Gearing Up Against Crime: a Dynamic Framework to Help Designers Keep up with the Adaptive Criminal in a Changing World

Paul Ekblom[1] Home Office Research and Statistics Directorate

International Journal of Risk, Security and Crime Prevention[1]

October 1997, Vol 2/4:249-265

This paper is a first, exploratory, attempt at providing some background, and a framework, to help designers more systematically incorporate crime prevention in their remit. The scope includes design of technological items, environments, systems and services. With all these products this is design against misappropriation, damage and misuse in the furtherance of crime; and design of products explicitly intended for the furtherance of prevention. The intention is to stimulate designers, commissioners of design and those like criminologists who conduct research that informs design in two ways: 1) shifting perspective from user to misuser to aid the day-to-day process of incorporating the preventive function in specific design tasks; and 2) in the more strategic process of helping crime prevention evolve as fast as crime in a world of adaptable criminals and changing opportunities, many of which stem from the permeation of society by IT. This involves setting up the infrastructure to speed up the feeding of information on crime and prevention to designers, and to promote the durability of preventive techniques. For the one certain thing in prevention is the obsolescence, sooner or later, of any individual measure.

Introduction

Designers - of built environments, homes, products, systems and services - need systematic training or guidance to help them incorporate crime prevention within their remit. But much of the available material is limited in scope and frequently offers no more than a string of loosely-connected ideas uninformed by theory. Good guides do exist (for example, Poyner's work on building design[2]) which strive to be evidence-based and to think in terms of design principles or issues. Criminology, for its part, is now well on the way to supplying a set of crime prevention principles which are up to the task, but the job is by no means complete. Much remains to be properly evaluated, and the working knowledge of prevention that exists is couched in a tangle of inconsistent and loosely-

[1] Now incorporated in *Security Journal.*

defined terms and concepts[3] which render it difficult for designers to access, to think about and to apply. Under these conditions it is unsurprising that 'pop' crime prevention ideas and movements fill the gap created by the absence of good ideas and a clear framework for generating and communicating them.[4]

Consequently, city centres are laid out, buildings are constructed, objects such as mobile phones are developed, and systems such as financial transaction networks and accountancy systems are set up either with little regard to their vulnerability to crime, or - if the motivation to tackle crime is there - with somewhat amateur concepts of crime and criminals. In many cases, the failure of designers to anticipate the vulnerability of their product to crime, or the criminal use to which their product might be put, means that individual victims and society as a whole are left to cope with a 'legacy' of crime. With the built environment and with some items such as cars, the legacy can last years before the products are replaced. Remedial or retrofit solutions are never as efficient as ones designed and incorporated into the product from the start. Even when crime prevention is incorporated at the design stage, in many cases this takes the form of 'bolt-on' afterthoughts, severely constrained by other design decisions already made, that are likely to have only a superficial impact.[5]

In trying to encourage designers to incorporate crime prevention within their remit, there are four broad sets of issues:

- First, the designers have to be motivated to do so - the people that commission the designs have to want any consequent crime to be reduced. This crime may affect the commissioners themselves (eg if they subsequently suffer burglaries in the factory they had built), other users (eg members of the public using a car park that failed to provide adequate line-of-sight surveillance), or the public interest (eg the taxpayer bearing the cost of the police response to the resultant crimes)

- Second, from a technical point of view, designers have to have the right knowledge of crime and crime prevention in the right form for them to use.

- Third, designers have to undertake a major shift of perspective. Their normal stance is one of catering for users who own or operate their products 'as intended' - or, if not, at least any misuse is without malicious intent. But the offender sees the target of crime, and its environment, from a completely different angle. 'What are the weaknesses of the house locks? How can I overcome the security code of the mobile phone? How can I plan a getaway through these back alleys? How can I misuse this security pass to gain access?' Designers have to be helped to 'think thief' - to add to 'user friendly', '*ab*user *un*friendly'. In a limited number of cases, designers deliberately employ 'retired' offenders to help them out - a strategy not without limitations or risks. In other cases, particularly with computer security, and sharing common ground

with counterespionage, 'penetration testing' is carried out. But - with the exception of some IT security processes[6] this is somewhat intuitive and haphazard.

- Fourth, it is becoming increasingly apparent that design against crime cannot stand still. Simply put, offenders usually adapt to existing preventive measures; and new technology brings new scope for offending. For any given preventive measure, therefore, eventual obsolescence is not a possibility but a certainty. Programmes to change the motivation of offending individuals, or alter offending subcultures, will of course be pursued in parallel to design solutions and will deliver social benefits wider than crime prevention alone. But we have to make the pessimistic though realistic assumption that they will have only partial impact: sufficient offenders will remain, and will continue to upgrade their efforts, for approaches through design to remain necessary for the foreseeable future.

This paper attempts to address the third and fourth issues, with some reference to the second. The first issue - which involves among other things convincing designers and their commissioners that design against crime is a necessary part of the job, and applying legitimate 'leverage' where public and private interests fail to coincide - is of a wholly different order to the rest and will not be covered here.[7]

If they are to adopt this shift of perspective designers need a coherent conceptual framework for crime prevention. On the basis of experience in evaluating the wide-ranging preventive action implemented in England's Safer Cities Programme[8] and elsewhere I have been developing one such framework aimed at meeting this need by placing great emphasis on precision and consistency of definitions.[9] This paper opens by briefly introducing the framework, called the *Conjunction of Criminal Opportunity*. A definition of crime prevention leads to a focus on the immediate causes of the criminal event, leading in turn to a schematic tree diagram of preventive measures and the location of design at various points on this. Next, it discusses the special features introduced into crime and crime prevention by IT. An extra dimension of crime is then identified - an *evolutionary* perspective on the development of design for crime prevention versus counterdesign by adaptable offenders. Finally, the practical implications of thinking thief and of taking the evolutionary perspective are developed through proposals for the development of an infrastructure in support of good, up-to-date crime prevention design, and a broader capacity to keep up with evolving methods of crime and new criminal opportunities. I call this approach *'gearing up against crime'*. The ideas themselves are very much 'first thoughts' on a wide range of issues, designed to stimulate and provoke discussion.

