Crime Prevention through Product Design

Paul Ekblom[1]

Ekblom, P. (2017). 'Crime prevention and product design' in N. Tilley and A. Sidebottom (Eds.) *Handbook of Crime Prevention and Community Safety* (2nd ed). London: Taylor and Francis.

Abstract

This chapter focuses on the design of three-dimensional products as a means of preventing crime. It first defines design, and illustrates how this intersects with crime. It continues by discussing a range of challenges faced by designing products against crime; then describes how design can respond to these challenges, drawing simultaneously on design know-how, and the emerging discipline of crime science. There is special emphasis on the 'people' side of undertaking and using design as here is where difficulties commonly arise. This is followed by a discussion of evidence for the effectiveness of designing products against crime.

Introduction

Design is creativity deployed to a specific end (HM Treasury, 2005). It is a generic *process* of creating some new or improved product which:

- Is materially or logically possible to make
- Is fit, or fitter than predecessors, for some specified principal purpose
- Does not significantly interfere with subsidiary purposes or with wider requirements of social and economic life and the environment (adapted from Booch, 1993)

Design is a wide-ranging field. Besides the creation of three-dimensional products (the focus of this chapter) it covers the creation of the built environment (see chapter by Armitage in this volume), graphics, communication, systems, and services; even procedures and social innovation. Design may include an engineering dimension but it is much more than just 'technology'.

Crime is equally wide-ranging, from antisocial behaviour to terrorism. It is directed against diverse human, material and informational targets. It intersects with design in many ways:

- *Poorly-designed products* may be vulnerable to crime (e.g. cars that are easily broken into); they may generate vulnerable behaviour among users (e.g. ATMs that make it hard to conceal the PIN code entered on the keyboard; or 'guarantee registration' postcards helpfully displaying the name and address of the purchaser of an expensive domestic device); they may provoke crime (as with 'machine-rage' damage to user-unfriendly computers, or annoying advertising posters that 'call out' for graffiti); or

[1] Grateful to the Editors for some useful suggestions.

they may be misused (e.g. beer bottles which can be broken to form weapons, or colour photocopiers which can copy banknotes)

- Products may be explicitly *designed to resist criminal attack* (such as laptops with an inbuilt attachment for an anchor cable which can be locked to furniture), or to *protect other items or people* against crime (e.g. a personal attack alarm)
- Generic *process-design* can be used to improve how crime prevention is undertaken, and to devise ways of capturing, organising and sharing knowledge of practice; this even extends to deliberate design of the terms and concepts within crime prevention.

This chapter discusses diverse challenges faced by designing products against crime: conflicts and tradeoffs, the issue of intelligent replication, the phenomenon of 'crime harvests' when new products emerge that are 'naïve to crime', and how design has to cope with social and technological change and adaptive offenders. It then goes on to describe ways that design can respond to these challenges, drawing on both design know-how, and the emerging discipline of crime science. In so doing, it presents both practical examples of products and processes, and frameworks for conceptualising these in systematic and disciplined ways which can support (rather than strangle) creativity and innovation. Special attention is devoted to Involvement – the 'people' side of crime prevention – and the motivation of designers to tackle crime through their products. This is followed by a discussion of impact evaluation and evidence for the effectiveness of designing products against crime.

The challenges of designing products against crime

One might think that designing a product to resist crime, or to help protect against it, was a straightforward task, like fitting a bolt to the door of a house. Although some design tasks are simpler than others, design as a whole faces significant challenges. Failure to address these can lead to products which do not fulfil their intended function, interfere with other functions and perhaps make life worse for honest people, rather than better.

Tradeoffs and conflicts

Incorporating a security function into a product – such as resistance to theft or deliberate damage – can make them inconvenient, or user-unfriendly. People often struggle to remember a PIN code at a cash machine, or to operate an awkward lock on a door. With complex entry-phone systems, users may bypass the security, for example by propping the door open with a fire extinguisher. Thus they may end up worse-off than with no formal security measure installed.

Some security features or products can be effective but ugly – for example a steel cage designed to protect a classroom computer projector from theft (e.g. www.paritymedical.com/mounts-projector-security-enclosed-cage.htm). Aesthetics apart, the 'fortress' image of such products may prompt fear of crime.

A product whose security function is energy-hungry, for example through intensive lighting, has an undesirable carbon footprint. Other products, which include RFID (radio frequency identification) tags for anti-shoplifting purposes, may enable information about the purchaser's choices and movements to be picked up and used inappropriately, violating their privacy.

Equally unethical is a security product that is deliberately discriminatory. A notorious example in the UK recently was the ‘Mosquito’ device which was marketed to discourage young people from hanging around outside shops, putting off customers. It worked by generating unpleasant noise at such a high pitch that only the young could hear it. The measure was roundly criticised for violating human rights and discriminating on grounds of social category rather than behaviour (see www.theguardian.com/society/2010/jun/20/teenager-repellent-mosquito-banned-europe)).

Few designs that are physically unsafe get through the testing procedures nowadays associated with, for example, motor vehicles, but immobilisers and steering locks do have the theoretical potential to accidentally activate when the vehicle is in motion.

Finally, cost is a major issue. And costs, and complexity, can be hidden by the bright light of an apparently clever idea for security. For example, putting a wireless tracker device into a car may be straightforward, but it will only work as a practical system via a process of registration, data storage, equipping the police with scanners and access to the register, and making demands on their time.

All these examples are instances of *bad* design. This can happen for several reasons. First, because the product has simply been ‘engineered’ without careful consideration of the context of use and of wider requirements; second, because disproportionate priority was accorded to security by, say, the police; third, because a professional designer was not employed; or fourth, because the manufacturers restricted the scope of the considerations that the designer was paid/allowed to address.

It is, fortunately, possible to design effective products which serve security and any other purpose (e.g. serving as a means of transport), and are simultaneously safe; user-friendly and undemanding of excessive effort or time; aesthetically-pleasing and reassuring; have a small carbon footprint; do not inappropriately discriminate or socially exclude categories of people; do not interfere with mainstream business requirements; are no more complicated to manufacture than insecure counterparts; and are of a cost that is proportionate to risk and/or to market requirements.[2]

The essence of good design is to use creativity, insight and professional research and design skills to reconcile conflicting requirements, and to do so without an unsatisfactory compromise. An illustration of a ‘creative leap’ (albeit one that neglects aesthetics) is the American style of fire escape (Figure 1) This lets occupants safely leave the building in an emergency but simultaneously, deliberately makes it difficult for burglars to break in. It works by the bottom run of steps being suspended well above ground level, and made to descend by the weight of the fleeing occupants.

[2] Other case studies of crime-resistant products are at www.designcouncil.org.uk/resources/report/design-out-crime-case-studies.

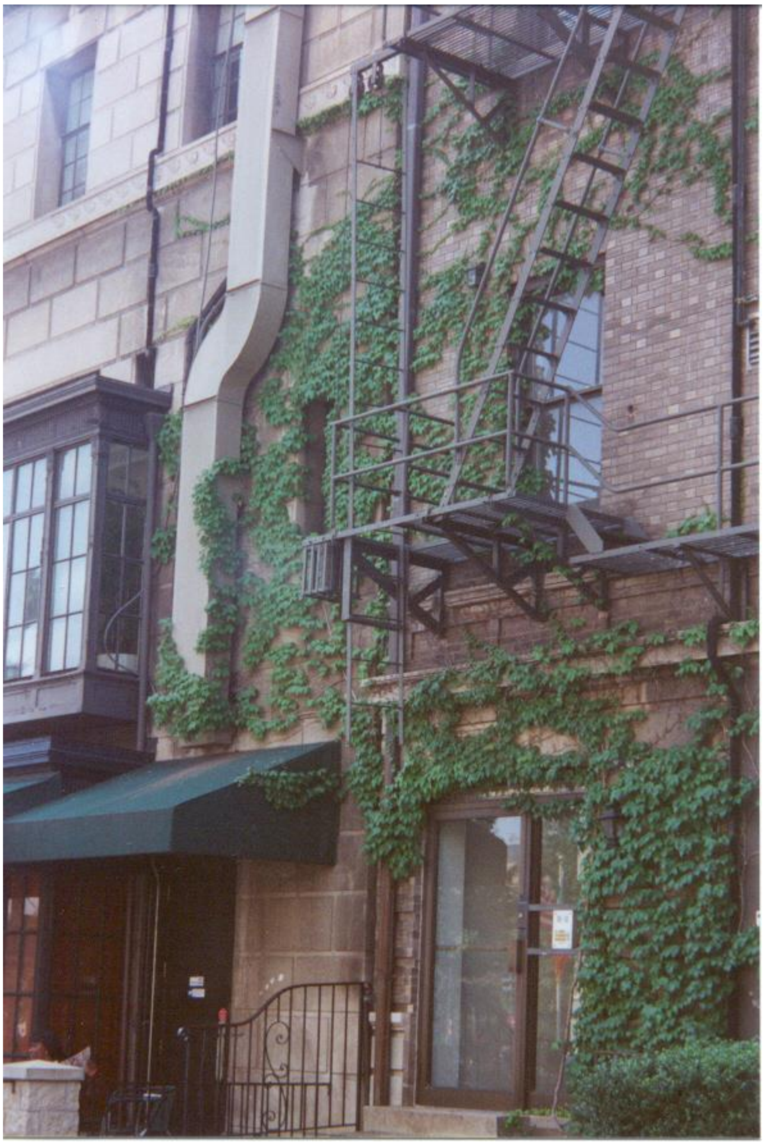

Figure 1 New York fire escape [photo: author]

Besides creativity, the fire escape demonstrates another generic principle of design against crime – being *user-friendly whilst abuser-unfriendly*. This requires differentiation between the two parties, the challenge being to create a design that responds to very specific or subtle distinctions. This is a problem when the very same properties that make a product attractive and convenient to legitimate users, make it attractive and, say, easy to steal for thieves – for example, the high value, light weight and concealability of smartphones can serve both parties. In such circumstances it is often information-based functions which support the desired capacity for differentiation, for example passwords.

