstream' of criminal events to reduce risk, but its suitability for counterterrorism required careful scrutiny. We began by examining SCP research explicitly addressing terrorism.

Situational crime prevention and counterterrorism

In response to terrorist attacks over recent decades, SCP-inspired measures have been widely implemented, ranging from crude emergency target hardening (e.g. concrete

[2] https://www.college.police.uk/research/crime-reduction-toolkit

vehicle barriers) to more sophisticated design solutions that provide protection without provoking fear (e.g. the ARSENAL sign outside London's Emirates Stadium). Rather than simply cataloguing such measures, we focused on SCP theory and research directly addressing terrorism from 2015 onwards.

Clarke and Newman's *Outsmarting the Terrorists* (2006) articulated a systematic opportunity-reduction approach to counterterrorism, rebutting objections to situational prevention. Their EVIL DONE framework (Exposed, Vital, Iconic, Legitimate, Destructible, Occupied, Near, Easy) characterises high-risk targets, a profile clearly applicable to large, complex stations. However, our concern lay less with target classification than with the detailed affordances within individual stations; accordingly, EVIL DONE informed rather than structured toolkit development.

More directly relevant were Clarke and Newman's four pillars of terrorist opportunity—targets, tools, weapons, and facilitating conditions—and their 20 principles of intervention. These include crime specificity, offender rationality, understanding terrorist procedures, controlling tools and weapons, prioritising vulnerable targets, anticipation, and avoiding 'magic bullet' solutions. Their injunction to 'think like a terrorist' was particularly influential in identifying method- and context-specific opportunities.

Transferring generic SCP principles

Given the limited terrorism-specific evidence, we adopted a Scientific Realist approach to knowledge transfer (Pawson and Tilley, 1997), focusing on causal mechanisms rather than evaluated interventions. Scientific Realism asks not only *what works* but *how it works*, allowing theoretically grounded mechanisms (e.g. deterrence, discouragement) to be transferred across contexts and intervention forms. Where such mechanisms have demonstrated effectiveness in one embodiment, they may plausibly operate in others.

Evidence that SCP works in principle is summarised in Clarke's (1997) case studies and, more systematically, in Bowers and Guerette's (2014) review. Although this literature does not disaggregate the effectiveness of individual SCP principles or techniques (Clarke, 2017), it provided a defensible basis for extrapolating generic SCP mechanisms to counterterrorism. This foregrounded a critical question: could opportunity, as SCP's core principle, adequately underpin the toolkit?

Can opportunity help?

The opportunity perspective originated within situational crime prevention in the 1970s, drawing on evidence that behaviour is strongly shaped by situational cues. It was strengthened by Rational Choice theory (Cornish and Clarke, 2017), which emphasised offender decision-making, and by Routine Activities theory (Felson 2017), which

modelled crime as the convergence of offenders, targets, and guardians. Crime pattern theory (Brantingham et al., 2017) later incorporated spatial dynamics, explaining how crime generators and attractors influence offender movement and target selection. Through refinements in Rational Choice, Routine Activities, crime scripts, situational precipitators, and the emergence of crime science, opportunity-based approaches became widely adopted. Yet the underlying concept of 'opportunity' itself has changed very little.

Scholars have increasingly argued that opportunity, in its traditional form, is too limited. Newman and Clarke (1997) noted that it fails to capture the complexity of person–situation interaction, while others (Bouhana, 2013) question whether opportunity can function as a causal explanation at all. Ekblom (2017) proposes a relational understanding: environmental features afford action only when offenders possess the necessary motivation, skills, and resources. This view aligns with affordance theory (Gibson 2014), implying a single integrated mechanism linking perception, environmental conditions, and action.

Ekblom also argues that opportunity must be defined in relation to purpose—opportunity to do what. He therefore reconceptualises opportunity as an ecological process in which agents encounter, seek, or create enabling circumstances for achieving various goals, including both rewards and protective 'hygiene' goals such as avoiding detection. Encountering reflects Routine Activities dynamics; seeking and creating reflect crime attraction and active offender strategies. Complex stations can support all three, with terrorism typically involving highly active forms of opportunity creation.

Terrorist exploitation of complex stations ranges from spontaneous lone-actor attacks to sophisticated multi-stage operations. Crime scripts (Cornish, 1994) conceptualise such attacks as sequences of interlinked actions, each presenting distinct opportunities that must be recognised and addressed. Situational precipitators (Wortley, 2017) highlight immediate environmental triggers that may intensify behaviour, even when motivation is already present, though these ideas remain only loosely integrated with opportunity-based models.

In summary, opportunity remains central to situational crime prevention and crime science but is theoretically underdeveloped and insufficiently integrated with complementary perspectives within SCP and wider security-oriented conceptions of threat and risk. These limitations motivated our adoption of a more nuanced, interactive conception of opportunity for toolkit development—one that explicitly connects offender goals, resources, motivations, and situational affordances into a unified framework.

Assembling knowledge content

We then needed both to identify relevant knowledge for the toolkit and to impose an immediately usable structure to be able to draw on that knowledge in toolkit construction. Knowledge assembly relied on a mixed-methods strategy; structuring was guided by the principle of 'putting like with like', allowing related findings to be 'hung on the same branch of the Christmas tree'.

Mixed-methods approach

Knowledge was assembled through four complementary methods. First, we extrapolated from tested crime science theory and evidence syntheses (e.g. Bowers and Guerette, 2014), combined with SCP principles derived from the project team's applied research experience. Second, we conducted a Realist review of academic and grey literature on terrorist attacks and interventions, prioritising theoretical plausibility of causal mechanisms over effect sizes, which were largely unavailable. Experience-based knowledge was included where clearly articulated and plausible. Searches covered 15 bibliographic databases and extensive consultation with organisations and experts, yielding 409 relevant sources (143 published, 266 grey), of which 139 were reviewed in depth. Third, fieldwork comprised visual audits and interviews at four complex stations across EU member states, involving security staff, police, and site managers, addressing incident management, partnerships, resources, interventions, good practice, and concerns. Fourth, insights emerging during rapid prototyping with security managers were incorporated iteratively.

Given the absence of rigorous evaluative evidence, Campbell-style systematic review standards were unattainable. We therefore developed a graded evidence scale for literature and fieldwork findings: best practice (experimental comparative designs); good practice (observational or simulation designs); potentially good practice (expert consensus); highlighted practice (expert opinion); and practices to avoid (supported by moderate-to-strong evidence or expert consensus).

Structuring the knowledge findings

To support knowledge synthesis and retrieval, we developed two complementary structures: a Conceptual Attack Framework (CAF) to characterise the range of terrorism risks at complex stations, and a Security Action Tree (SAT) to organise intervention knowledge.

Conceptual attack framework

Risk modelling required systematic representation of attack diversity. Drawing initially on the RAND terrorism database (Rand nd), we developed the CAF to cover tactical attack methods (explosion, melee, knife attack, vehicle ramming etc), weapons

(including misused tools), targets (human and material), and attack procedures. Each dimension comprised approximately a dozen categories, implying a huge number of possible attack configurations and underscoring the need for structured, contingency-based guidance for station security managers. Figure 1 shows the tactical attack method tree and Figure 2 a section of the tactical attack procedures.