A definition of crime prevention: focus on causes

Crime prevention seeks to reduce the risks of criminal events and related misbehaviour by intervening in their causes. This definition is simple, positive and non-restricting (it could apply equally to design approaches and to surveillance by CCTV, setting up a youth club, police patrolling or incapacitating offenders).

There is an infinity of possible causes of criminal events. Some causes are remote - such as abuse in childhood producing violent assaults in adolescence, or structural and technological change introducing completely new opportunities for crime. Others are closer to hand - the presence of a motivated offender in a suitable situation for committing a crime. It is these *immediate circumstances* surrounding the criminal event - the offender in the situation - which form the final point on which all the diverse structural, social, ecological and psychological causes of the criminal event must inevitably converge. Before discussing prevention through design or any other approach, we have to develop a clear picture of the criminal event and its causes.

The immediate circumstances surrounding the criminal event: the Conjunction of Criminal Opportunity

A criminal event happens when the right *conjunction of criminal opportunity*[10] takes place. This comprises:

- a motivated *offender*, accompanied perhaps by *facilitators* of crime such as tools, weapons or false security passes and other *resources* such as agility, knowledge or skills

- a vulnerable and attractive *target* of crime (person, object, service, system or information) in a vulnerable and attractive *target enclosure* (compound, building, room, safe)

- the absence of willing and able *crime preventers* - active roles in which people make crime less likely to happen - by shaping the situation before the criminal event (eg hiding valuables, providing access control), *intervening* during the event (eg sounding an alarm), or *reacting* after (eg pursuit, arrest, identification) - deterring the offender in anticipation and also affecting subsequent criminal events. Preventers can be formal (police, security staff, other jobs with a security element, crime prevention implementers such as community safety officers) or informal (eg residents protecting their own homes or property)

- the presence of unwitting, careless or deliberate *crime promoters* - active roles in which people make crime more likely to happen - by *shaping the situation* (eg leaving attractive goods visible in an unlocked parked car), *intervening* during the criminal event (eg egging an assailant on), or *reacting* after (eg conveying approval, buying

stolen, pirated or contraband goods). Together, crime preventers and promoters can be called ‘crime modulators’

- an *environment* logistically favourable for the offender and crime promoters and unfavourable for crime preventers (eg one that promotes concealment or inhibits pursuit); and one that may attract the offence (eg a wealthy neighbourhood) or motivate it (thin walls engendering conflict between neighbours over noise)

Prevention ultimately works by disrupting this conjunction.

The process dimension

To this *structural* picture of the causes of criminal events must be added a *process* dimension. Foremost is *decision-making by the offender*,[11] balancing aspects of anticipated cost, risk, time and reward in relation to their own capacity and resources to commit the offence in choosing whether, when, where, how and against what target to offend. Such decisions could be close to criminal events (eg tactically veering off a robbery at the last second) or remote (eg strategically deciding to focus on a different type of crime or even to go straight). There will also be decision-making by the players of the other roles featuring in the conjunction of opportunity; social interactions between all the players; and the offender's negotiation perhaps of a series of 'scenes'[12] - achieving subsidiary goals to prepare for the crime (such as obtaining a forged security pass) and to complete it (such as disposing of stolen goods). *Tactics and strategies* of offenders (their modus operandi) may have some of the following generic features, which can guide designers - they may be surprising, cryptic (hard to detect that a crime is being committed), deceptive, bold, mobile/ transmittable to other offenders, evasive (moving operations around to avoid detection and countermeasures in any one location), resistant (impervious to countermeasures), or mutable (capable of being altered to circumvent countermeasures).[13] Mutability is taken up later.

The outcome of one crime situation (success or wasted effort for the offender in perpetrating the crime, and avoiding detection and punishment) will influence the probability and nature of future crime situations (eg through offenders learning or preventers exercising better prevention). Of course, structure and process stretch back in time and space beyond the immediate circumstances surrounding the criminal event. For example, lifestyle factors lead those people with particular potential to offend, to frequent particular environments such as entertainment districts. Offenders plan to exploit situations and actively seek them out or even (as with certain frauds for example) create the situation into which the victim walks. Certain (wider) environments channel potential offenders and targets together, as with railway termini - a suitable venue for pickpocketing.

A simple diagram of preventive methods

Figure 1 shows a classification of methods of prevention in terms of the above list of components of the conjunction of opportunity that they aim to alter or remove. There is a key divide between two complementary strategies: reducing crime by changing what potential offenders bring to the immediate crime situation (offender-oriented prevention), and by changing the situation itself (situational prevention). On the *offender-oriented* side, we can distinguish between three types of activity: i) what could be called *'criminality prevention'* or tackling the 'roots of criminality' - influencing people's potential to offend by intervening in their early lives in order to bring about changes in the trajectories of development and the 'programming in' by family and subculture of motivations, values, emotions and skills; ii) remedying the *current life circumstances* of individuals (such as debt, poor entertainment facilities, or membership of offending peer groups) which may be influencing their current state of motivation, emotion or decisions to offend; and iii) *restricting resources* that offenders can bring to bear on the crime target or use to deal with crime preventers and logistically difficult environments. On the *situational* side[14] preventive methods can reflect a focus on i) the *target* of crime (eg making banknotes harder to forge) or the *target enclosure* (eg strengthening doors); ii) on *crime preventers* (eg installing security guards or providing *prevention aids* such as CCTV or tamper-evident seals); iii) on *crime promoters* (eg incorporating buzzers to alert lax car owners to unlocked doors, setting up 'interlocks' to force till operators to follow payment security procedures, enhancing property identification systems to deter handlers of stolen goods, or even designing the promoter out altogether by for example making locking automatic); and iv) on the *environment* (eg on the logistical side clearing shrubs to reduce hiding places and blocking 'rat run' alleyways to hinder escape; or, on the motivational side, soundproofing walls between flats).