Discrimination of the wrong kind, as with the 'Mosquito' devices, can be replaced by a more acceptable, universal measure. For example, an English shopping centre had problems with young people lingering by the parapet of the upper floor, and throwing empty drink cans or spitting on people at the lower level. The manager, in an imaginative home-made design, had the floor by the parapet re-laid at a slight slope, and installed heat-radiant lights (the kind fitted in bathrooms) so anyone who spent too long there felt uncomfortable, and moved on. The inconvenience was universal, but was judged (albeit from a commercial perspective) only to have a significant adverse impact on those loitering and potentially causing nuisance.

Invisibility of the security function is another benefit of good design. The shopping-centre measures just described had the advantage of not being consciously noticeable as a security intervention; thus, they were less likely to provoke attempts by the offenders to circumvent them, or even retaliate. Second, the measures were either entirely invisible to ordinary shoppers passing by, or if they did detect them, they did not receive the message 'this is an insecure place where the managers have had to take preventive action'. Equally invisible is the security function of the three-metre high metallic letters spelling ARSENAL at the London football team's Emirates Stadium (www.arsenal.com/emirates-stadium/emirates-stadium-history/key-facts). These are in fact designed to stop a large truck laden with explosives from crashing through into the crowd, though this is not obvious and hence does not engender anxiety among visitors.

Forgettability takes the human out of the loop, and is useful where a design removes the need for the user to remember and to make the effort to lock the door, shut the computer down, or (on older vehicles) to telescope the car aerial shut and perhaps lock it, as protection against vandalism.

Where functions cannot be thus hidden or forgotten, designers often make a deliberate *feature* out of them. One of the pleasures of strolling round traditional quarters in Latin American towns is the profusion of beautifully-designed window grilles (Figure 2).

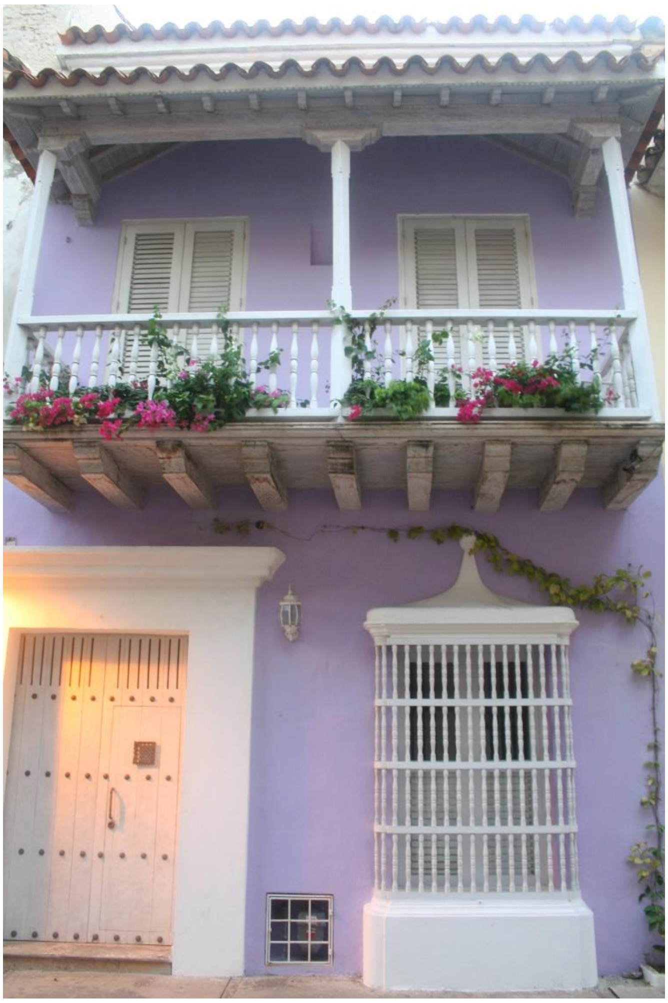

Figure 2 Traditional window grille, Cartagena, Colombia [photo: author]

Crime resistant designs need not cost much. A road sign indicating the ‘River Uck’ was frequently vandalised by the addition of a letter ‘F’, to make a well-known obscene word. The local council commissioned new signs, at very little cost, where the sign plate is indented to remove the space for the offending letter (Figure 3).

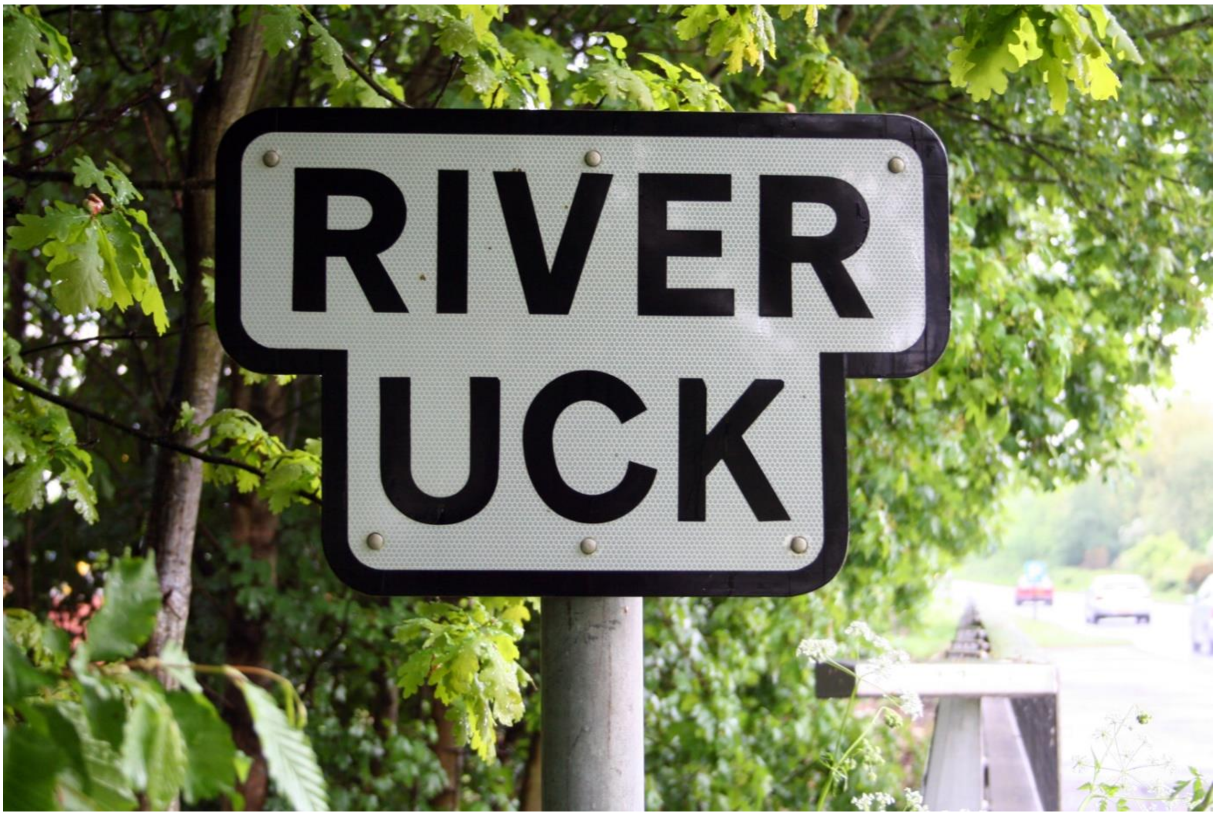

Figure 3 Graffiti-resistant road sign [photo: author]

Intelligent replication and flexibility

'Cookbook copying' of successful crime prevention projects often fails to deliver successful results, a theme followed-up below. An attempt to install an electronically-controlled secure parking facility for bicycles at a North London metro station was a close copy of a success-story in Belgium. In the UK however it met with user resistance because there was no culture of paying for bike parking, or of leaving one's bike at some distance from the station. A more general example of 'replication failure' was described by Tilley (1993) who studied several attempts to emulate a successful anti-burglary project conducted in one neighbourhood in the north of England. None of the replications worked. This was because the replicators copied the end-product (i.e. the preventive measures taken in the original project) rather than the intelligent process of identifying and addressing their own specific problem, and generating their own solution based on tested *principles* of prevention, whose practical realisation was then customised to the local context. Much as it is important to get designers 'thinking thief', it is important to get ordinary crime prevention practitioners (in the police or local government, say) thinking like designers.

Crime harvests

No security product or component works well if it is superficially 'bolted-on' to a building or other item of property, as an after-thought. The security requirement has to be identified and incorporated in the design process at an early stage, so that a fully-integrated approach can be taken; the scope for 'design freedom' offering creative solutions can be enhanced; and trade-offs between multiple requirements or drivers can be optimised, perhaps through iterative testing of prototypes.

Unfortunately, many products are placed in the market, which have been designed in a way that is 'naïve' to crime. Classic examples here are insecure motor vehicles (up to the 1980s) and early-model mobile phones. Pease (2001) identifies a process he calls the 'crime harvest'. Here, a phone, say, is designed to be highly portable, full of useful (and not so useful) functions and of relatively high value. As well as attracting legitimate purchasers, these properties tempt thieves, so after the product has begun to awaken demand from the former, it also begins to interest the latter, whether to own it themselves or to sell it on. We thus get a sudden burst of theft or robbery, say, followed by a hasty government attempt to control the outbreak. The haste, and the limited scope for control, mean that retro-fit solutions tend to be expensive, inconvenient, and far from optimal.

Avoidance of crime harvests can never be a perfect art, but it can be helped through anticipation – in particular when designers adopt a 'think criminal' mindset.

Coping with socio-technological change, adaptive offenders and arms races

Today, we inhabit a Heraclitean world of accelerating change, whether this is driven by developments in material or information/communications technology, new business or financial models, conflicts, migrations, climate change, or simply in fashion. As part of this process, products which are successful today, may become obsolete or rejected tomorrow. This applies particularly to products with a security function which is dependent on the maintenance of particular technological or social conditions.