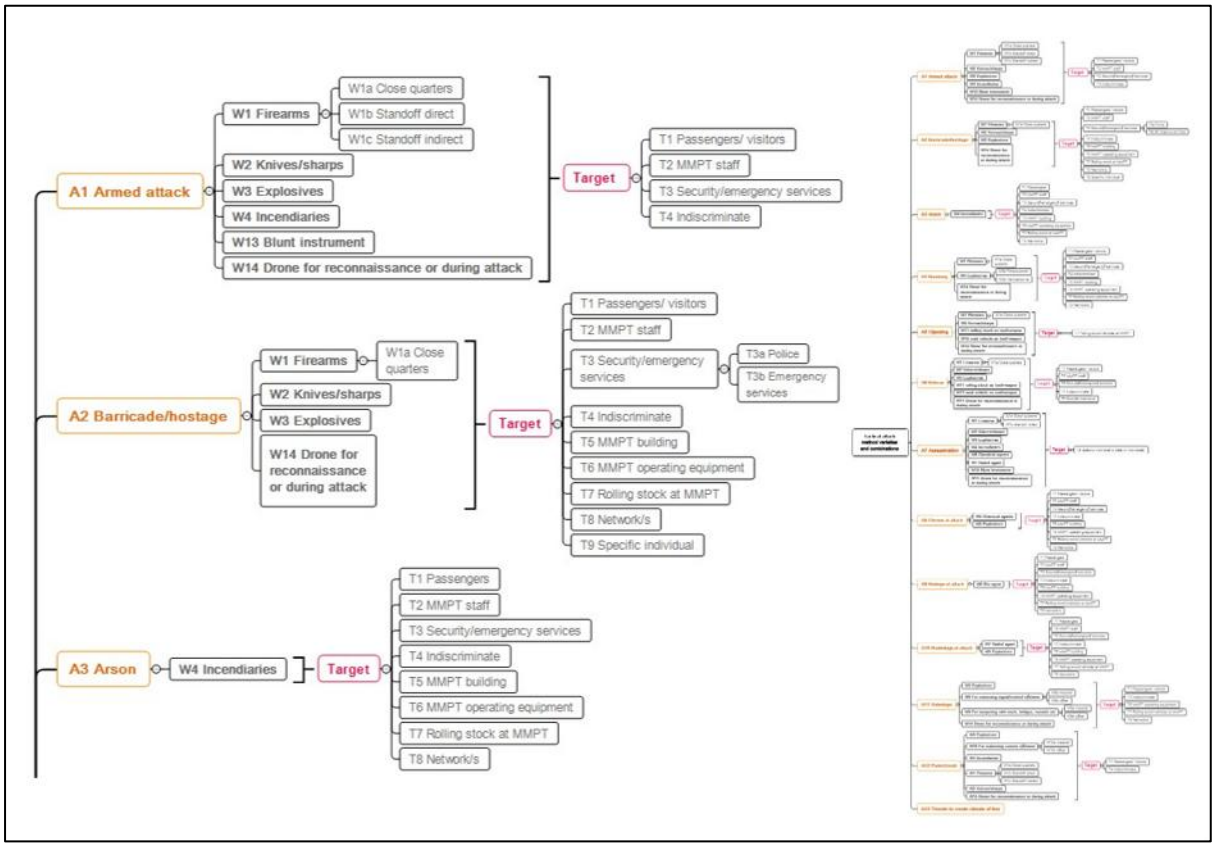

Figure 1 Conceptual Attack Framework – Tactical Attack Methods

Based on RAND Database, showing extract (L) and full tree (R)

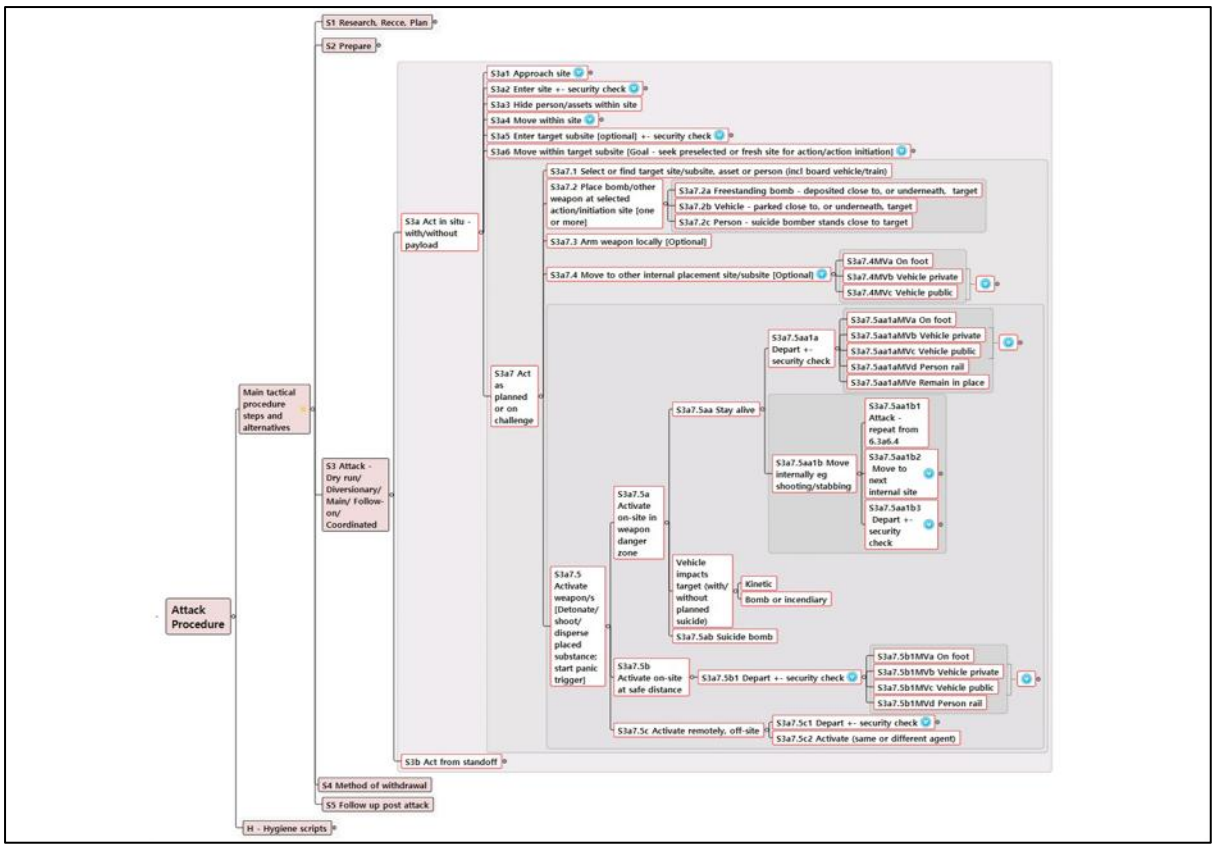

Figure 2 Conceptual Attack Framework – Tactical Attack Procedures

Some steps collapsed for space purposes

While broadly consistent with Clarke and Newman's (2006) four pillars of terrorist opportunity, the CAF substantially extended these by incorporating detailed attack procedures derived from UK's Project Griffin.[3] This yielded some 11 generic action stages, from reconnaissance to entry, movement, attack, and exit, which were adapted and further decomposed for complex station contexts.