- [Figure 1 about here]

Interestingly, one striking aspect of prevention is the *multiplicity of causal mechanisms* by which any given preventive method can work.[15] Of fundamental relevance to designers is the distinction between mechanisms of *deterrence* (the preventive method works by influencing the offender's perceived risk of anticipated negative outcomes such as expenditure of effort and risk of arrest) and of enhancing *objective difficulty* (the method works by physically blocking the offence, necessitating more time to complete it or requiring more skill and equipment). Often, the two act in parallel - if offenders, for example, perceive that a new lock physically requires more time to pick then they may be deterred from trying it because to do so would involve more effort and prolonged exposure to risk.

Design against crime

The diagram illustrates how design against crime is achieved through situational approaches, reconciling improved *use* of the designed object, system or environment (fitness for purpose, cost, reliability, efficiency etc), with reduction in *misuse, misappropriation or damage*. Prevention is a secondary consideration in the design of most products, but it can also be the main feature, as with locks and safes. This task of

reconciliation is particularly challenging since making something suitable for legitimate use may simultaneously make it more vulnerable or attractive to the offender (for example a mobile phone or laptop aims to be small, easily carried, and with few barriers to ease of use or replacement of parts.) The design task can thus require great subtlety, resembling development of an anti-cancer drug that zaps the tumour without zapping the rest of the body.

However, designers at least have increasing experience in coping with unintentional or non-malicious misuse. Many complex modern artifacts, such as electric drills, video recorders or computer software, available to buy or hire off-the shelf and operate without training or supervision, are now designed with various inbuilt checks and interlocks which anticipate common user errors, due to failure to understand or even read instructions, which could jeopardise performance or safety.

Design against crime seeks to disrupt conjunctions of opportunity by making changes in the physical world and in the consequent perceptions of offenders. (As will shortly be discussed below, it also acts in the specialised world of information systems.) It hardens target objects or makes them less attractive; it reduces the usefulness of objects to facilitate crime (eg making it harder to change the signature on a credit card). It reshapes environments to hinder and deter offenders and crime promoters, and aid crime preventers (including making it easier for *managers of places* such as shopping centres to protect their workplace).

But this situational focus does not mean the offender is ignored. An environment only affords concealment to an offender who blends in well and is accomplished in stealth. A certain level of access control assumes, for example, that the offender has no code, pass, key or lock-picking skills. A target is only vulnerable in relation to the offender's strength to carry it away, agility to reach an open window or knowledge of how to cope with its security fixings (perhaps through access to illicit information). Any target's attractiveness is in the eye of the beholder, whether this is the direct appeal of the latest Porsche or a more calculated consideration of the ease of disposing of it - eg access to 'fences', and the going price for the loot (the state of the market for resale of stolen goods).[16]

Designing against rational offenders?[17]

The highly rational view of the offender portrayed above is an ideal image which does need some qualification. Researchers widely assume this rationality is limited by imperfect knowledge and imperfect calculation and selection of alternative outcomes. In some cases rationality can be extremely limited. Wright and Decker,[18] in interviews with active burglars in St Louis, show how offenders in this particular 'street' setting are highly impulsive. What is more, the impulsivity is not simply a matter of deficient mental skills on the part of the offenders, but seems to be rooted, even valued, in the lifestyle of their subculture. This same lifestyle actually *places* them in positions of frequent financial crisis (to get money to pay off debts, buy the next fix of drugs or simply to party) which means

they are often *forced* at short notice to find some target to burgle. Under these conditions, the amount of decision-making that they can exercise even at the fairly tactical level ('target this street or the next?') is highly constrained and offenders even seem to shut down their decision-making deliberations to force themselves to overcome anxieties and *act*.

Nevertheless, enough of the more rational kinds of offenders exist to make designing against them a continuing challenge. And even under extreme conditions where deterrence through the manipulation of perceived risk makes no impact on offenders, design still has a part to play in raising the objective difficulty of crime. An armoured glass screen protects the bank against the most desperate and bone-headed till-snatcher. One interesting possibility is that 'selection pressure' from crime prevention and policing is forcing the divergence of criminals into two broad groups occupying rather different niches - skilled specialists and unskilled generalists.

A second aspect of offending which qualifies - but does not rule out - rationality is the distinction to be drawn between 'instrumental' (calculating means to an end) and 'expressive' crime (whose commission is an end in itself, such as smashing windows 'for fun' or assaulting someone in retaliation for an insult). Expressive crimes may often be impulsive, and here design-against-crime possibilities are constrained but not excluded. Some expressive crimes may, though, be planned - consider an organised racial attack putting fire bombs through letterboxes.

With both 'less rational' offenders, and expressive crimes, design still has an important role to play. But the kind of design solutions that are appropriate will clearly differ.

The IT dimension

As with all other aspects of modern life, IT has begun to pervade crime prevention. In the long term, the evolution of IT probably favours neither offenders nor preventers. It can equally supply targets of and aids to crime, or facilitate its prevention. More broadly still, it can set the scene in which crime and crime prevention occur. In fact (apart from the physical theft of or damage to IT components), we can re-cast the conjunction of criminal opportunity in cyberspace. IT enters the picture in three related realms: *networks and communications, systems and data capture and response*.[19]