At the simplest, existing security technology can wear out with use – locks may become easier to manipulate as their parts erode. Keys and passwords can 'leak' from sole possession by the legitimate user by various routes; or the code can be cracked. Offenders can learn how to circumvent a particular security feature. For example, car thieves discovered that the alarm sounder on a certain model of luxury car was located just inside the radiator grille, so they used a spray can of quick setting insulation foam to silence the alarm before breaking into the vehicle.

A more complex example is where thieves acquired a wristwatch designed to learn the codes on the remote control of your TV set, and co-opted it for criminal purposes. They would visit a showroom for expensive cars, and when the sales assistant unlocked the vehicle they would covertly record the code with their watch, only to return later to play back the code, unlock the vehicle and disarm the alarm. (The eventual solution was to develop a car immobiliser with rolling codes, that changed on each use in a complex (and to the thief, unpredictable) way, rather like a spy's 'one-time message pad'.) We thus have a situation of adaptive offenders exploiting socio-technological changes: this means that our knowledge of what works now in security is a wasting asset that diminishes over time. To illustrate this, car thieves have recently learned to circumvent the security of keyless top-end models like the Land Rover Evoque in the UK (www.bbc.co.uk/news/technology-29786320). These are currently being stolen so fast that insurers are declining cover unless, say, cars are parked off-street, and primitive security devices like add-on steering wheel locks are fitted.

In fact, we have the conditions for co-evolutionary *arms races* to emerge (Ekblom, 1997, 1999, 2016) between crime preventers and adaptive offenders who innovate, exploit change and enjoy the obsolescence of familiar crime prevention methods. A good illustration (Shover, 1996) is the unfolding history of safes and safe-crackers where, over decades, we have seen a succession of measures and counter-measures emerge such as combination locks, explosives, cutters and laminated casings, where technology has given first one side, then the other, some momentary advantage. More recent arms races have tended to focus on ICT, for example in hacking of computers and networks.

Offender dissemination and innovation are accelerating. Previously, criminal techniques were often acquired in prison, but guides on making bombs or picking locks now regularly appear on the Internet. Facilities like *script kiddies* enable less-accomplished programmers to generate computer viruses. *3D printers*, originally tools for prototyping designs, have been used to boost criminals' own capability. For example, they have been deployed to manufacture accurately-fitting and realistic-looking scanning mouthpieces for ATMs – where you insert the card – to illicitly read and transmit customers' card details. And as soon as the bank security team modify the ATM front panel, all it takes is a ball of wax, a laser scanner and computer-aided design and manufacture (CAD-CAM) software linked to the 3D printer to rapidly create and produce an updated mouthpiece (Krebs, 2011). There is now also on the market an Internet-of-Things kit and support service for connecting up and remotely activating whatever one wants (www.bbc.co.uk/news/technology-31584546), which will surely be of interest to terrorists and other criminals.

Design against, and for, crime thus cannot be considered as a simple case of determinism. Rather, design is a component of the dynamics of a *complex adaptive system* in which particular groups of agents anticipate, and adjust to, the goals and actions of other such groups, against a changing social and technological background. In this context, a longer-term, strategic view indicates that crime levels depend on which side is innovating, and disseminating their innovations, faster than the other.

How can crime preventers keep up? They can develop the capacity to anticipate; they can learn from other 'co-evolutionary struggles' including military arms races, predator versus prey, antibiotic versus bacteria and pest versus pest control; and they can create the right economic and policy climate of expectations and incentives to influence designers, manufacturers, regulators, consumers and users. Above all, they can shift perspective from winning individual battles, to strategically developing and disseminating *innovative capacity* among designers. Ekblom (1997, 1999, 2016) sets out a wide suite of strategies for 'gearing up against crime', covering:

- Accelerating the learning curve for designers by setting up 'learning paths', involving systematic assembly of crime Modus Operandi information of the right kind (e.g. how the lock was broken/ how the security code was obtained or circumvented), so the vulnerability can be detected and fixed
- Designing not to fixed construction standards, like incorporating particular types of lock or using particular resistant materials, but to performance standards (e.g. 'the lock must withstand 20 kg of force and resist expert picking for 20 minutes by currently-available tools, or ideally by the kinds of tools likely to become available during the lock's working lifetime'). This slows obsolescence, and frees designers to devise diverse solutions rather

than constraining them to a single measure whose vulnerabilities can quickly be transmitted among offenders. It also prevents manufacturers from absolving themselves from responsibility by 'designing down' to minimum construction specifications. Offenders who face uncertainty about what preventive systems they may encounter in the next home or ATM, are at a logistical and psychological disadvantage.

- Knowing the offenders and their current and future capabilities. It is important to differentiate between design problems imposed by calculating, skilled and adaptable criminals and those where only the impulsive and poorly-resourced must be countered. Conduct systematic studies of offenders' resources (Ekblom and Tilley, 2000; Gill, 2005): knowledge, information sources and networks, skills and adaptability and methods of offending. Such studies could come from offender interviews (see Lasky et al 2015 for innovative ways of eliciting the information from shoplifters using eye-tracking in real situations followed by interview and instant replay of the 'view-from-the-offender); and/or from analysis of information on perpetrator tools and techniques from crime reports and scene-of-crime investigations.
- Learning by analogy from other fields facing similar problems (control of disease or pests, military or espionage approaches; natural predator-prey, parasite-host, or even herbivore-plant relations (Ekblom 1999; Felson, 2006; Sagarin and Taylor, 2008).
- Learning the methods of foresight/horizon scanning (e.g. see DTI, 2000). Do not act on very specific predictions but ensure security plans are versatile across a wide envelope of possible futures.
- Designing-in the easy upgrading of security, where anticipation fails.
- Helping crime prevention practitioners, as users of designs and customers of designers, to become adaptive themselves. This means teaching them to use fundamental principles rather than superficially rely on fixed 'cookbook' recipes from occasional success stories (Ekblom and Pease 2014); and ready to draw on design more widely than merely by using its products, an issue discussed next.

Responding to the challenges of product design

Responding to all these challenges requires good design; it must also incorporate concepts, theory, and research from crime science. These are covered in turn.

Design processes

Often, when police and other professional crime preventers make use of design, they tend to focus on its *products*, namely the objects, places, procedures etc. that designers have generated, such as secure buildings or vehicles. Undoubtedly these are useful, but their benefit is confined to particular problems and contexts. A far wider benefit comes from understanding and working with design as a *process*. The 'design way of thinking' has much to offer security practitioners.

A good description of the process of design is the UK Design Council's 'Double Diamond' model (see www.designcouncil.org.uk/news-opinion/design-process-what-double-diamond). It comprises four stages, alternating between divergence and convergence of thinking. *Discover, Define*, *Develop* and *Deliver.* Increasingly, users and stakeholders are involved in the process, not just in stating their requirements for the product, but in *co-design*. The rationale for this is twofold: users and other parties usually have much local, or problem-specific knowledge to contribute to the design (for example on the nature of the problem and the acceptability of the solution); and the greater their involvement in the design process, the greater their commitment to purchasing, installing and using the product.

Handling conflicts and tradeoffs

The design process is rich and complex – even the simplest idea for a security product, say, may need to address a diversity of conflicting demands and trade-offs, as described under *challenges*, above. As an example, the Design Against Crime Research Centre's Grippa clip is fixed underneath tables in bars, to help customers protect their bags against theft. The fundamental idea is obvious and simple, but the realisation was demanding. The clip had to satisfy several kinds of stakeholder (male and female customers, bar staff, bar management). Their requirements ranged widely, covering economic cost, easy installation; matching the décor of the bar; easy stacking of tables; no injury to customers or damage to their clothing; easy cleaning; self-evident purpose of the clip (so customers would know what it was for/how to use it); not alarming customers that this was an exceptionally high-crime bar; differentiating between bag owners and thieves (easy for the former to operate, hard for the latter, i.e. 'user-friendly, abuser-unfriendly'); and of course strong and large enough to support quite large and heavy bags containing laptops etc. All this necessitated a high-performance design. The Grippa Clip is shown in detail at www.grippaclip.com and the design is further described below. Further discussion of the handling of tradeoffs and design contradictions through systematic use of inventive principles is in Ekblom (2012a)

Reframing

Sometimes neither trade-offs nor creative solutions are sufficient in themselves to address what stakeholders require. The latter often approach designers with fixed ideas about their problem, and what the appropriate kind of response should be. Experience shows that further research and thinking may suggest a different track. A key concept here is *reframing* (Dorst, 2015). To illustrate, the city rail authority asked the Designing Out Crime Research Centre at the University of Technology, Sydney (www.designingoutcrime.com), to design an anti-terror litter bin. The initial concern was with reducing blast injury. However, discussion with the clients revealed that, while actual explosions obviously brought severe harm they were also extremely rare; a more routine, tangible problem was the disruption and financial losses from the many false alarms. Lulham et al. (2012) describe both the problem renegotiation process and the product, a bin reducing the risk of both explosions *and* disruption. This was achieved by making insertion of large objects difficult, rendering the sides transparent and including a slot for the bomb squad to insert an X-ray plate, drastically speeding up the checking of suspicious contents.

Visualisation

The process of thinking and perhaps reframing the problem is greatly assisted by *visualisation* of problems and solutions. Gamman and Pascoe (2004) make the general case, and the Design Against Crime Research Centre has pioneered the use of graphic cartoons in both warning the public about criminal modus operandi, and briefing designers to help them understand what criminal techniques they are designing against. Examples are at www.designagainstcrime.com/methodology-resources/perpetrator-techniques/ and a video cartoon at www.bikeoff.org/design_resource/ABT_problem_who_steals.shtml. The 3D printer (already seen as a tool for offenders) can also aid visualisation and physical handling of prototypes. This was used to convert designs of the Grippa Clip on computer, into accurate plastic models which could be offered up, played with and assessed in tangible ways in stakeholder workshops.