Security Action Tree

Intervention findings varied widely in scope, specificity, level, quality, and source, ranging from tactical measures (e.g. invacuation) to organisational capacity-building (e.g. staff training). To make this material accessible, findings were organised graphically in a Security Action Tree. Its structure drew eclectically on crime science

[3] A programme to mobilise commercial security staff to be alert and respond to terror threats on their premises: https://www.gov.uk/government/publications/project-griffin/project-griffin now incorporated within ACT Awareness.

frameworks[4] but was organised by the 5Is process model (Ekblom, 2011)[5]: Intelligence, Intervention, Implementation, Involvement, and Impact/process evaluation. Where possible, entries were linked to intended causal mechanisms, consistent with a Scientific Realist approach. Figure 3 shows a section of the *Intervention* branch of the SAT that derived from the 'target enclosure', an element in the Conjunction of Criminal Opportunity (CCO) referring to a building or other structure within which the target of attack (e.g. passengers) is located.

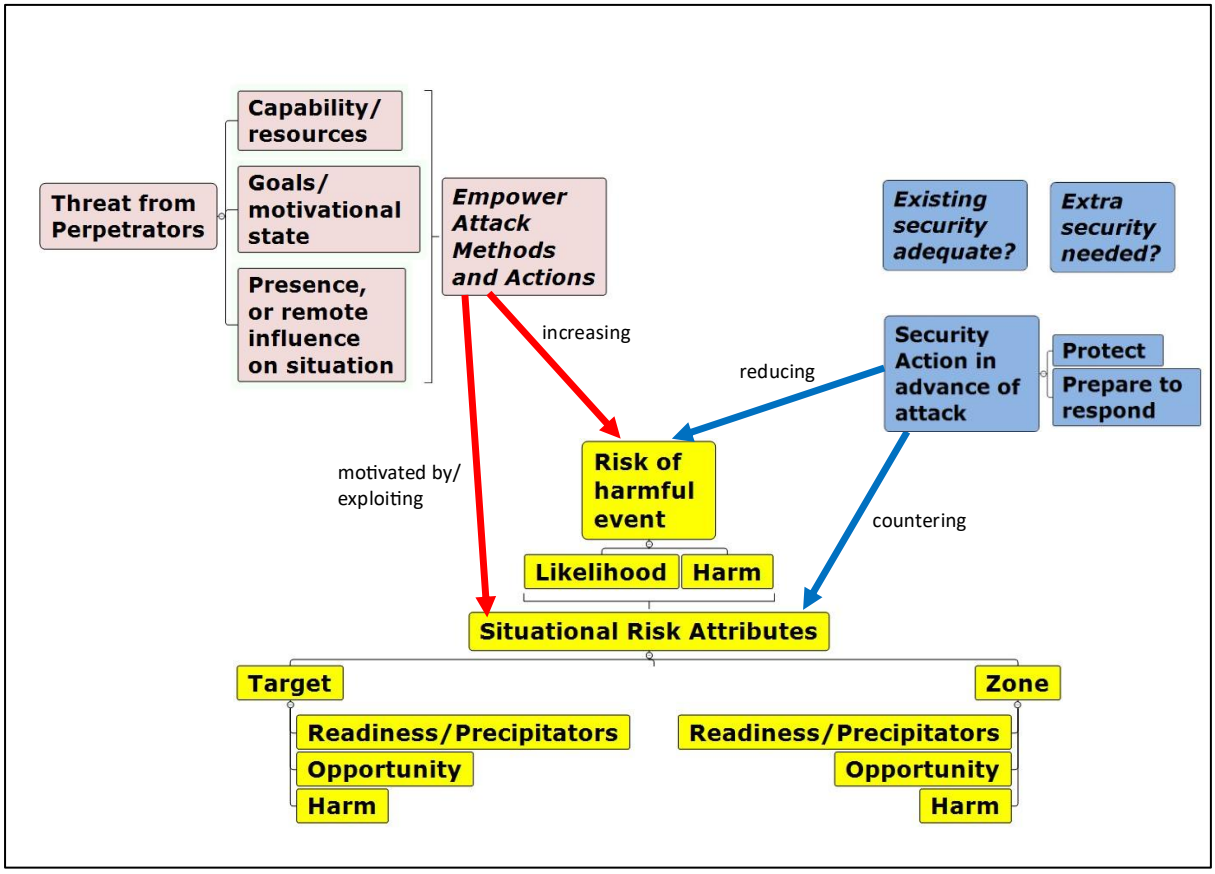

Figure 3 At the Heart of the Toolkit – Concept of Reducing Risk by Matching Security Actions to the Threat

Each SAT node consisted of a concise intervention description, source attribution (fieldwork or literature), a link to fuller documentation, and an evidence quality rating. As a living structure, the tree evolved iteratively as new material emerged. Contradictory findings were explicitly flagged (e.g. glass walls aiding surveillance but reducing ballistic

[4] Including Rational Choice (Cornish and Clarke, 2017), Routine Activities (Felson, 2017), Crime Precipitators (Wortley, 2017), the broad concept of Opportunity (Clarke, 2012), the integrating Conjunction of Criminal Opportunity framework (Ekblom, 2011) and its terrorism adaptation (Roach et al., 2005).

[5] And see https://crimeframeworks.com/5is-intelligence-intervention-implementation-involvement-impact/

resistance), and visualisation helped identify knowledge gaps, following the slogan ‘for gaps, you need maps’. Engagement with security practitioners during tree development generated further refinements and additions.

Towards synthesis: bridging crime science, security, and risk management

Completion of the CAF and SAT enabled delivery of an initial ‘indicative toolkit’, structured as a static flowchart based on the 5Is framework, depicting risk analysis (intelligence), intervention selection, implementation, and involvement. A subsequent, phase 2, project extended this into an interactive toolkit covering both terrorism and more routine station crimes, on the premise that routine use would build capacity and motivation for addressing rarer but more severe terrorist risks. For brevity, this paper focuses on terrorism.

Transforming a risk map and a large body of intervention findings into interactive, process-based guidance posed further challenges. The material required conceptual integration and simplification, bridging crime science and conventional security, and compensating for weak theoretical integration within SCP itself, including the under-specification of opportunity.

Conventional security discourse centres on threat, emphasising offender intent and capability, whereas SCP foregrounds situational opportunity and treats offenders as analytically ‘thin’. Because opportunity leaves offender goals implicit, whereas intent is central to threat, we incorporated more explicit offender-centred concepts. Existing work provided foundations: situational precipitators; Ekblom’s (2007) call to ‘make offenders richer’; the 11 Ds framework (Ekblom and Hirschfield, 2014) which takes the perspective of the offender to Deter, Demotivate, Deflect etc; and the Conjunction of Criminal Opportunity (CCO – Ekblom, 2011), which integrates situational and offender factors, including goals/predispositions, resources, motivational/emotional readiness, perception of risk/effort/reward, and presence. Roach et al.’s (2005) adaptation to terrorism further distinguished between target vectors (people or things harmed to send a message) and target audiences (politicians or public intended to be influenced by the message).