Networks and communications

With the advent of telecommunications, the immediate circumstances surrounding the criminal event need no longer be defined exclusively by physical conjunction of the components in time and space. *Offenders* may act from a remote location - through *'telepresence'* - hacking into a computer to commit fraud, dispatching a bomb by post, making an obscene phone call or using mobile phones to reduce the risk in dealing in

drugs.[20] The Internet may even be used to exchange knowledge of methods of offending, boosting *offenders' resources*[21] and facilitating conspiracy to commit offences. Likewise, in the crime situation, *crime preventers* can remotely observe the state of the target of crime and/or actions of offenders, through CCTV, intrusion detectors etc; and equally remotely operate security doors or summon assistance to the spot. Various kinds of Watch networks could circulate information on intranets, pagers or public lines.[22] A computerised financial network, or the Internet, could act as the logistical *environment* in which offenders and crime preventers take each other on, and attack, or defend, the target information. Facilities like Internet firewalls specifically designed to prevent access to the home system can be regarded as the *target enclosure*. A network environment can also convey motivational influences such as a 'meeting of minds' of paedophiles. As for *targets* themselves, telecommunications equipment such as mobile phones can be the target of theft, and of destruction - as by vandals or (on a larger scale) terrorists. There has been a long-term trend towards greater value and greater portability of objects such as computers or TVs, which has enhanced their attraction and vulnerability. Targets can however be *reduced* in value if, through telecommunication, the exposed, portable element of a system is made cheap and replaceable while the complex and/or vulnerable element is kept in more secure conditions. An example here would be a cheap *terminal* connecting through cheap high-capacity links to a well-protected central *computer*. Encryption of messages (or stored data more generally) is a kind of target-hardening of information. Interestingly, the whole area of *telesales* seems to be a rare example of a system actually *waiting* for credible crime prevention arrangements to be developed before it takes off.

Systems

Computer systems can be the *target* of *physical* crime (theft of whole or parts, malicious physical damage) or the *environment* of crime against *information* as target (threats to confidentiality, integrity or availability of information on that computer or in that system perpetrated by external hackers, internal misusers or viruses; breach of software copyright or data protection rules). They can also be *crime facilitators*, enabling offenders to hack into other systems for fraud, industrial espionage or vandalism, or circumvent utility charges (eg overcoming access controls to satellite pay-TV). *Crime preventer* functions can be built into computers, whether protecting their own hardware, software or information, or serving to protect other, external, targets.

Data capture, decision and response

The ability to gather information, perceive suspicious patterns and respond are universal elements of the crime prevention function - whether conducted by humans, guard dogs, or artificial active systems. The capacity to *perceive* what is in the process of occurring can be programmed into a CCTV system - eg detectors of movement, open doors or breaking glass. Likewise intelligent systems can be created to monitor financial transactions, such as credit card payments, for suspicious patterns. Decision involves judgement as to whether action is necessary (and if so, what type) - whether the judgement operates

through a simple 'signal detection' process distinguishing the infra-red signature of a cat from a cat burglar, or something far more subtle (eg checking out suspicious noises in relation to an understanding of who is likely to be in the house legitimately, and when; or even judging whether a valuable item is being removed by a legitimate owner or a thief). *Response* can range from sounding an alarm to locking gates, initiating a video recording, immobilising a vehicle or a computer, transmitting a tracking signal or pumping out obscuring smoke (but not yet making a cybercitizen's arrest unless one counts banks closing all exits automatically to 'imprison' the offender).

'Master, Master, he's stealing me!' cried the magic harp as Jack bore it away from the Giant's castle. Smart technology, combining data capture, decision and response, can turn previously passive targets of crime into active crime preventers. (Preventers need not always be human, although Robocop is still a long way off.) It can store identification information to aid reacters in retrieving stolen property, proving ownership, apprehending and convicting offenders and inhibiting resale. It can insert new crime preventers into the crime environment to act on their own or in conjunction with human preventers. The design challenge described earlier can become a design opportunity. While value to offenders of exposed targets (such as mobile phones or laptop computers) can be increased by smart functions, by the same token the targets can be made better able to defend themselves by summoning assistance (protesting or sending messages via tracking systems or simply over the telephone) shutting down until a security code is supplied, coating their internal components with dye (in both cases reducing their value to the thief) or making life difficult for the offender (sticking out arms to make themselves awkward to carry or conceal).

IT: distinctive features

One of the most distinctive features of IT is its rapid evolution. This applies to IT-based criminal methods and countermeasures: both offenders and defenders can swiftly upgrade their software or hardware. And, as previously remarked, new facilities such as mobile phones or the Internet offer completely new conjunctions of opportunity. Another distinctive feature of IT as a whole is the reduced importance of physical constraints of proximity, physical strength etc in transactions whether honest or criminal. To take this point further, much evolution of IT is largely formalised in software development. Here, when humans rewrite the script and redefine the environment in which it unfolds, they are less constrained by hard physical reality than by *convention* (there are disturbing parallels with the development of successive generations of cops and robbers computer games!). With IT, there is also increased scope for creating highly-integrated *preventive systems* - in which features of the target readily dovetail in with features of the environment and those of crime preventers . (For example, 'electronic article surveillance' involves a target article designed to communicate with a detector, which is itself placed in an environment designed so that a) offenders have to pass through the detector and cannot exit any other way, and b) crime preventers in the shape of store staff have time to intervene before the offender escapes.)

In the IT field, offenders are assumed to be generally very skilled and knowledgable - hence highly creative in spotting opportunities and adaptive in coping with countermeasures. But IT-based crime preventers also increasingly have the adaptive capacity to handle *contingencies*. Such contingencies could be covered by inbuilt intelligence and creativity, or by intensive preprogramming to tackle all possible outcomes (such as the expected menu of tactical countermoves by offenders - chess-playing computers are an extreme example of something similar, albeit playing to a very narrowly-confined set of rules).

The evolutionary dimension: the adaptable offender

Offenders can fight back against design modification: this bestows a particular quality on design in the service of crime prevention. The concept of *displacement* describes the possibility that offenders, blocked in their first choice of target, will not always give up but try different methods of attack, seek similar targets at other times and places, or change to another type of target altogether. If overall crime levels are not actually reduced the gain to society from the investment in prevention may be neutralised. Recent reviews, however, indicate that displacement is at worst only partial.[23]

However, there is no doubting the active, adaptive nature of offending, which sometimes involves a design process of its own. This is not new - shortly after the Greeks introduced silver coinage in about 600 BC, someone produced a silver-plated bronze forgery.[24] Elizabethan fraudsters apparently developed 14 different kinds of crooked dice.[25] More recently, car thieves, according to police wisdom, will rent a new model to reveal its vulnerabilities (for example, thieves discovered on a particular model whose central locking system relied on compressed air lines, that a tennis ball with a hole cut into it, when placed over a door lock and struck, obligingly caused all the locks to open.) The fruits of such 'professional' research and development may of course be transmitted to a wider circle of 'amateur' offenders, meaning that the actions of a few highly-skilled and determined pioneers have far wider repercussions. To continue with the car example, still more sophisticated developments involve remote locking devices. Simple systems transmitting a single fixed access code have proved vulnerable to electronic 'grabbers' which can detect and mimic the signal; consequently, manufacturers have been forced to create the equivalent of the spy's one-time pad, where the access code resets after each use in a quasi-random fashion.