Crime science – content

Architects do not produce good buildings if they fail to take account of the laws of physics, the properties of construction materials and the requirements of the occupants. Designers, too, need to combine creativity with discipline and a systematic, analytic approach (Dorst 2015). In particular, those who design products to be secure need to take account of what we know about the causes of criminal events and the kinds of interventions in those causes that reduce the risk of the events. Even if they are entirely new and innovative, their security function needs to be *plausible* – i.e. it must be theoretically sound and have a good chance of being produced and working in a practical context. Such plausibility comes from *crime science* (Pease, 2010). This seeks to understand and reduce the risk of criminal events by developing a clear picture of crime risks, focusing on their proximal (or immediate) causes, and intervening in the crime situation – the place where the event happens and the time shortly before, during or after the event. Part of that situation is the designed product. This section begins by discussing the nature of crime risk and risk factors; continues by covering causes and interventions; and ends by presenting a framework for systematically considering the design of security functions within products. The section that follows outlines a process model of doing crime prevention that emphasises design-type approaches to crime prevention whether via the development and installation of products or more generally, and was itself deliberately designed to be fit for purpose – the 5Is framework.

Risk and risk factors associated with products

Risk can be defined as *possibility* (the nature of the undesired events that can happen), probability and harm. Harm itself can happen both during the criminal event (damaged car, injured robbery victim) or afterwards (traumatised victim; crime proliferation from stolen identity documents or keys). Design seeks to eliminate the possibility of a class of criminal events (e.g. where external car radio aerials, the target of vandalism, are replaced by conducting layers on window glass); or if not, to reduce the probability; or failing that, to reduce the immediate or subsequent harm.

Cohen and Felson (1979) identified products at risk of being targets of crime through the acronym VIVA: from the perspective of the offender, something is worth stealing if it is high in Value, low in Inertia (weight), high in Visibility and high in Accessibility. Evidence came for example from the correlation between the decreasing weight of items in the Sears Catalog (such as TV sets) over time and the increase in their relative popularity as crime targets. Clarke (1999), drawing on a range of data including crime surveys, extended this analysis of risk factors to identify 'hot products' as CRAVED: Concealable, Removable, Available, Valuable, Enjoyable and Disposable (i.e. easy to sell). Gill and Clarke (2012) further characterised 'fast-moving consumer items' such as fancy expensive disposable razors, as 'AT CUT PRICES': Affordable, Transportable, Concealable, Untraceable, Tradeable, Profitable, Reputable, Imperishable, Consumable, Evaluable, Shiftable (i.e. can be sold on).

Specific risk factor sets such as these can be used to guide which products need extra security protection during distribution, retail and use. They can also be used in 'crime proofing', i.e. identifying in advance, early in the design process, whether a product is likely to be at elevated risk of theft, and thereby deciding what security functions should be designed in. Armitage (2012) describes an attempt to convert the principles of CRAVED into a systematic crime proofing process which could be used to guide how much security to design into a given class, make or model of product. For example, a product that was judged at high risk of theft (e.g. a smartphone) should be given a commensurately high level of security, whereas one at low risk should not bear this burden of cost and inconvenience.

A complementary 'protective factors' approach was developed by Whitehead et al. (2008) who summarised the crime-*resisting* properties to design into mobile phones. IN SAFE HANDS describes phones with these characteristics:

- **I**dentifiable – by owner, e.g. through marking
- **N**eutral – anti-theft design features should not adversely affect user's experience or elevate risk of other crimes
- **S**een – to be protected – deterrence
- **A**ttached – mechanical/electronic links to its owner
- **F**indable – lost/stolen product can be tracked and found
- **E**xecutable – can be deactivated if lost/stolen
- **H**idden – e.g. concealed about the person, and used covertly
- Automatic – security built-in/automated
- **N**ecessary – to be the owner, to be able to use product, e.g. via mechanical keys, codes, biometrics
- **D**etectable – make it obvious product is being/has been stolen, e.g. via alarm
- **S**ecure – protection itself should not be easily removable or hackable.

Note that these specifications for security properties are very generic: as such, they facilitate *design freedom* rather than forcing designers to incorporate very specific, fixed features, and so aid adaptability and the generation of a variety of solutions. But from another angle, both the risk and the protective factors discussed are quite specific: they concern quite narrow types of crime, centring on theft. A complementary approach seeks to widen the range of crime types considered during product design and deployment. Working through a long list of offence categories is impractical but a compromise between detail and simplicity is the *Misdeeds and Security Framework* (Ekblom, 2005). This endeavours to help designers (and anyone doing security) to envisage how some new product, place or service might feature in crime, mostly in terms of how the perpetrator treats it. Thus a product, for example, could be *Misappropriated* (stolen), *Mistreated* (harmed), *Mishandled* (smuggled, given false identity), *Misbegotten* (counterfeited), *Misused* (as tool, prop or weapon), *Misbehaved with* (e.g. making noise) or *Mistaken* (false alarm, wrongful accusation).

Causes and interventions

Risk and protective factors are correlational – an understanding of *causes* gives designers a more certain and direct route to incorporating the required security properties within their product. Crime science has adopted the Scientific Realist approach to causation (Pawson and Tilley 1997), namely a focus on understanding and influencing *causal mechanisms* of crime and of crime prevention. To take a simple example, a CCTV camera may have a preventive effect via the mechanism of *deterrence* – but in order for that mechanism to be triggered, the potential offender has to know that the cameras are present and active, and believe that someone is watching the monitor screens who is willing and able to detect and respond by, say, summoning the police. Preventive mechanisms can be realised by practical interventions as delicate as this example or as robust as a high brick wall. But in virtually all cases the mechanism is highly *context-dependent*. In particular, designers have to treat the product and its normal human users who may buy, install and/or operate it correctly or incorrectly, as a *system.*

Causal mechanisms within crime science have typically been depicted via theoretical situational approaches centring on *opportunity* (Felson and Clarke 1998). One such approach is the Routine Activities perspective on the causes of criminal events (Cohen and Felson 1979) where a likely offender encounters or seeks out a suitable target in the absence of capable guardians (suitability relating for example to the 'hot products' factors described above). Another is the Rational Choice perspective (Clarke, 2008) in which offenders decide whether or not to commit a particular crime on the basis of perceived risk, effort and reward. Yet another is Wortley's (2008) Crime Precipitators approach, in which exploitation of opportunity is preceded by an awakening or release of motivational/emotional processes through stimuli present in the crime situation – prompts, permissions, pressures and provocations (an example of the latter being an insulting poster which motivates people to deface it). In all cases, the preventive intervention involves *blocking, weakening, deflecting or removing the causal influence and hence reducing the opportunity or the precipitating factors*. Designing a particular product whilst taking account of its context of use and abuse may be one way of doing this.

In textbooks and guides, these traditional opportunity theories are normally presented one after the other. But for the designer, having to assimilate, integrate and apply them is inhibited by the fact that they partially overlap, use differing terminology, and refer to different analytic levels (Routine Activities is ecological, Rational Choice is psychological). Likewise, the knowledge of practical preventive methods that realise these theories is normally listed in a classification known as the 25 techniques of situational prevention (Clarke and Eck, 2003 and www.popcenter.org/25techniques/. This is organised around a loose blending of the Rational Choice decision agenda and aspects of crime precipitators; as such, it is more like a catalogue than an 'Ideas generator' which designers would prefer. One approach that tries to provide a single unifying and analytic, mechanism-oriented framework covering all the situational theories and connecting too with offender-oriented approaches to causation and intervention, is the *Conjunction of Criminal Opportunity* (CCO: Ekblom, 2011 and http://5isframework.wordpress.com/conjunction-of-criminal-opportunity/) and see a designers' modification at www.doca.org.uk/#/case-studies/4574672271 click DesignersGuide).

CCO, like Routine Activities, is an ecological model of the immediate causes of criminal events. It centres on human *agents* playing particular roles in a particular setting comprising several types of inanimate *entity*. In brief, CCO describes circumstances where a predisposed, willing and appropriately-equipped offender encounters, seeks or engineers a situation in which he/she chooses to steal or attack a target object or person, perhaps inside an enclosure, whilst coping with people who might prevent the crime and exploiting those who might facilitate it.

Among agents, *Offenders,* described below, are obvious. *Crime Preventers* make criminal events less likely, by their mere presence or actions including surveillance of strangers, supervising children or using window locks. Preventer roles can be undertaken by police/security staff, vigilant employees, parents controlling children or 'good citizens' reporting vulnerabilities. Crime *Promoters* increase the risk of criminal events, with varying degrees of intentionality. They include someone accidentally provoking the (potential) offender; a 'friend' encouraging vengeance for an insult; a fence buying stolen goods from a burglar; or someone leaving their laptop visible when parking their car. Prevention often seeks to convert careless promoters into careful preventers.

Entities are the 'things' in crime situations. The *Target* of crime may be an object that is inherently criminogenic: vulnerable, valuable or provocative; or a person (victim, in the passive sense, who may also act as preventer or promoter).

The target may be located in a *Target Enclosure* including safes, locked rooms or gated compounds. Enclosures are characterised by periphery, boundary fence, access doors/gates and interior. Each such feature may have criminogenic or criminocclusive properties.

Enclosures are situated in turn in a *Wider Environment*, e.g. a mall or housing estate. Environments (and enclosures) can be characterised in two ways. The *instrumental* environment relates to the goals of offender and preventer: how far the physical layout, lighting etc. tactically favours one or other agent (see 'script clashes' below). The *motivating* environment covers, say, how many attractive targets the environment contains. Using Wortley's (2008) situational 'precipitators', it may also supply settings or agents that prompt, pressure or provoke aggressive actions (like 'collision points' at crowded stations, or spectators cheering-on youths racing stolen cars). All of these entities – targets, enclosures, environments and resources for offending – can be designed to directly reduce the risk of crime.

Although designers can only directly influence the entities in crime situations, indirect influence on offenders, preventers and promoters is possible. And as suggested above, 'knowing the offender' is a vital part of attuning situational influences to maximally affect this party (Ekblom, 2007).

The offender side of crime causation starts with *predisposition to offend* – aggressive tendencies, antisocial attitudes etc.: permanent potential for criminal behaviour that is present, but not always expressed, in all situations the offender encounters.

Resources to avoid offending include self-control and skills to earn an honest living.

Readiness to offend comprises emotional/motivational states induced by current life circumstances (like unemployment) or recent experiences (stressful journey, needing drugs money, intoxication).