Despite these correspondences, terminological inconsistency remained a major barrier to incorporating insights from the widest range of literature and experience, and to make sense to practitioners with divergent backgrounds in crime science, security and risk management. This was exacerbated by having to translate the toolkit into 15 EU languages. We therefore developed a controlled vocabulary, synthesising crime science and security glossaries, including CCO-based terms, those of Ekblom and Sidebottom

(2008), and the US DHS lexicon (2008). Besides the conventional 'dictionary list' version, we developed a graphical representation[6].

Core concepts

Threat was defined as offender-centred and comprising *resources/capabilities* (Ekblom and Tilley 2000), *goals and intent* (e.g. regarding targets), *motivational and emotional readiness*, and *presence* (physical or remote). Together, these elements describe *empowered, goal-directed offenders*. As is evident, this characterisation contains some of the defining elements of opportunity as discussed above, though the interactional nature of the concept means they straddle both sides of the offender-situation divide. For example, aspects of the situation/target of crime which are rewarding are those that meet the offender's goals to cause harm. This unavoidable entanglement can only be accommodated by terminological convention.

Risk was defined, drawing on risk management, as the *likelihood and harm of adverse events*, incorporating both immediate and cascading consequences. In the toolkit, risk emerges from the interaction of *threat* with a conducive *environment*. *Situational risk attributes*, making the risk of harmful events more (or less) likely, cover both target-related and site-related factors. They include *precipitators, opportunity attributes* affecting effort, risk and reward, and *harm attributes* such as vulnerability and exploitable hazards. This reframes the Routine Activities model in more security-specific terms. Incidentally, the original *likely* offender (Cohen and Felson, 1979) is more useful here than the more recently-favoured 'motivated offender' because it includes capability.

Security was defined as *action to reduce risk arising from criminal threat*, encompassing both *protection* and *preparedness* for response, consistent with the UK CONTEST[7] distinction. Security includes existing provisions and the identification and implementation of additional interventions where risk levels remain unacceptable.

Development of the interactive toolkit

Extending the toolkit beyond a simple 'list–filter–search' design was driven primarily by concerns about cognitive load on users in handling complexity of threat and environmental context. The toolkit therefore had to bridge crime science and security/risk management concepts and guide users stepwise through risk analysis and intervention selection, presenting choices specific to the nature of the terrorism/crime

6 Both available at https://crimeframeworks.com/wp-content/uploads/2023/02/glossary-for-ct-toolkit-complex-stations-ekblom-et-al-2015.pdf.

7 CONTEST – the UK counterterrorism strategy https://www.gov.uk/government/collections/contest.

threat they were considering, the range of local situational risk attributes facilitating the crime and the available repertoire of intervention methods. It also had to remain adaptable across jurisdictions, stations, and evolving threat profiles. These requirements necessitated an interactive, computer-based design.

This section sets out the conceptual architecture, workflow, and key design features of the toolkit. The toolkit's central purpose is to reduce the threat posed by offenders and decrease the risk of harmful events by recommending security actions before an attack occurs. These actions cover both protection of target vectors and preparation for effective first response. Because the interactive phase had limited time and resources and needed to address both terrorism and everyday crimes, the focus was placed on identifying appropriate interventions rather than offering full guidance on implementation, partnership involvement, or evaluation.

Conceptual architecture

The architecture rests on several linked components:

Threat arises from offender capabilities and resources, goals and motivational state, and presence (including remote influence such as hacking). These elements enable attackers to use particular methods and associated actions, organised into a script sequence. Risk increases when the *threat* interacts with *situational risk attributes*. These include properties of both the targets (human, material, or system-centred) and the zones of a complex station where attacks could unfold.

These attributes encompass readiness/precipitating factors, opportunity factors, and harm-generating factors, shaping both offender motivation and the ease with which targets/environments in station zones can be exploited. Security actions reduce risk by addressing offender capabilities (a lesser focus here) and modifying the situational attributes that raise likelihood or harm. The conceptual model was refined through rapid prototyping and iterative testing with security managers from multiple EU Member States, supported by workshops and dissemination through the EU Crime Prevention Network.

Workflow dynamics

Transitioning from a static to a dynamic toolkit required explicit definition of workflow, guiding users through sequential analytic perspectives.

1. Thinking offender and threat
2. Thinking situational risk generated by station design and operation
3. Thinking offender–situation interaction
4. Thinking security (prevention and first response)

Further perspectives (design, management, and long-term future-proofing) were intended but not fully developed due to resource constraints.

Key design features

To manage complexity and user cognitive load, the toolkit incorporates:

- A focus on one kind of crime (here, terrorism), one attack method and one station zone at a time,
- Context-specific conditional dropdown menus
- Clear screen labelling, breadcrumb trails, and progress indicators
- Sidebars summarising user choices and enabling easy backtracking
- Context-sensitive help
- Extensive local customisation: adding regulatory requirements, defining zones, uploading and marking up site maps with structured symbol sets (e.g., seating, ticket barriers)
- Editable dropdowns and free-text fields for site-specific detail and new categories, enabling future-proofing of content
- Translation into 15 EU languages, refined by native-speaking editors
- Online-only access to prevent misuse and support mobile, pause-and-resume use during site walkthroughs

Toolkit in operation

The toolkit supports setup, tutorial, and main risk-analysis sessions.[8]

Thinking offender

Main sessions begin by selecting the *offence type* (terrorism or specific common station crimes), specifying the offender's primary operational goal (e.g. to commit terrorism, pick a passenger's pocket etc). Users then select the relevant *attack method or technique* (e.g. explosives, knife attack, vehicle ramming), which frames subsequent analysis.

Thinking situational risk

Users then switch to a situational perspective, analysing the station in *zones* corresponding to stages of offender movement and action. Zone-based analysis reflects the context dependence of SCP. In *setup* mode Figure 4), users will have uploaded station plans, and on these defined zones (e.g. car park, foyer, platforms), and annotated *attack-relevant features* (e.g. access points, shops, ticket barriers).

[8] Illustrative video run-throughs of these modes are at (https://www.youtube.com/playlist?list=PL3bVqGvUixWRhvlEFyrk4qQgWCFUicUgd).

Users are asked to identify the *risk attributes* of the current zone that might boost the likelihood of, and harm from, offender action in that zone. The risk attributes cover both *attack targets* in the zone (rewarding, provocative etc) and the zone as *environment/enclosure* of the attack procedure in which the target resides and is exposed to risk. The attributes are detailed and applicable to the context of complex stations. They were informed by crime science knowledge, site visits and interviews with security managers; also from scrutiny of accounts of terrorist attacks e.g. in the RAND report (nd). To ease the cognitive load on users, the particular risk attribute menus that drop down are customised for different crime types and attack methods. The zone map and the features entered on it, remain on-screen and act as prompts.