Amazingly, something akin to a grabber was invented in Victorian times, suggesting that the new ‘mechanical’ technology of the Industrial Revolution gave rise to as many new crime opportunities as the new electronic technology of today, indicating perhaps that ‘Kondratiev long waves’ occur in crime as well as in the ups and downs of the legitimate economy.[26] In the case in point, one George Bliss, an American bank burglar, purchased combination locks as they came on the market, to study their mechanisms. Tiring of

conventional lock picking to get into safes, he invented the 'Little Joker' - a tiny instrument of thin steel wire which he concealed under the combination dial knob. Returning to the bank a night or two later, Bliss was able to read from the marks left on the wire, which numbers had been selected. All he had to do to get into the safe was identify the right sequence.

Like spies, security systems can themselves be particularly vulnerable to 'turning' into double agents: pickpockets can watch commuters helpfully pat their concealed wallets as they pass a 'beware - pickpockets' poster. In the comfort of their own homes, criminally-inclined residents can monitor TV pictures of communal entrances to apartment blocks to see, not which stranger is coming in, but which neighbour has just gone out.

But despite these anecdotal examples, little is known systematically about offenders' approach to R & D - how it occurs, and how it is disseminated. Academic research interviewing offenders has not yet significantly focused on this aspect.

An evolutionary perspective on design

We thus have a picture of offenders and preventers engaged in move and countermove in a ceaseless struggle for temporary advantage, with the design of the car, the banknote, the accounting system or whatever, continually evolving as a result. This '*crime struggle*' resembles other struggles: the *arms race* (ranging from the design of cannon versus improved fortifications, to radar versus stealth technology), *intelligence* (espionage versus counterespionage), the *control of disease and pests* (bacteria versus antibiotics or rats versus warfarin), and even completely 'natural' struggles such as *microbes versus immune system*, and *predator versus prey*. Common to these struggles is *protracted conflict between adaptive agencies*. All the struggles (whether they are mediated by rational thought or some other process such as natural selection) are pursued through development in tactics, strategy, and evolution of design. Evolutionary ecology offers a useful framework - the more recent ecology of predator-prey relationships and survival strategies through changing structure or behaviour, rather than the ecology of zones used by earlier criminologists to characterise urban form and to understand the location of criminal neighbourhoods.[27]

At the risk of oversimplification, an equilibrium can be approached in which a certain level of crime (or disease, or predation) is the lowest that preventers can achieve, when set against increasing cost and other requirements such as freedom and privacy, and the highest that offenders can achieve, when set against risk and effort.[28] A major purpose of this paper is to argue that these equilibria are dynamic and not static, provisional and not permanent, with important consequences for design.

In biological evolution such stand-offs can hold for very long periods of time, with predators and prey ceasing to evolve significantly (although numbers of predators and numbers of prey may fluctuate from year to year). Normally only external perturbations

such as climate change or invasion of a new species will tip such equilibria off-balance. Related to this is the familiar sequence of *'naive' new target ? crime harvest ? retrofit solution*,[29] which is parallelled by analogous outbreaks of *new disease ? heavy toll ? population resistance*, or *new weapon ? momentary military advantage ? balance of force restored*. In human struggles, however, we are nowadays constantly living on self-disturbed ground. Technological, social and economic change disrupt equilibria or prevent them from ever forming. New targets for crime are continually emerging - initial theft rates of mobile phones are extremely high (will the next target be the digital still camera - attractive, expensive, highly portable?). New tools become available to help offenders - the cordless drill is a boon to phone-box cash thieves. New lifestyles leave homes unprotected during the day. And new crime environments appear - such as the Automatic Teller Machine (rather like the African waterhole around which predators loiter).

The classic example of externally-driven change, perhaps, is the shop. The evolution of the enclosed, small, well-staffed counter-shop from the open market stall was, for some decades, the culmination of nearly perfect crime-prevention. This near-equilibrium was then completely swept aside by the arrival of the supermarket, against which the counter-shop could not compete except in restricted niches, but which as an unwelcome by-product provided much more opportunity for crime. Owners were able to sustain the consequent high levels of crime for a while because of the *very* high level of sales, - but eventually the security struggle resumed in earnest, albeit in a very different kind of game with store detectives, electronic theft detectors and so forth.

Crime prevention design can learn from these ecological connections, in the design of specific countermeasures. For example, some harmless insects cheat on investment in poison glands, by adopting other species' warning colours; in crime prevention, cost savings can be made by restrained use of dummy alarms or dummy speed cameras.

But we can also use the evolutionary perspective to step back from the immediate struggle to offer more strategic guidance.[30] The use of a *variety* of antibiotics is a strategy that doctors employ to slow down the adaptation of pathogens; in crime prevention, approaches which operate through performance standards to foster design freedom can promote similar variety in preventive measures. Standardisation of products or techniques, on the other hand, although superficially attractive, is likely to be counter-productive. In agriculture, the Potato Blight spread like wildfire through a crop monoculture; likewise, if one offender learns to overcome a mass-produced standard car lock, soon all will know the trick. Genuinely poisonous insects adopt warning coloration to *speed up the learning process* of birds - who rapidly come to avoid the foul-tasting or stinging prey; in crime prevention, increasing objective resistance of targets should be accompanied by signalling to this effect (whether using stickers on the targets or wider publicity campaigns), to reduce the damage from failed attempts and gain a better payoff from deterrence to add to the mere effects of physical blocking. At a more general level,

we should be able to learn the kinds of defensive strategies prey animals, food plants (or the military) evolve to see them through the long term, and whether there are any common features of short-lived strategies that crime prevention designers could avoid.