Resources for offending (Ekblom and Tilley, 2000; Gill, 2005) empower offenders to tackle the risks and exploit the possibilities for instrumental crime and to realise expressive crimes including revenge attacks. They range from facilitators like tools/weapons to perpetrator techniques, knowledge of opportunities, and insider confederates; also, ability to 'psych themselves up' for an attack. Tools and weapons may in fact be present in the crime situation (as for example with traditional beer glasses which can be misused in bar fights); or offenders can procure them in advance.

Perception/decision to offend captures the offender's immediate perception/anticipation of, and response to, the 'Rational Choice' agenda of risk, effort and reward (Clarke, 2008); and reaction to precipitators.

Obviously, *Presence of offender in situation* is also necessary (although this can be 'telepresence e.g. via online hacking, and indeed CCO can be re-cast in cyberspace terms (Collins and Mansell, 2004).

CCO adopts the twin perspectives of causation (as just described) and intervention to block, weaken or deflect those causes. On the former, it can be applied to understanding the vulnerabilities of designs (for example, as *targets* of misappropriation or mistreatment, as *resources* for misuse in offending, or *enclosures or wider environments* which provide criminal opportunity of any kind). Likewise it can describe with some precision how products can be designed to *counteract* these vulnerabilities in order to resist or protect against crime. The CCO and related frameworks in a design context are viewable at www.bikeoff.org/design_resource/DB_crime_frameworks.shtml and www.designagainstcrime.com/methodology-resources/crime-frameworks.

An alternative formulation of causal influences focusing more specifically on the offender, but consistent with CCO, is the 'D principles' (Ekblom and Hirschfield, 2014): Deter known and unknown, Discourage, Defeat, Detect, Deceive, Demotivate, Disconcert, Disarm/disable, Direct/deflect, Detain. Again, this can help focus the thinking, and the trialling and improvement processes, of designers.

By listing the factors in the immediate situation, what the offender brings to that situation, and how these can be influenced, CCO and the D principles provide fairly static pictures of causation. Designers need also to consider the dynamics – what processes bring these causal ingredients together, and how they then interact with one another. A key factor here is the offender him/herself, who may play an active role: designing props (such as counterfeit share certificates) and procedures to entrap the victim and carry out the crime. The concept of *crime scripts* (Cornish 1994; Ekblom and Gill 2015) is important here. Scripts are the procedural steps by which an offender carries out the crime, at each step creating or exploiting opportunity – for example to steal an expensive car and sell it abroad may involve steps of locating the car/s, identifying their vulnerabilities, obtaining the necessary tools, actually taking the car, obtaining false vehicle identity documents, driving the car across the border and selling it. Each step offers different ‘pinch points’ which designers may address to make life more risky, more effort and less rewarding for offenders.

But it is not just offenders whose actions can be characterised by scripts. Preventers, too, act through procedures extended in time and space – for example, finding a secure car park, locking the car before leaving it etc. And the procedures of offenders and preventers/users may interact. *Script clashes* (Ekblom, 2012a) characterise archetypical tactical conflicts between offenders and preventers, such as pursue vs escape, detect vs conceal, challenge vs explain one’s presence or action, wield force vs resist force. It is the designer’s job to shape the product and/or the physical and social environment or enclosure in which it is typically located, to differentiate in favour of the script of the good guy over that of the bad.

The Security Function Framework

How can the above crime science frameworks be woven into the process of design? Guides have been written which attempt to do so – for example the Design Council guide to designing out crime mentioned above includes an adaptation of the CCO. But an alternative approach is the *Security Function Framework* (Ekblom, 2012b). This was conceived as a way of helping designers to articulate the *rationale* of their design, a process which is important in sharpening the specification so it reflects crime science theory and research, giving structure to their thinking (without reducing their flexibility and creativity), sharing/accumulating knowledge of practice; and encouraging reflection. The last – reflective practice (Schön 1983) – is considered particularly important in the design field.

The Security Function Framework systematically describes products in terms of:

- *Purpose*. What is it for; especially, what crimes is it intended to prevent or mitigate, and what other, ‘civil’ purposes does it have? Whose purpose/s does it serve?
- *Security niche*. How does it fit with the ‘ecology of security’? Is it, for example, a *security* product (like an ultraviolet banknote scanner, with no other purpose than to prevent crime – in this case, forgery)? Is it a *securing* product, with a principal purpose other than security – like the ‘Stop Thief’ chair for cafes, equipped with notches for customers to securely hitch their bag behind their knees (see Figure 4 and www.designcouncil.org.uk/our-work/challenges/Security/Design-out-crime/Case-studies1/Stop-Thief-Chair-and-Grippa-Clips/? Or is it an inherently *secure* product? An example is the Puma folding bike (Figure 5 and see www.bikeoff.org/design_resource/DR_bikes_examples_puma.shtml, which contains various inbuilt anti-theft features including replacement of the diagonal member (the ‘down tube’), normally a rigid steel part, with a flexible cable that unlocks at one end, and can be wrapped round a lamp post, say, to secure the bike to it. The idea is that if a thief breaks the cable to release the bike, the bike itself becomes unusable or unsaleable.

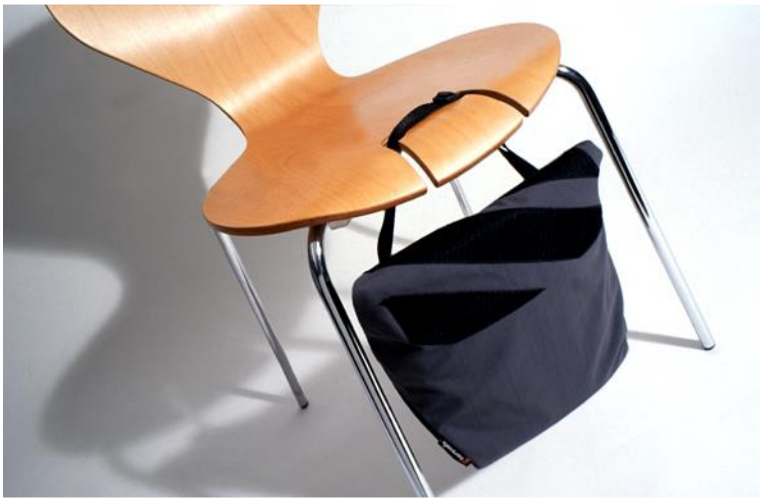

Figure 4 Stop Thief Chair [Photo: Design Against Crime Research Centre]

- *Mechanism*. How does it work in cause-effect/theoretical terms? Which of the CCO elements does the mechanism involve, or which of the D principles? It is usually possible to conjecture the operation of multiple mechanisms, given the complexity of the causation of criminal events.
- *Technicality.* How is constructed and manufactured, and how does the user operate it?

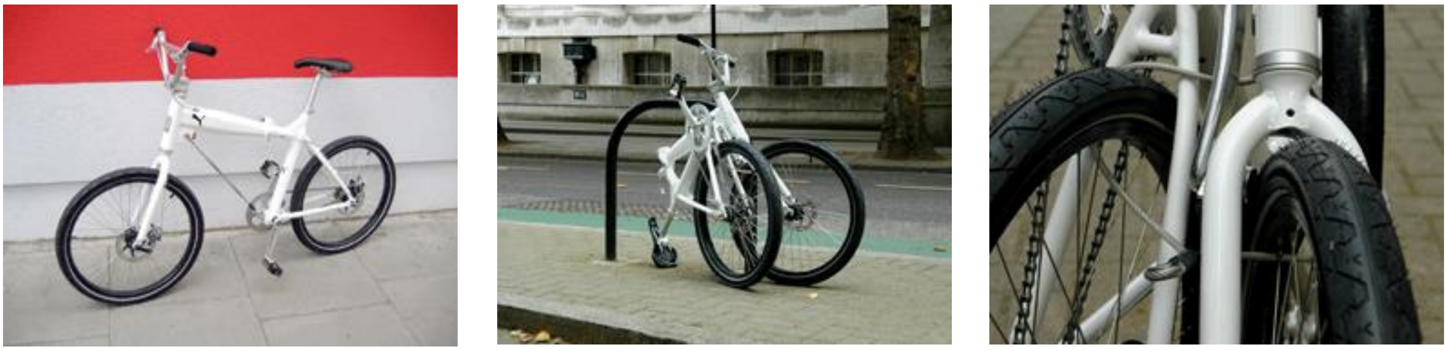

Figure 5 Puma bike [Photo: Design Against Crime Research Centre]

During the design process, the first one or two aspects (purpose and niche) can be pre-specified and the designer is left free to come up with mechanism and technicality. (In the case of more radical design, discovery, definition and reframing can allow the designer still wider scope.) Meyer and Ekblom (2011) use it to provide a prospective specification for an explosion-resistant railway carriage. For information sharing, the framework can be used to develop retrospective descriptions of products.

An in-depth example is available for the previously-described Grippa clip for securing customers' bags to bar tables (Figure 6; Ekblom et al., 2012).