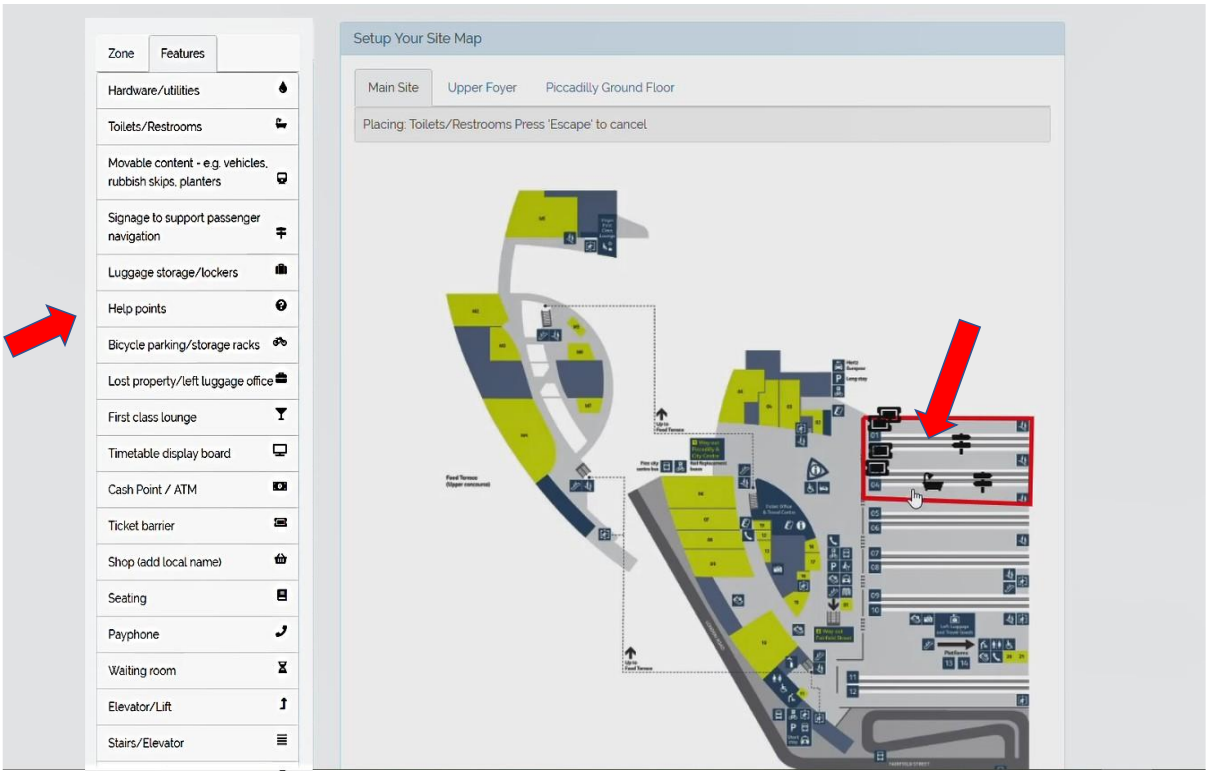

Figure 4 Screenshot of Site Setup – Add Station Map – Insert Boundaries and Features

Thinking offender–situation interaction

The focus then shifts to *offender actions within and around the selected zone*, structured by *crime scripts* and Cornish's (1994) concept of the 'script permutator' – setting out an array of alternative pre-prepared action choices at each stage of the script. The toolkit prompts security managers to think separately about the offender's actions when *approaching, attempting to enter, acting inside and exiting the zone; how they move (on foot, vehicle etc.) any weapons carried; and who/what the targets of the attack could be* (humans including passengers, transport staff, security staff; features listed for zone e.g. destination board, waiting area).

Illustration: hostile vehicle ramming

This example demonstrates how the toolkit analyses and responds to a hostile vehicle ramming attack in a station foyer. The vehicle serves as the primary weapon, and the offender approaches, enters, acts within, and exits the zone using a car or larger vehicle. Key preparatory actions include concealing intent, orienting toward the entrance, identifying obstacles, and accelerating towards the target. Figure 5 shows a truncated screenshot of offender actions in one zone.

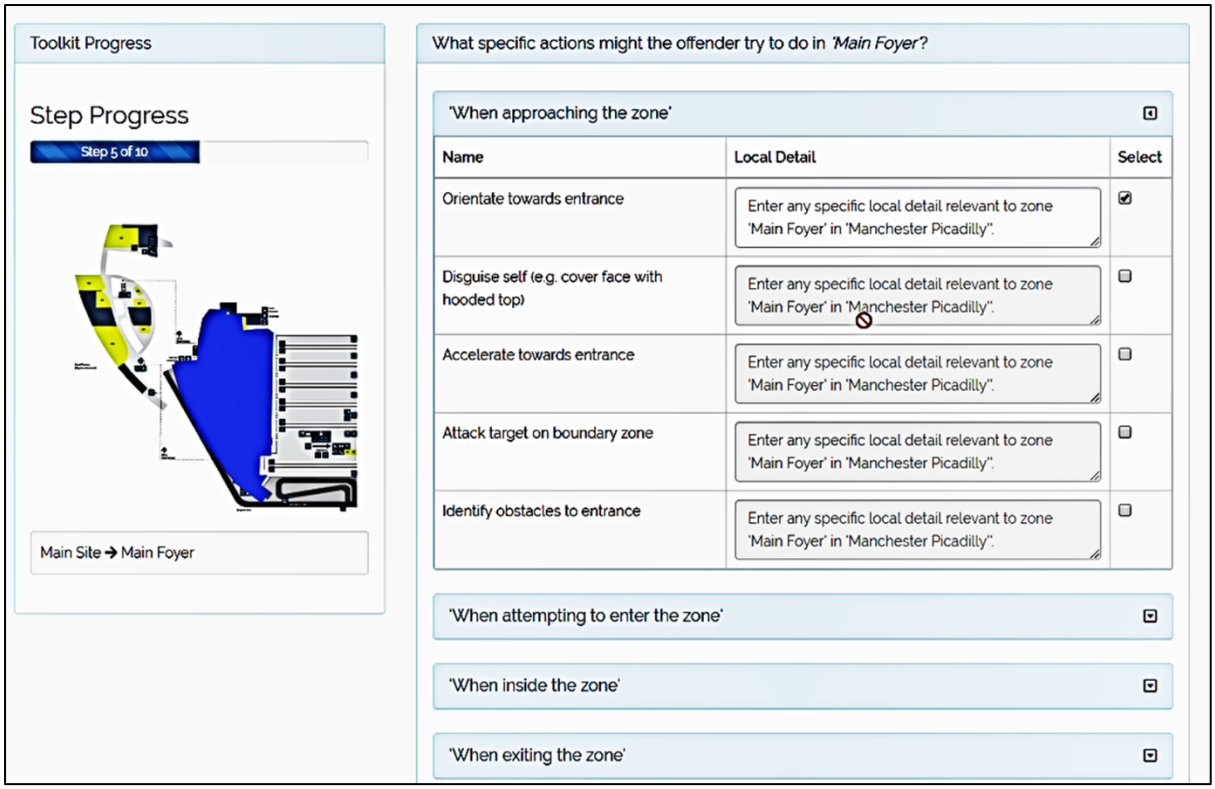

Figure 5 Offender Actions in Zone to Enact Hostile Vehicle Attack Method

The toolkit identifies situational risk attributes that make such an attack more likely or more harmful. Likelihood increases where the foyer allows easy vehicle movement, has weak screening at entry points, lacks robust barriers, or contains inadequate shelter or evacuation routes. Figure 6 shows a truncated screenshot of some of the opportunity factors in the zone.