Gearing up against crime

Up to now, those involved in crime prevention have rather assumed this was a 'one-off' activity that needed only to be applied a limited number of times to a given crime problem, for it to be permanently reduced. This is analogous to early beliefs in the 'miracle' of antibiotics. We now have to move to a much more *dynamic* approach. Evolution has been described as a 'Red Queen's game'[31] (from Alice through the Looking Glass), in which you have to keep running merely to remain in the same place. In this instance the challenge is to keep up with the adaptive criminal in a changing world. *More particularly, how can we help methods of 'prevention by design' to evolve as fast as methods of offending, in the face of a stream of new opportunities for crime?*

From previous sections we can draw together a number of points of action, whether operating on a day-to-day *tactical* basis dealing with specific, immediate design problems or over a more 'evolutionary' and *strategic* timescale of months or years. Beyond this is what might be called action to promote the *infrastructure* of design against crime - creating an environment of theory, knowledge gathering and dissemination, understanding, and perhaps, even, the law which can empower designers more generally to gear up to tackle new problems as they emerge. Some of the points that follow involve boosting the capacity for *anticipation* - the preferred solution. Others serve the inevitable requirement to shut the stable door before the *next* horse bolts. This involves *reacting* to design failure (where a new design ignores or falls short of criminals' current capacities) and design obsolescence (where changes in the techniques and tools available to criminals make them more effective at defeating an originally successful design). In all cases we assume that sufficient numbers of sophisticated, determined, calculating and adaptable offenders will continue to enter the field for the evolutionary process to provide a constant challenge to design.

Design tactics

- During design, consider the *causal mechanisms*[32] by which the preventive design feature works: for example, if the feature is supposed to work by heightening subjective risk to the offender, is the risk posed plausible? Such links with theory are vital: beware the 19th century British craftsman-engineers who remained stuck with intuition while their continental and American competitors steamed ahead with engineering science.[33]

- *Anticipate criminals' countermoves* - whether tactical (eg when balked by a security screen in a bank, what if the robber takes a customer hostage?), or strategic (eg how

long before an offender designs a new picklock or computer hacking procedure?). This capacity of legitimate designers to anticipate criminality requires a major reversal of design perspective - from 'how can this object, system or service be improved for legitimate users?' to 'how will it be misused, damaged or misappropriated?' and 'how will they obtain or crack the code?' Designers' immediate capacity to 'think thief'can be developed from interviews with offenders or employing a 'retired' offender on the design team to try to find vulnerabilities, and can be applied through challenging the design process or penetration testing of prototypes. CAD or virtual reality facilities to 'walk around' a design could be used to aid visualisation from the offender's perspective ('Someone could get up that drainpipe if that ledge isn't removed.').

- *Block as many countermoves as possible* - for example by designing household security as a holistic package in which there are no Achilles' heels (there is little point in fitting strong locks if burglars can simply kick the weak door frame in). There is a need, nevertheless, to remain aware of diminishing returns and costly 'over-engineering' to counter the professional when most offenders in the particular local circumstances are amateurs. Thus awareness of the kind of offenders currently likely to exploit a given opportunity is an important consideration in the decision to invest in design and production costs on crime prevention - an aspect of fitness for purpose. However, crime targets or environments that interest amateurs today may attract professionals tomorrow - so designers should perhaps build in the potential for upgrading security if this subsequently becomes necessary (much as car manufacturers keep some innovations in their new model in reserve, to entice people to buy next year's version).

- More generally, anticipate design failure or obsolescence by *building in the possibility for remedy* - making the inevitable retrofit solution easier. Here, the information technology software or hardware *upgrade* in mobile phones or computers is the model, rather than the slow changes possible in the next generation of houses or cars (the half-life for replacement of the British car stock is 10 years). Modular design of physical products will promote physical upgrades too, although *dispersal* of a function, such as the components of a car radio or the security facilities within a mobile phone, is a countervailing technique that may need to be considered.

- *Act on several fronts* simultaneously (like multiple antibiotic regimes) - eg hardening the target of crime whilst rendering it less attractive for resale by increasing its identifiability and cracking down on the marketing of stolen goods. In this, prevention by design can be integrated with other preventive approaches.

- Acknowledge that methods of offending, vulnerabilities of targets (including 'back door entries' used by maintenance engineers to gain access to software or hardware), and methods of prevention will from here on proliferate more rapidly than ever before, becoming *readily accessible knowledge to offenders* via the Internet. Seek therefore to devise problems that are *difficult for offenders to solve*, even if they know

how the preventive measure works (for example some encryption systems rely on offenders *not* possessing massive computing power for the foreseeable future).

Design strategy

- Encourage anticipation of misuse by conducting *'crime impact statements'* for proposed new tools, trading practices and so on, identifying features which may make existing preventive measures obsolete. *Producers* could be motivated to do this from a 'good citizen' perspective (seeking praise or avoiding accusations of 'aiding and abetting' crime). To augment market forces, *users* of potential crime targets could be helped to spot any threat from a new product as early as possible, by consumer or professional assessments, as currently happens with cars.

- Acknowledge that despite anticipatory measures, even the best preventive method will have a *limited life span*, the designer's aim being to develop ones that merely become obsolete less rapidly. From military and biological evolution comes the concept of *momentary advantage* - that afforded by a new kind of fortification or a new kind of claw - useful briefly, but soon to be matched by a new kind of projectile or a fleeter foot. Military science may illuminate how best to use a whole sequence of momentary advantages.

- Where anticipation fails, cope rapidly with 'crime harvests' by accelerating the learning curve for designers. Setting up a *'learning path'*, involving systematic assembly of crime incident information of the right kind (eg how the lock was broken/ the security code was obtained or circumvented), can speed up the process whereby they get feedback on the vulnerability of their products and make suitable adjustments. In this way, products can be kept ahead of most offenders. The reluctance of victims - particularly corporate victims - to risk public embarrassment by reporting crimes and otherwise passing on vulnerabilities, is a problem likely to need addressing.