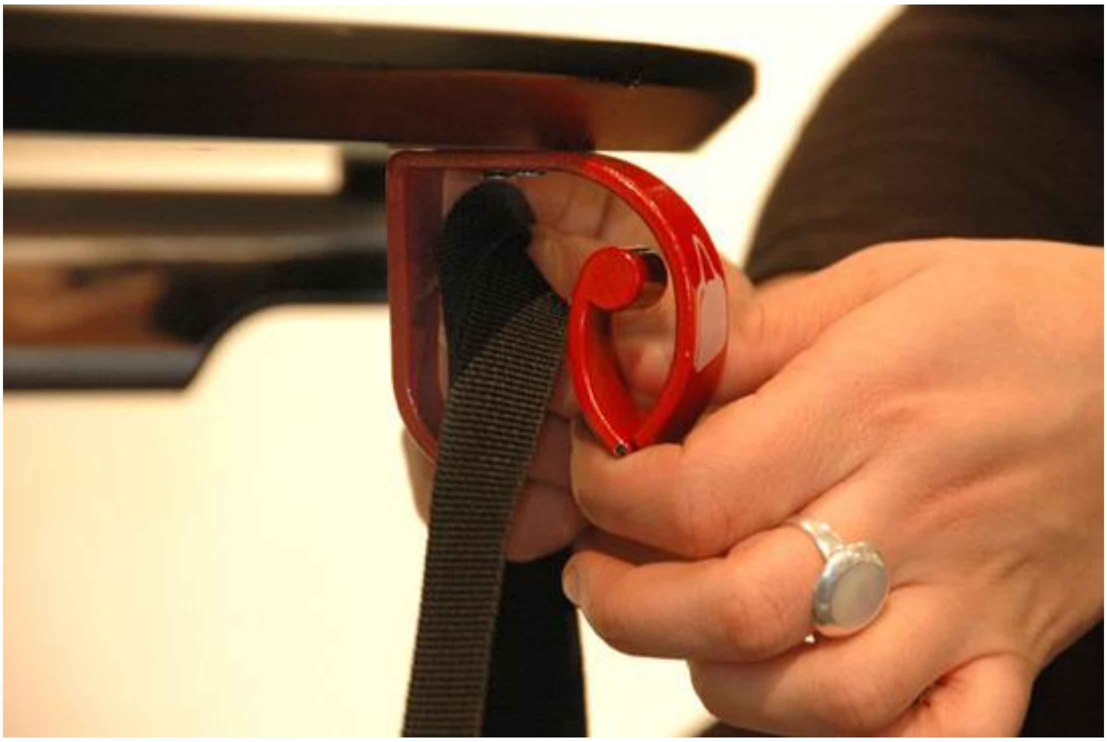

Figure 6 Grippa clip [Photo: Design Against Crime Research Centre]

Crime science – process

Crime science is not just about risk, cause and effect: at the heart of its applied, action-oriented approach to crime is an interest in the process of undertaking crime prevention. For this, it needs a process model. The most common process model is SARA (e.g. Clarke and Eck, 2003) – Scanning, Analysis, Response and Assessment. However, whilst SARA is an excellent, quick-to-learn introduction to the know-how of problem-oriented crime prevention, it is insufficiently detailed and structured to handle the messy complexity of preventive action on the ground. Moreover, it cannot capture the depth of practical detail of action, nor the full range of intervention principles needed to support the intelligent selection and replication of crime prevention success stories, and plausible innovation in their absence, as described above. These limitations are especially constraining for designers in particular. Before they can develop and test proposals, they require rich information and subtle understanding of the problem, and also the possibilities, enablers and constraints for solution – including the human ones relating to users and other stakeholders.

The 5Is framework

An alternative process model which builds on SARA but goes into far greater detail is the 5Is framework (Ekblom, 2011 and http://5isframework.wordpress.com). 5Is is an advanced framework for capturing, consolidating and sharing knowledge of good practice in crime prevention. It aims to improve performance, scope and delivery of that practice locally, nationally and internationally, enabling smarter responses with reduced resources. It is applicable to all of crime prevention, covering both situational and offender-oriented approaches, and service-like approaches as well as project-based ones. It has wider applicability e.g. for constituting the core schema underlying crime prevention education and training, guiding researchers on process evaluation, structuring and assessing bids for crime prevention action funding and managing and monitoring crime prevention projects. Beyond crime prevention it may be adaptable to practice areas such as public health or wider social innovation.

5Is (Figure 7) structures the process of crime prevention in terms of five interlinked task streams: *Intelligence, Intervention, Implementation, Involvement and Impact.* In effect, at the highest level it merges the Scanning and Analysis stages of SARA but divides Response into three main chunks. Intervention covers mechanisms, principles and practical methods to block or weaken the causes of criminal events, supply reassurance etc; Implementation centres on the practical *tasks* to be undertaken in order to make the Intervention methods happen; and Involvement is the *people* dimension whereby a wide range of stakeholders or 'dutyholders' beyond the crime prevention professionals are engaged to undertake or assist with the Implementation tasks – hence, Involving people in Implementing the Intervention.

Each of the 5Is task streams is further differentiated into detailed subsidiary tasks, organised using supplementary frameworks. For example, the Conjunction of Criminal Opportunity framework supplies (for Intelligence) an integrated map of the immediate causes (and theories) of criminal events, and (for Intervention) a counterpart map of preventive principles/ mechanisms. Four main levels structure and manage the richness of practical detail assembled: *Message* (the 5Is themselves, e.g. *Involvement*); *Map* (principal subheadings, e.g. Involvement: *Partnership, Mobilisation, Climate-setting*); *Methodology* (e.g. 'Mobilisation: *Clarify* crime prevention task to undertake; *Locate* appropriate agency or individuals to implement it; then *Alert, Inform, Motivate, Empower* and *Direct* them); and *Meat* (e.g.

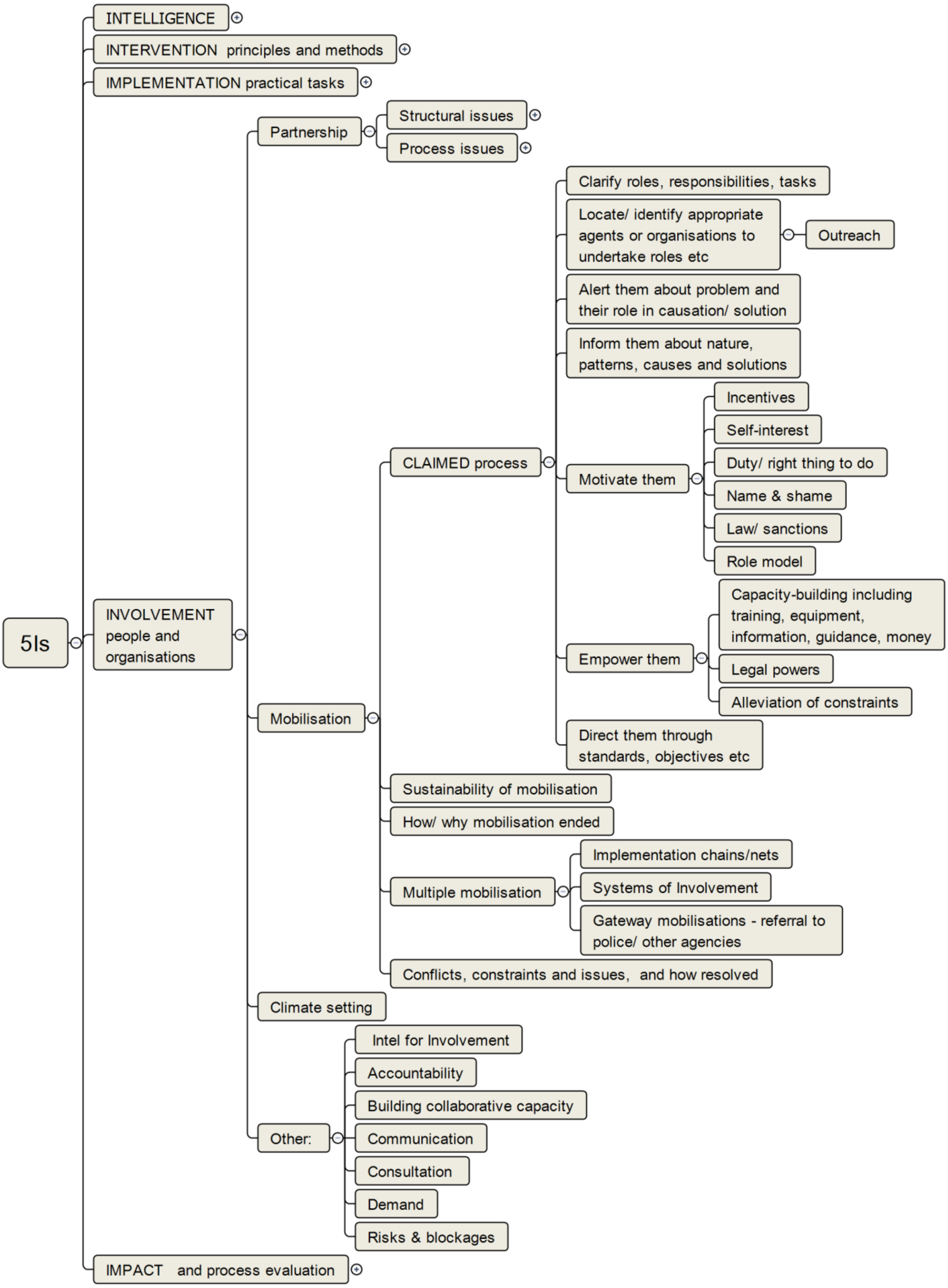
5Is
INTELLIGENCE
INTERVENTION principles and methods
IMPLEMENTATION practical tasks
INVOLVEMENT people and organisations
Partnership
Structural issues
Process issues
Mobilisation
CLAIMED process
Clarify roles, responsibilities, tasks
Locate/ identify appropriate agents or organisations to undertake roles 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
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
Climate setting
Other:
Intel for Involvement
Accountability
Building collaborative capacity
Communication
Consultation
Demand
Risks & blockages
IMPACT and process evaluation

Figure 7   5s framework showing detail of Involvement task

Motivate: *incentivise, name-and-shame, legislate* etc.). Graphic representations are at https://5isframework.wordpress.com/graphic-and-spreadsheet-versions-of-5is/).

The affinity between 5Is and, say, the 'Double Diamond' process model of design is self-evident. But design relates to 5Is at a number of levels. 5Is itself was deliberately designed to be fit-for-purpose as a knowledge management and action-guidance system, through the development of an explicit specification. It uses a standardised and carefully-designed set of terms and interlocking definitions of key concepts such as crime prevention, security and community safety. The framework is also designed to be flexible and adaptive, able to describe the complex 'stories' of crime prevention activity in a way that helps practitioners formulate and clarify their own problems, select appropriate action to emulate, and either replicate this action intelligently customised to context, or innovate based on first principles. The vision is of practitioners who are more like designers and less like technicians with limited diagnostic and response repertoires. In fact, getting conventional crime prevention practitioners in the police, local government and elsewhere to 'draw on design' has become of equal importance to the original Design Against Crime mission of getting designers to 'think perpetrator'.