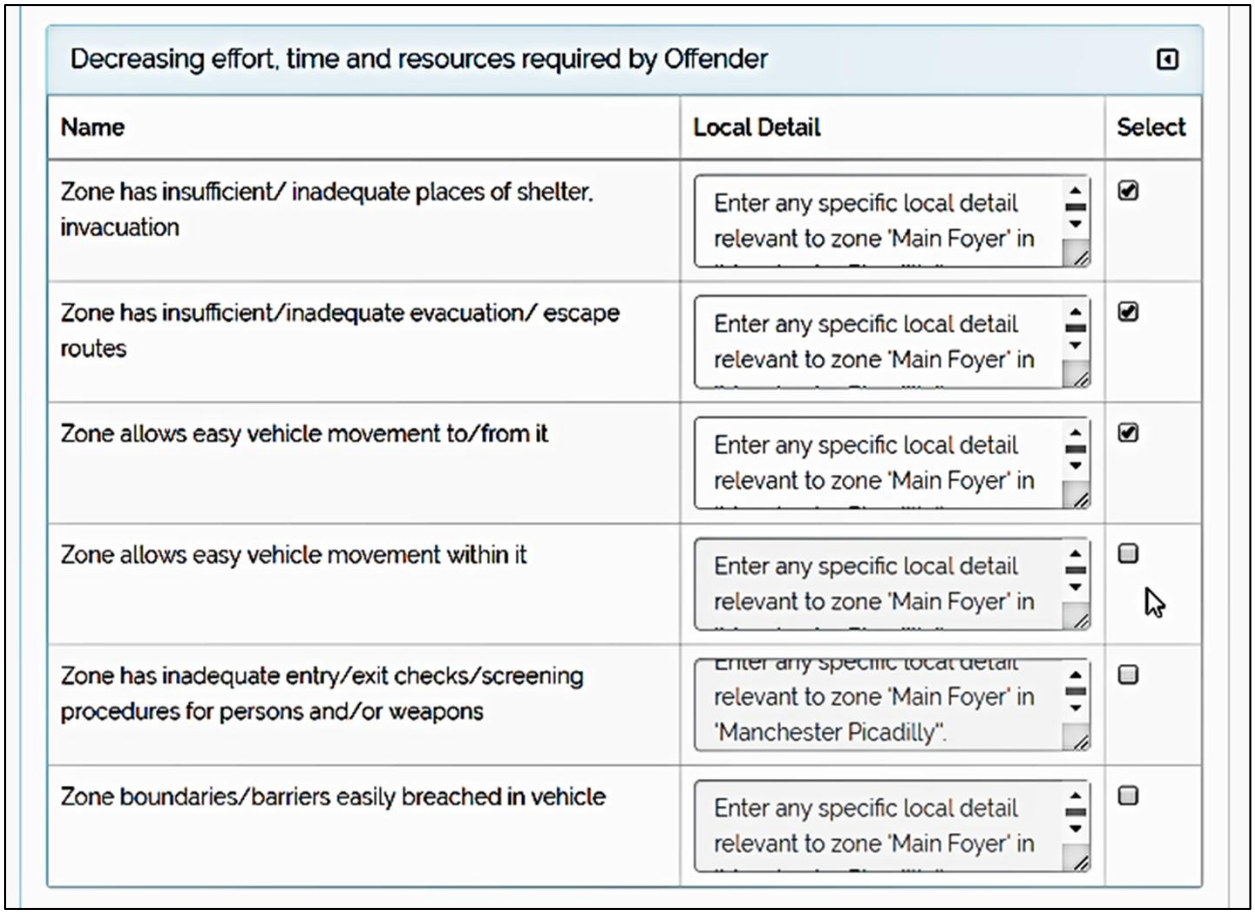

Figure 6 Opportunity Factors in Zone to Enact Hostile Vehicle Attack Method

Additional prompting factors may trigger or intensify offending. Harm escalates with dense crowds and exploitable hazards (e.g., glass, structural weaknesses, combustible materials).

After risks are identified, users review *existing security measures* and decide whether they offer sufficient protection/preparation. If not, the toolkit provides context specific *security options*, such as reorganising queues, relocating hazards, dispersing crowds, redesigning traffic flows, altering assets to reduce harm, or conducting regular evacuation drills. Users can note *local details* and *assign responsibility* across the various organisations operating within a complex station. Figure 7 shows part of the menu of suggested security interventions against risks, provocations and harms identified in the zone.