- Design not to fixed construction standards, such as incorporating a particular type of lock, but to *performance standards* (eg 'the lock must be able to withstand 20 kg of force and to resist expert picking for 20 minutes').[34] This slows down obsolescence: it gives designers the freedom to devise a range of different solutions rather than constraining them to a single one whose vulnerabilities can quickly be learned and transmitted among offenders. It also prevents manufacturers from 'designing down' to minimum construction specifications and thereby absolving themselves from responsibility. Offenders faced with *uncertainty* about what preventive systems they may find in the next home or the next ATM, are at a considerable logistical and psychological disadvantage.

- Consider deliberately *shaping* offenders, their subcultures and the markets for crime - for example by forcing offenders to become more specialised in terms of knowledge,

skills and equipment - hence confined to a specific niche, and perhaps more easily personally identifiable (as with old-time safecrackers). By viewing offenders as illicit entrepreneurs, price them out of the market in terms of the cost/difficulty of obtaining equipment in relation to the risks and rewards of offending. Look for biological or military analogies - eg where the Soviet Union was priced out of the arms race (they spent 18% of GDP on defence, the Americans 6%).

- Anticipate *adverse shaping* - eg when offenders are forced to focus on weak human links in otherwise tight security - hostage taking of customers when bank robbers foiled by security screens; carjackers taking drivers with them to operate the car security system. Seek, by design or by procedure, to remove utility of humans as unwilling crime facilitators (eg 'keys held at depot'). More broadly be wary of shaping offenders towards *organised* crime (on the unevaluated assumption that this is generally worse than the free-for-all equivalent).

- *Know your offenders* - differentiate between design problems imposed by calculating, skilled and highly adaptable criminals and those where only the impulsive and poorly-resourced have to be countered. Distinguish also between the kinds of problems posed by instrumental versus expressive offending.

- Be alert to becoming locked in a *pointless competitive spiral* of design and counterdesign - being prepared to jump sideways in strategy using lateral thinking. Jumping right out of the design track may be more appropriate under some circumstances - for example where technology currently gives the advantage to offenders, deliberate switching of crime control effort to conventional law enforcement and offender-oriented approaches may be more appropriate until the balance of power changes back. More radically, one might consider decriminalisation - for example, decriminalising vehicle road fund licence evasion simply by abolishing the tax disc and collecting revenue through fuel tax. (In effect this is a kind of design approach to the tax and legal systems.)

Design infrastructure

- Conduct systematic studies of i) *offenders' resources* - knowledge, information sources and networks, skills and adaptability and ii) *methods of offending*. Resting content with the crude distinction between 'professionals' and 'amateurs or opportunists' is no longer enough. This approach could for example result in development of a 'criminal expert system' to help designers think thief.

- The 'conjunction of opportunity' *conceptual framework* described in this paper could be developed further to serve this latter purpose.

- Learn from the *extinction* of crimes - which ones have fallen into disuse,[35] such as safecracking or robbing banks, and why?

- Learn 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.[36]

- Learn the methods of, and cautiously use the predictions of, sohpisticated attempts at *technology foresight.*[37]

- Examine the *legal context* - can laws or the rules of evidence be made more helpful to prevention in particular circumstances - eg on proof of ownership? Is there scope for developing civil liability of designers who neglect crime prevention principles, as in the USA?

- Help crime prevention *practitioners*, as users of designs and customers of designers, become *adaptive* themselves - accustomed to using fundamental principles rather than superficially relying on fixed recipes from a few success stories.[38] Beware, for example, of the 'communal entrance porch' that was designed to restrict access to each block of flats on an estate, but merely enabled burglars to gain access to all the first floor windows.

- Finally, in contributing to this infrastructure, criminologists in their turn have to 'think designer'. This applies across the board from practical detail such as alertness to issues of cost benefit, to provision of guidance in suitable formats, or to legal issues.

The suggestions for action put forward in this paper are preliminary and I welcome comments to take the ideas further. They flow from the central premise that crime prevention by design (and indeed by other situational strategies) not only involves the designer in a radical shift in perspective (from envisaging use to envisaging misuse) but also in gearing up to keep pace with changing circumstances and adaptive offenders. The suggestions are necessarily diverse. Some are the province of central Government policy and research, others involve the police, others designers and their commissioners, and organisations responsible for professional standards and guidance. A number require collaboration. Currently in England, the Home Office Crime Prevention Agency is taking this process forward, addressing not just the technological and design issues covered here but also the problems of implementation - arranging for the incentives and levers to make it all happen.

Notes

1 Principal Research Officer, Offenders and Corrections Unit, Home Office Research and Statistics Directorate, 50 Queen Anne's Gate London SW1H 9AT. E-mail paul.ekblom@rpu.hmg-ho.gov.uk. For ideas and encouragement I am grateful to Professor Ken Pease of Huddersfield University - and Chair of the Technology Futures working group of the Crime Prevention Agency Board; also to my colleagues Peter Goldblatt, Gloria Laycock and Professor Nick Tilley.

2 Poyner, B. and Fawcett, W. (1995) *Design for Inherent Security: Guidance for non-residential buildings*. London: Construction Industry Research and Information Association.

3 For an in-depth discussion of the conceptual tangle of crime prevention, and a proposed solution - drawn on later in this paper - see Ekblom, P. (1996) Towards a Discipline of Crime Prevention: A Systematic Approach to its Nature, Range and Concepts, in Bennett, T. (ed) *Preventing Crime and Disorder: Targeting strategies and responsibilities.* Cambridge, England: Institute of Criminology.

4 For a review of 'schools' of crime prevention through design, and an attempt to connect the design process to the 'preventive process', see Ekblom, P. (1995) Less Crime, by Design. *Annals, American Academy of Political and Social Science,* May issue, pp 114-129.

5 Poyner and Fawcett, op cit, argue the case for 'inherent' security - taking it into account from the start of the design process.