Involvement

There is not space to consider the design aspects of all the tasks and sub-tasks of 5Is here, but *Involvement* is of especial importance in understanding and facilitating successful crime prevention in general, and successful designs of criminocclusive products in particular. As said, it is often the 'people' aspects of some intervention – even one that centres on a physical product such as a lock – whose neglect leads to failure. A salutory example is that of the anti-theft Grippa clip already described.

Despite the care and effort lavished on the design of Grippa clips, and despite surveys indicating that customers liked the principle and the realisation, in the two London pubs where they were tested, observations revealed that few people were using them. A comparison trial in two venues in Barcelona however did show significant usage levels, as did a subsequent smaller-scale trial in a coffee shop at one of London's main rail termini. What was happening? A more detailed account is in Ekblom et al. (2012), but essentially in the London pubs there were several kinds of *involvement failure* (Ekblom, 2011), i.e. failure of people and organisations to adopt crime preventer roles. The *partnership* with the pub company, which had enabled the trials to be set up, weakened over time as staff moved on and the economic recession hit. *Mobilisation* of the staff in those pubs was also limited by poor communication down the management chain, and by the rapid turnover of bar-staff. Mobilisation of customers by the bar staff ('watch your bag, use the clips') was constrained by the latters' lack of motivation; a concern not to drive away custom by flagging the pub as a risky venue; and communications failures. (Cardboard hangers were initially put on the clips to advertise their presence and purpose, but these fell to the floor and were not replaced; subsequently the clips themselves were embellished with the embossed bag logos.) In Barcelona, a general *climate* of acceptance of high crime risk by all bars allowed staff to be freer in their security advice to customers. And both there and in the London coffee shop, staff were encouraged to care for customers besides *themselves* being accorded greater respect and permanence of employment.

A central aspect of Involvement, covering both partnerships and the more one-sided mobilisation of people and organisations to undertake crime prevention tasks and responsibilities, is the analysis of *roles*. Two broad perspectives are possible: crime-related roles and 'civil' roles, i.e. those in the everyday world of work, leisure and domesticity. The fundamental crime-related roles can be defined using the CCO framework: crime preventers, crime promoters and offenders. After the criminal event has happened we also have victims. Preventers can include the well-known 'guardians of targets, managers of places and handers of offenders' set out in the Problem Analysis Triangle (www.popcenter.org/about/?p=triangle) but the preventer is a far more flexible concept – after all, we want to include designers, who unfortunately can also be promoters if they design a vulnerable and attractive product.

In design against crime there is a particular interest in the civil roles. Taking graffiti as an example, the roles can be classified as *Dutyholders* (people who have a relevant paid responsibility, e.g. the manager of the municipal street cleaning department), *Stakeholders* (those with some other, perhaps less formal, interest in the cleanliness of the streets – such as the owners of businesses whose walls are covered in the graffiti) and *Actors* – people with non-specific roles and no strong or focused interest, such as passers-by or the manager of a hardware store. The product we are interested in is the spray can, a resource for offending that is misused by graffiti artists (although note that in some cases acceptable street art is an important positive activity). We can cross-classify the crime and civil roles. So for example we can find the municipal dutyholder acting as preventer; the store manager actor serving as promoter (selling spraycans to young people) or preventer (refusing to sell to young people); the business stakeholder acting as victim. Understanding the scripts, goals and resources of each of these role combinations and the script clashes between them gives a major insight into the design of products with a security function (Gamman et al., 2012). Only by analysing roles in this way can the wider context of Implementation and Involvement be understood, whether the product is a target or resource for crime, or an aid to prevention. Design of the product itself, and how it is marketed, sold and deployed, are similarly important when attempting to reduce a product-related crime or solve a crime through use of some prevention-related product.

In all these approaches, the designer's use of a set of *personas* likely to be associated in some way with the product – individual users, stakeholders and even including offenders (Hilton and Irons, 2006), each with a mini biography, character, interests, resources and agenda – can contribute to the envisioning of how particular design proposals might be received and responded to.[3]

Motivating designers and manufacturers

The crime generated by vulnerable and attractive products does not directly affect the designers and manufacturers of those products. In economics terms it is a negative *externality*, an unwanted by-product of their activity which adversely affects third parties including the owner (whose car is stolen), other victims (the bank which is robbed using the

[3] The development and use of the Personas method in the context of a Graffiti project is to be available at http://project.graffolution.eu, currently in progress.

stolen car) and society as a whole (including the cost of funding the police and criminal justice system). Allocating the right level and type of responsibility to designers and manufacturers for such externality is, however, tricky: responsibility ranges from incidental to reckless to deliberate; and from moral to civil liability (lawsuits by victims of crime due to negligently-designed products) to criminal responsibility (for example, the prosecution of manufacturers of equipment intended to bypass the security codes on mobile phones).

As Figure 7 shows, a key task in the Involvement process of crime prevention is the mobilisation of preventers to implement an intervention; and a key step in the CLAIMED process of mobilisation is to motivate them. Such motivation can come from incentives (e.g. tax relief on secure products, or image of corporate social responsibility); regulations and laws (see chapter by Eck in this volume), and naming and shaming. Naming and shaming has been used for example to get unwilling mobile phone service providers to tighten security.[4] So has consumer pressure (Learmount, 2005). The UK government has published a 'car theft index' (Laycock, 2004) which enabled purchasers to identify vehicle makes and models at particular risk. Combined with immobilizer legislation already described, and with pressure from insurance companies (who collectively attack-test new models and assign them a security rating which influences their insurance premium cost), this has succeeded in raising the priority that manufacturers accord to security, and now they even proclaim their security credentials in advertisements for new models. A similar index has been developed for mobile phone theft www.gov.uk/government/publications/reducing-mobile-phone-theft-and-improving-security.

Since business motivation is principally driven by self-interest (Clarke and Newman, 2005), encouraging manufacturers and their designers to make products more secure is not straightforward. Government has been reluctant, save in extreme circumstances (as with vehicle immobilizers and mobile phones), to make legal requirements to encourage crime prevention on a polluter pays basis (see Roman and Farrell, 2002). But it has shown interest in developing wider 'policy levers' with which to influence business (Home Office, 2006), including positive incentives, negative naming and shaming and awakening consumer pressure. Newman (2012) has suggested an equivalent to carbon trading allowances, allocated to manufacturers to limit the amount of crime their products can acceptably generate.

Impact – evaluation of products designed against crime

Inherent to the iterative process of directed improvement that is product design (Thorpe et al., 2009) are assessment and feedback from workshop tests and field trials. Once the product is deployed in the field, feedback is available (if the designers and manufacturers are motivated to collect and use it) from the experience of users and perhaps from service engineers. Ultimately feedback on crime problems and crime resistance may come from sales, profitability and market leadership, although here the strongest relationship is likely to be with dedicated security products. In terms of the kind of impact and cost-effectiveness evaluation increasingly applied to crime prevention, however, there is unfortunately little

[4] Former Metropolitan Police Commissioner Sir John Stevens and Broadcaster Nick Ross (2000) memorably described mobile phone providers as 'pimping for crime'.

hard evidence that relates to product design as opposed to 'target-hardening' and other situational approaches in general. Such evidence as exists is often characterized by weak research designs. Formally evaluated products were summarized in Clarke and Newman (2005, Table 4) and few such studies have emerged since.

One reason for this evidence gap is that prototypes are expensive to produce and test in sufficient quantities to support an impact evaluation of sufficient statistical power (Bowers et al., 2009). Another is the timescale for developing a product then evaluating it within a typical research funder's timeframe. Yet another is the private nature of research and development in industrial settings.

Circumstantial, correlational evidence points to the contribution of vehicle security technology towards the substantial and sustained reduction of theft of cars in the UK in recent years, following implementation of a European Directive on compulsory factory-fitting of immobilisers from 1998 and more general tightening of security design (Brown, 2013). Likewise, the arrival in 2013 of the new iOS7 operating system on Apple phones, with its remote security lock-out function, seems to have markedly reduced thefts compared with other makes (Behavioural Insights Team, 2014). There is more general evidence, too, attributing the recent 'crime drop' in many western nations to the 'security hypothesis' i.e. increased situational prevention including product-based measures (Farrell, 2013).

Other evidence is more anecdotal but almost entirely self-evident (Clarke and Newman, 2005). An example is the fabric curtain between certain London Underground train carriages, retrospectively fitted to stop boys riding the couplings. A glance reveals nowhere left for the boys to stand. But self-evidence cannot be taken for granted; and gives no information on comparative cost-effectiveness.

A study (Sidebottom et al., 2009) of attempts to reduce bike theft by installing advisory stickers on the bike stands has yielded reliable *intermediate* outcome evidence, important where the design of some secure, securing or security product requires mechanisms of behavioral change of those who act as crime preventers or promoters. The stickers were designed after systematic observation of bike-locking behavior and analysis of perpetrator techniques. The simple advice – lock both wheels and frame to the stand – yielded significant and substantial reduction (from 62% to 48% of observations) in the proportion of bikes locked insecurely (available funding did not, however, cover evaluation of impact on theft.). Further intermediate outcome indicators revealed the success of M-shaped bicycle stands (Thorpe et al., 2012 and see www.bikeoff.org) in encouraging cyclists to lock their bikes in the secure manner just described. Likewise, the pavement art patches in front of ATMs has also encouraged people to yield more space between the person taking their turn at the console, and the next in the queue (Thorpe 2013).

Conclusions

Designing products against crime now appears to have established a position in crime prevention policy and practice in many Western nations. But further research effort is needed to continue to build detailed practical knowledge – especially on the 'people' side of purchasing, installing and operating the designs. And a continual stream of good-quality evaluations of impact and cost-effectiveness are needed to maintain the pressure on policymakers and business to actively support this approach.

References

Note: all websites listed in text accessed 27 November 2015

Armitage R (2012) Making a brave transition from research to reality. In: Ekblom P (ed) *Design Against Crime: Crime Proofing Everyday Objects.* Crime Prevention Studies 27. Boulder, CO: Lynne Rienner, pp.65—86.

Behavioural Insights Team (2014) *Reducing Mobile Phone Theft and Improving Security*. London: Home Office.

Booch G (1993) *Object-Oriented Analysis and Design with Applications*, 2nd Edition. Boston, Ma.: Addison-Wesley Professional.