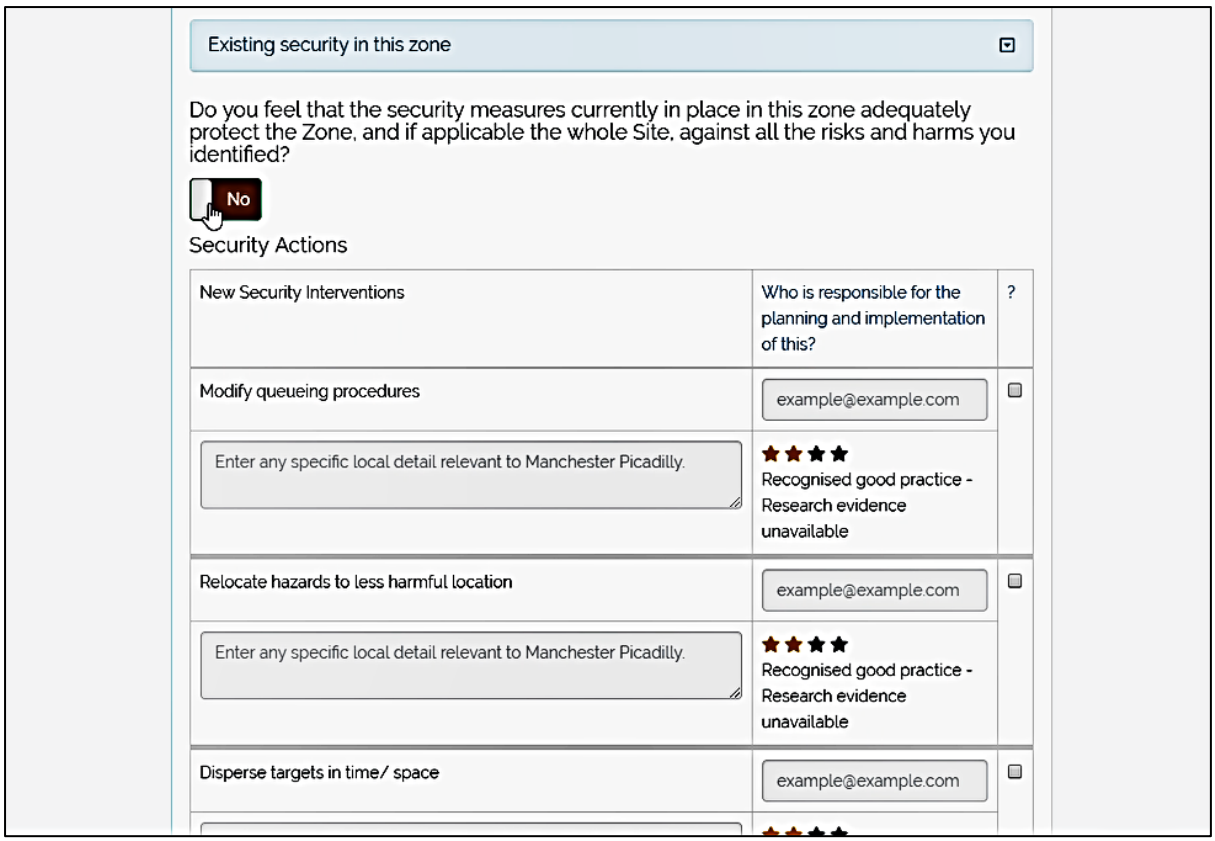

Figure 7 Security Action against Hostile Vehicles – Partial Listing of Interventions against Risks, Provocations, Harms Identified in Zone

A final *session summary* consolidates the analysis: the focus of the session (e.g., hostile vehicle attack), the risks identified for the foyer, relevant zone users and features, offender actions and weapons, and selected security recommendations. Users are also reminded to consider legal requirements, operational needs, and potential conflicts with existing measures.

Discussion

Implications for evidence-based approach

Since developing the toolkit, additional empirical work on situational risk factors for terrorism has emerged. For example, the EVIL DONE framework has been extended (e.g., Marchment and Gill, 2022 added Tolerable and Relevant), while other studies have questioned its applicability in particular contexts like Northern Ireland (Monaghan et al., 2023). One advantage of the toolkit was that it was intentionally designed to be updateable, and thus future iterations can evolve with the research evidence.

However, the fundamental evidentiary deficit in SCP remains. Freilich et al. (2019) report that most SCP-terrorism studies are non-empirical, with only a small minority using quantitative or qualitative methods, and almost none using mixed-methods.

Empirical testing of opportunity-based frameworks remains limited, with little evaluation of several prominent models. Freilich et al. argue for more sophisticated testing of opportunity 'pillars' but note that the scarcity of empirical studies likely reflects the difficulty of accessing the highly sensitive data required. They also highlight the broader challenge researchers face in obtaining official datasets and suggest creative strategies to overcome these barriers.

Developing rigorous 'what works, where' resources such as the EMMIE toolkit is already demanding. Constructing an interactive toolkit for terrorism and crime reduction from highly heterogeneous evidence, and across complex station environments, is equally challenging. The added complexity of guiding users through structured, site-specific threat and risk assessments increases the value of interactivity: it ensures systematic coverage, contextualisation, reduced cognitive load, and durable documentation for organisational learning. Key design lessons include the importance of mixed-methods research, disciplined conceptual and terminological clarity, early development of glossaries or ontologies, rapid user-centred prototyping, and early integration of multilingual translation, which proved feasible in an academic setting.

Limitations and future directions

Beyond the limited evidence base, project scope was constrained by time, funding, and limited institutional capacity to actively promote uptake. In an ideal scenario, we would have extended guidance to cover implementation and involvement; conducted more extensive field testing; obtained systematic feedback on uptake and use; and undertaken formal evaluation of toolkit impacts, using intermediate outcomes or routine crime measures as proxies for rare terrorist events.

More generally, future work would benefit from: contractual arrangements that support feedback, maintenance, and iterative improvement; employing the toolkit as a structured learning engine to capture ongoing user experience; broader dissemination within crime science and security communities; and ongoing updating to incorporate emerging threats, crimes, and research evidence, to ensure adaptability and future-proofing.

Theoretical contribution: opportunity and beyond

Developing the toolkit required strengthening and extending the concept of opportunity in several ways. First, we grounded the traditionally intuitive, largely unexamined notion of opportunity more firmly within crime science. This was achieved by systematically linking it to established frameworks concerned with places, offender scripts and methods of attack, decision-making, situational precipitators, and routine or non-routine movements. The toolkit operationalises these links, giving practitioners and researchers a concrete representation of how these elements interact in real situations.

Second, by bridging crime science with conventional security—which centres on threat—we reframed opportunity as an interaction between offender and environment rather than a property of the situation alone. This required the explicit inclusion of offender goals, intent, motivation, resources, perceptions of risk and effort, and physical or remote presence. The resulting model provides a more holistic, system-oriented account of how crimes and terrorist attacks occur, including those involving highly motivated or 'advanced persistent threat' actors.

Although this reconceptualisation increases theoretical complexity, embedding it within an interactive toolkit *simplifies* practice by enabling structured cognitive scaffolding. This exemplifies Ashby's (1956) Law of Requisite Variety: representations must be sufficiently complex in themselves to manage highly complex systems.

Earlier scholars, including Clarke and Felson, recognised the limitations of overly simple opportunity models, noting that traditional formulations failed to capture the full person–situation interaction. Cohen and Felson's (1979) emphasis on 'likely' offenders—incorporating both motivation *and* capability—expressed this nuance, but it has often been lost in later applications of situational prevention. This narrowing arose partly from the adoption of the 'good enough theory' approach (Smith and Clarke, 2012), designed to prioritise utility over completeness. Simple explanations were seen as adequate for local crime problems typically addressed by resource-limited agencies. But for complex stations—highly dynamic environments subject to sophisticated terrorist threats—such parsimony is insufficient. The challenge is even greater in domains such as cybercrime and hybrid threats, where offender capabilities and system complexity far exceed earlier assumptions.

And more generally speaking, excessive parsimony has its limits: Einstein said 'Everything should be made as simple as possible, but not simpler'[9] and Bouhana (2013:683) 'The move towards a more dynamic, interactionist model has been resisted, for fear that it would compromise RCP's radical parsimony, a condition of its heuristic usefulness.' We believe that theory and theoretical constructs should be advanced at the *leading edge* of thought rather than constrained by the *trailing edge* of immediate practical utility; but this poses no barrier to intelligently simplifying the advanced model for the guidance of practitioners. The principle of 'appropriate complexity' (Ekblom 2011; Norman 2013) can apply to every practical use context.

Conclusion

In addressing the challenge of terrorism and crime prevention at large, complex transport hubs, we integrated opportunity-based crime science with threat- and risk-

[9] Einstein: This is on many quotation websites but none gives original source. Bouhana (2013) cites a more elaborate version.

centred security approaches, producing an interactive toolkit fit for contemporary and emerging challenges. In doing so, we believe we have advanced the conceptualisation and practical application of opportunity, strengthening its integration with crime science and security/risk management.