Bowers K, Sidebottom A and Ekblom P (2009) CRITIC: A Prospective Planning Tool for Crime Prevention Evaluation Designs. *Crime Prevention and Community Safety* (2009) 11, 48—70.

Brown, R (2013) Reviewing the effectiveness of electronic vehicle immobilisation: Evidence from four countries. *Security Journal* doi: 10.1057/sj.2012.55.

Clarke R (1999) *Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods.* Police Research Series Paper 112. London: Home Office.

Clarke R (2008) Situational crime prevention. In: Wortley R and Mazerolle L (eds) *Environmental criminology and crime analysis*. Cullompton: Willan.

Clarke R and Eck J (2003) *Become a Problem Solving Crime Analyst in 55 Small Steps*. London: Jill Dando Institute, University College London.

Clarke R and Newman G (2005) Modifying criminogenic products – what role for government? In: Clarke R and Newman G (eds) *Designing out Crime from Products and Systems*. Crime Prevention Studies 18. Cullompton: Willan.

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

Collins B and Mansell R (2004) *Cyber Trust and Crime Prevention: A Synthesis of the State-of-the-Art Science Reviews* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/299219/04-1147-cyber-trust-reviews.pdf.

Cornish D (1994) The procedural analysis of offending and its relevance for situational prevention. In: Clarke R (ed) *Crime Prevention Studies* 3: 151—196. Monsey, NY: Criminal Justice Press.

Di Tella R, Edwards S and Schargrodsky E (eds) (2010) *The Economics of Crime: Lessons for and from Latin America.* Chicago: University of Chicago Press.

Dorst K (2015) *Frame Innovation: Create New Thinking by Design.* Cambridge, MA: MIT Press.

DTI (2000) *Turning the Corner*. *Report of Foresight Programme's Crime Prevention Panel.* London: Department of Trade and Industry.

Ekblom P (1997) Gearing up against crime: A dynamic framework to help designers keep up with the adaptive criminal in a changing world. *International Journal of Risk, Security and Crime Prevention*, 2: 249—265. www.veilig-ontwerp-beheer.nl/publicaties/gearing-up-against-crime/view.

Ekblom P (1999) Can we make crime prevention adaptive by learning from other evolutionary struggles? *Studies on Crime and Crime Prevention* 8: 27—51. www.veilig-ontwerp-beheer.nl/publicaties/can-we-make-crime-prevention-adaptive-by-learning-from-other-evolutionary-struggles.

Ekblom P (2005) How to police the future: Scanning for scientific and technological innovations which generate potential threats and opportunities in crime, policing and crime reduction. In: Smith M and Tilley N (eds) *Crime Science: New Approaches to Preventing and Detecting Crime*. Cullompton: Willan.

Ekblom P (2007) Making Offenders *Richer*. In: Farrell G, Bowers K, Johnson S and Townsley M (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.

Ekblom P (2012a) Happy returns: Ideas brought back from situational crime prevention's exploration of design against crime. In: Farrell G and Tilley N (eds) *The Reasoning Criminologist: Essays in Honour of Ronald V. Clarke.* Crime Science series. Cullompton: Willan.

Ekblom P (2012b) The Security Function Framework: Towards a systematic language and approach for designing against crime. In: Ekblom P (ed) *Design Against Crime: Crime Proofing Everyday Objects.* Crime Prevention Studies 27. Boulder, CO: Lynne Rienner.

Ekblom P (2016) Terrorism – lessons from natural and human co-evolutionary arms races. In: Taylor, M Roach and Pease K (eds.) *Evolutionary Psychology and Terrorism.* London: Routledge.

Ekblom, P and Gill M (2015) Rewriting the Script: Cross-Disciplinary Exploration and Conceptual Consolidation of the Procedural Analysis of Crime. *European Journal of Criminal Policy and Research* (online first). DOI 10.1007/s10610-015-9291-9

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 Pease K (2014) Innovation and Crime Prevention. In: Bruinsma, G and Weisburd, D. (eds.), *Encyclopedia of Criminology and Criminal Justice*. New York: Springer Science+Business Media.

Ekblom P and Tilley N (2000) Going equipped: Criminology, situational crime prevention and the resourceful offender. *British Journal of Criminology* 40: 376—398.

Ekblom P Bowers K Gamman L Sidebottom A Thomas C Thorpe A and Willcocks M (2012) Reducing handbag theft in bars. In: Ekblom P (ed) *Design Against Crime: Crime Proofing Everyday Objects.* Crime Prevention Studies 27. Boulder, CO.: Lynne Rienner.

Farrell G (2013) Five tests for a theory of the crime drop. *Crime Science* 2: 5.

Felson, M (2006) *Crime and Nature*. Sage: Thousand Oaks, California.

Felson M and Clarke R (1998) *Opportunity Makes the Thief. Practical Theory for Crime Prevention*. Home Office Police Research Series 98. Available from http://webarchive.nationalarchives.gov.uk/20110218135832/rds.homeoffice.gov.uk/rds/prgpdfs/fprs98.pdf.

Gamman L and Pascoe T (eds) (2004) *Seeing is Believing*, special issue of *Crime Prevention and Community Safety Journal* 6/4.

Gamman L, Thorpe A, Malpass M and Liparova E (2012) Hey babe – take a walk on the wild side!: Why role-playing and visualization of user and abuser "scripts" offer useful tools to effectively "think thief" and build empathy to design against crime. *Design and Culture* 4/2 171—193.

Gill M (2005) Reducing the capacity to offend: Restricting resources for offending. In: Tilley N (ed) *Handbook of Crime Prevention and Community Safety'.* Cullompton: Willan.

Gill M and Clarke R (2012) Slowing thefts of fast-moving goods. In: Ekblom P (ed) *Design Against Crime: Crime Proofing Everyday Products*. Crime Prevention Studies 27. Boulder, CO: Lynne Rienner.

Hilton K and Irons A (2006) A "criminal personas" approach to countering criminal creativity. *Crime Prevention and Community Safety*, 8: 248—259.

HM Treasury (2005) *The Cox Review of Creativity in Business.* London: HM Treasury.

Home Office (2006) *Changing Behaviour to Prevent Crime: an Incentives-Based Approach*. Online report 05/06. London: Home Office. http://webarchive.nationalarchives.gov.uk/20110218135832/http://rds.homeoffice.gov.uk/rds/pdfs06/rdsolr0506.pdf

Krebs B (2011) http://krebsonsecurity.com/2011/09/gang-used-3d-printers-for-atm-skimmers/.

Lasky N, Fisher B and Jacques S (2015) "Thinking thief" in the crime prevention arms race: Lessons learned from shoplifters. *Security Journal* advance online publication doi: 10.1057/sj.2015.21

Laycock G (2004) The UK Car Theft Index: An example of government leverage. In: Maxfield M and Clarke R (eds) *Understanding and Preventing Car Theft*, Crime Prevention Studies 17. Monsey, NY: Criminal Justice Press.

Learmount S (2005) Design against crime. In: Clarke R and Newman G (eds) Designing out Crime from Products and Systems. Crime Prevention Studies 18. Cullompton: Willan Publishing.

Lulham R Camacho Duarte O Dorst K and Kaldor L (2012) Designing a counterterrorism trash bin. In: Ekblom P (ed. *Design Against Crime: Crime Proofing Everyday Objects.* Boulder, CO: Lynne Rienner.

Meyer S and Ekblom P (2011) Specifying the explosion-resistant railway carriage – a desktop test of the Security Function Framework. *Journal of Transportation Security* 5: 69—85.

Newman G (2012) A market approach to crime prevention. In: Ekblom P (ed) *Design Against Crime: Crime Proofing Everyday Objects*. Crime Prevention Studies 27. Boulder, CO, Lynne Rienner.

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

Pease K (2001) *Cracking Crime through Design*. London: Design Council.

Pease K (2010) Crime Science. In: Shoham S, Knepper P and Kett M (eds.) *International Handbook of Criminology* 3—23. Boca Raton, FLA: CRC Press.

Roman J and Farrell G (2002). Cost-benefit analysis for crime prevention: opportunity costs, routine savings and crime externalities. *Crime Prevention Studies,* 14. Cullompton: Willan.

Sagarin R and Taylor T (eds.) (2008) *Natural Security. A Darwinian Approach to a Dangerous World.* Berkeley: University of California Press.

Schön D (1983) *The Reflective Practitioner: How Professionals Think in Action*. London: Temple Smith.

Shover N (1996) *Great Pretenders: Pursuits and Careers of Persistent Thieves*. London: Westview Press/Harper Collins.

Sidebottom A, Johnson S and Thorpe A (2009) Using targeted publicity to reduce opportunities for bicycle theft: A demonstration and replication. *European Journal of Criminology* 6: 267—286.

Stevens Sir J and Ross, N (2000) Police Foundation Lecture 2000. London: Police Foundation.

Thorpe A (2013) *ATM Art Evaluation Programme*. London: Socially Responsive Design and Innovation Press. ISBN 978-0-9570719-3-3.

Thorpe A Gamman L Ekblom P Johnson S and Sidebottom A (2009) Bike Off 2 – catalysing anti-theft bike, bike parking and information design for the 21st century: An open innovation research approach. In: Inns T (ed) *Designing for the 21st Century, Volume 2: Interdisciplinary Methods and Findings*. Farnham, Gower.

Thorpe A Johnson S and Sidebottom A (2012) Designing against bicycle theft. In: Ekblom P (ed) *Design Against Crime: Crime Proofing Everyday Products*. Crime Prevention Studies 27. Boulder, CO: Lynne Rienner.

Tilley N (1993) *After Kirkholt: Theory, Methods and Results of Replication Evaluations. Crime Prevention Unit Paper 47*. London: Home Office.

Whitehead S Mailley J Storer I McCardle J Torrens G and Farrell G (2008) IN SAFE HANDS: A review of mobile phone anti-theft designs. *European Journal on Criminal Policy and Research*, 14: 39—60.

Wortley R (2008) Situational precipitators of crime. In: Wortley R and Mazerolle L (eds) *Environmental Criminology and Crime Analysis*. Willan: Cullompton.