50 years on, the concept and the use of the term 'opportunity' (and its reduction) has continued, largely unexamined, within situational prevention. That this is so, can be attributed to intuitive, vernacular appeal; the preference, within crime science, for extreme simplicity not only in practice but also research; and the existence of the more formalised theoretical perspectives (Rational Choice, Routine Activities) that do most of the conceptual heavy lifting. Opportunity could thus be viewed as a 'Peter Pan' concept: while extremely lively and helpful, it has still to mature, and it floats above fundamental ground-level theories. Yet, as has been shown, opportunity as extended and developed within a more integrated theoretical approach can be taken forward in meeting the challenge of constructing an interactive toolkit fit for the purpose of guiding security managers through extremely complex and challenging risk analysis, decision-making and intervention design.

Note: Official enquiries about obtaining the toolkit for tackling terrorism and crime at complex stations to:

MOVE-EU-LANDSEC@ec.europa.eu cc eucpn@ibz.eu

References

All links accessed [date] 2026.

Ashby, W. (1956). *An Introduction to Cybernetics*. London: Chapman and Hall.

Bouhana, N. (2013). 'The reasoning criminal vs. Homer Simpson: Conceptual challenges for crime science.' *Frontiers in Human Neuroscience, 7*:682-692.

Bowers, K. and Guerette, R. (2014). Effectiveness of Situational Crime Prevention. In: Bruinsma, G., Weisburd, D. (eds) *Encyclopedia of Criminology and Criminal Justice*., New York: Springer.

Brantingham, P.J., Brantingham, P.L. and Andresen, M. (2017). 'The Geometry of Crime and Crime Pattern Theory.' In R. Wortley and M. Townsley (Eds.) *Environmental Criminology and Crime Analysis* (2nd edition). London: Routledge.

Clarke, R. (1997). *Situational crime prevention: successful case studies*. Harrow and Heston.

Clarke, R. (2012). Opportunity makes the thief. Really? And so what? *Crime Science,* 1:1-9.

Clarke, R. (2017) 'Situational crime prevention.' In Wortley, R. and Townsley, M. (eds) Environmental criminology and crime analysis, 2nd edn. Willan Publishing, Cullompton, UK, pp 286–303.

Clarke, R. and Newman, G. (2006). *Outsmarting the terrorists*. Praeger Security International.

Cohen, L. and Felson, M. (1979). 'Social change and crime rate changes: A routine activities approach'. *American Sociological Review,* 44: 588-608.

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

Cornish, D. and Clarke, R. (2017). 'The Rational Choice Perspective.' In R. Wortley and M. Townsley (Eds.) *Environmental Criminology and Crime Analysis* (2nd edition). London: Routledge.

DHS (2008). *DHS Risk Lexicon.* https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf.

Ekblom, P. (2007). 'Making Offenders *Richer*' in G. Farrell, K. Bowers, S. Johnson and M. Townsley (Eds.), *Imagination for Crime Prevention: Essays in Honour of Ken Pease.* Crime Prevention Studies 21: Monsey, N.Y.: Criminal Justice Press.

Ekblom, P. (2011). *Crime Prevention, Security and Community Safety Using the 5Is Framework.* Basingstoke: Palgrave Macmillan. See also https://crimeframeworks.com/conjunction-of-criminal-opportunity-2/.

Ekblom, P. (2012). 'Conceptual and Methodological Explorations in Affordance and Counter Terrorism' in Taylor, M. and Currie, P. (Eds.) *Terrorism and Affordance*. London: Continuum.

Ekblom, P. (2017). 'Technology, opportunity, crime and crime prevention – current and evolutionary perspectives' in B. Leclerc and E. Savona (Eds.) *Crime Prevention in the 21st Century*. New York: Springer.

Ekblom, P. and Hirschfield, A. (2014). 'Developing an alternative formulation of SCP principles – the Ds (11 and counting).' *Crime Science*, 3:2.

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.

Ekblom, P. and Tilley, N. (2000). 'Going Equipped: Criminology, Situational Crime Prevention and the Resourceful Offender' *British Journal of Criminology* 40:376-398.

Felson, M. (2017). 'The Routine Activity Approach.' In R. Wortley and M. Townsley (Eds.) *Environmental Criminology and Crime Analysis* (2nd edition). London: Routledge.

Freilich, J., Gruenewald, J. and Mandala, M. (2019). 'Situational Crime Prevention and Terrorism: An Assessment of 10 Years of Research.' *Criminal Justice Policy Review Criminal Justice Policy Review,* 30:1283-1311. https://doi.org/10.1177/0887403418805142.

Gibson, J. (2014). *The Ecological Approach to Visual Perception: Classic Edition*. Psychology Press.

Johnson, S., Tilley, N. and Bowers, K. (2015). Introducing EMMIE: an evidence rating scale to encourage mixed-method crime prevention synthesis reviews. *Journal of Experimental Criminology* 11:459–473.

Lum, C., Kennedy, L. and Sherley, A (2006-9). *The Effectiveness of Counter-Terrorism Strategies. A Campbell Systematic Review*. Philadelphia: The Campbell Collaboration.

Marchment, Z., & Gill, P. (2022). Spatial decision making of terrorist target selection: Introducing the TRACK framework. Studies in Conflict & Terrorism, 45(10), 862–880. https://doi.org/10.1080/1057610X.2020.1711588.

Mayhew, P., Clarke, R., Sturman, A. and Hough, M. (1976). *Crime as Opportunity.* Home Office Research Study 34. London: Home Office.

Monaghan, R., Slocombe, B., McIlhatton, D. and Cuddihy, J. (2025). 'Examining the relevance of 'EVIL DONE' to the current terrorist threat landscape in the United Kingdom', *Behavioral Sciences of Terrorism and Political Aggression* 17:285-311, DOI: 10.1080/19434472.2023.2220017 .

Newman, G. and Clarke, R. (1997). 'Reconsidering the role of opportunity in situational crime prevention.' In G. Newman and R. Clarke (Eds.) *Rational Choice and Situational Crime Prevention: Theoretical Foundations.* London: Routledge.

Norman, D. (2013). *The Design of Everyday Things: Revised and Expanded Edition* (2nd Edn.). New York: Basic Books.

Pawson, R. and Tilley, N. (1997). *Realistic Evaluation*. London: Sage.

RAND (nd) *RAND Database of Worldwide Terrorism Incidents. https://www.rand.org/nsrd/projects/terrorism-incidents.html*

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

Silke, A. (2001). The Devil You Know: Continuing Problems with Research on Terrorism. *Terrorism and Political Violence*, *13*:1-14. https://doi.org/10.1080/09546550109609697

Smith, M. and Clarke, R. (2012). 'Situational Crime Prevention: Classifying Techniques Using "Good Enough" Theory.' In D. Farrington and B. Welsh (Eds) *The Oxford Handbook of Crime Prevention*. Oxford: OUP. Pp 298-315.

Wortley, R. (2012). 'Affordance and situational crime prevention: Implications for counter-terrorism.' in Taylor, M. and Currie, P. (Eds.) *Terrorism and Affordance*. London: Continuum.

Wortley, R. (2017). 'Situational precipitators of crime.' In R. Wortley and M. Townsley (Eds.) *Environmental Criminology and Crime Analysis* (2nd Edn.). London: Routledge.