6 See for example 'UK ITSEC' - the UK IT Security Evaluation and Certification Scheme.

7 A good discussion of this and other crime prevention implementation issues is in Laycock, G. And Tilley, N. (1995) Implementing Crime Prevention, in Tonry, M. and Farrington, D. (eds), *Building a Safer Society: Strategic Approaches to Crime Prevention.* Crime and Justice: A Review of Research, Vol. 19. London and Chicago, University of Chicago Press.

8 Ekblom, P., Law, H., and Sutton, M. (1996) *Research Findings 42: Domestic Burglary Schemes in the Safer Cities Programme.* London: Home Office.

9 See note 3 above. It is intended to update the 'conjunction of criminal opportunity' framework. The author welcomes comments.

10 The notion of the conjunction of criminal opportunity was developed, and extended, from Cohen and Felson's widely-cited 'Routine Activities Theory'. Cohen, L. and Felson, M. (1979) Social Change and Crime Rate Trends: a Routine Activity Approach. *American Sociological Review.* Vol. 44, pp 588-608. Felson, M. (1992) Routine Activities and Crime Prevention: Armchair Concepts and Practical Action. *Studies on Crime and Crime Prevention.* Vol.1 pp 30-34.) In RAT, for the criminal event to happen, there must be a conjunction of a 'likely offender', a 'suitable target' and the 'absence of capable guardians'. Basically I have added 'environment' to begin to incorporate the perspective developed particularly by the Brantinghams - eg Brantingham, Patricia and Brantingham, Paul (1995) Criminality of Place: Crime Generators and Crime Attractors. *European Journal on Criminal Policy and Research.* Vol. 3, No. 3, pp 5-26) . I have also attempted to fill in why the offender is likely, the target suitable and the guardians (crime preventers) capable; and have added crime promoters. In my earlier papers (eg see note 3 above) the 'immediate circumstances' surrounding the criminal event, in which the conjunction of criminal opportunity occurs, were referred to as the 'proximal circumstances'.

11 For an exposition of the 'Rational Offender' approach see Clarke (1995, in note 14 below) and Cornish, D. and Clarke, R. (eds) (1986) *The Reasoning Criminal: Rational Choice Perspectives on Offending* New York NY: Springer-Verlag.

12 The useful concept of scenes is set out in Cornish, D. (1994) The Procedural Analysis of Offending. *Crime Prevention Studies 4,* pp 151-196, Monsey, N.Y.: Willow Tree Press.

13 These concepts are taken from Cohen, L., Vila, B. and. Machalek, R. (1995) Expropriative Crime and Crime Policy: An Evolutionary Ecological Analysis. *Studies on Crime and Crime Prevention* 4:2, pp 197-219.

14 For an authoritative review of situational prevention, see Clarke, R. (1995) Situational Crime Prevention, in Tonry, M. and Farrington, D. (eds), *Building a Safer Society: Strategic Approaches to Crime Prevention. Crime and Justice: A Review of Research*, vol. 19. London and Chicago: University of Chicago Press.

15 Tilley, for example, identified *nine* different ways installing a CCTV installation in a car park could prevent crime - some operating through crime preventers (direct monitoring and arrest; attracting already security-conscious patrons), others through the offender. Tilley, N. (1993) *Understanding Car Parks, Crime and CCTV: Evaluation Lessons from Safer Cities.* Crime Prevention Unit Paper 42. London: Home Office.

16 The market for stolen goods - how it might influence the crime rate and how it might be manipulated for purposes of prevention - is an under-researched area. See Sutton, M. (1996) Supply by Theft: Does the Market for Second-Hand Goods Play a

Role in Keeping Crime Figures High? *British Journal of Criminology*. Vol. 35/3, pp 400-416.

17 I am grateful to an anonymous reviewer for setting me on this train of thought.

18 Wright, R. And Decker, S. (1994) *Burglars on the Job* Boston: Northeastern University Press. For a contrary example of highly rational, professional offenders see Wiersma, E. (1996) Commercial Burglars in the Netherlands: Reasoning Decision-Makers? *International Journal of Risk, Security and Crime Prevention*. Vol. 1 No. 3. pp 217-225.

19 I am grateful to Professor Joshua Bamfield of Nene College for suggesting these headings.

20 The role of mobile phones as facilitators of crime is discussed in Natarajan, M., Clarke, R. and Johnson, B. (1995) Telephones As Facilitators of Drug Dealing: A Research Agenda*. European Journal of Criminal Policy and Research.* Vol.3, No.3, pp 137-154.

21 The role of the Internet in crime is discussed in Mann, D. and Sutton, M. (Forthcoming, British Journal of Criminology) *>>Netcrime: More Change in the Organisation of Thieving.*

22 British Telecom are currently piloting a local community intranet in the Ipswich area.

23 Hesseling, R. (1994) Displacement: A review of the literature*. Crime Prevention Studies 4,* pp 197-230, Monsey, N.Y.: Willow Tree Press.

24 James, P. and Thorpe, N. (1994) *Ancient Inventions*. London: Michael O'Mara Books.

25 Salgado, G. (1984) *The Elizabethan Underworld*. Gloucester: Alan Sutton. For a good review of more recent shifts in criminal opportunities see Shover, N. (1996) *Great Pretenders: Pursuits and Careers of Persistent Thieves*. London: Westview Press/Harper Collins.

26 Hamilton, C. (ed) (1953) *Men of the Underworld: the Professional Criminals' Own Story* London: Gollancz.

27 A review of links between modern ecology and crime is in Brantingham, P. and Brantingham, J. (1991) *Niches and Predators: Theoretical Departures in the Ecology of Crime*. Presented at Western Society of Criminology, Berkeley, California.

28 van Dijk, J. (1994) Understanding Crime Rates: On the Interactions Between the Rational Choices of Victims and Offenders. *British Journal of Criminology,* 34, pp 105-121. Also on similar lines Cook, P. (1986) The Demand and Supply of Criminal Opportunities, in Tonry, M. and Morris, N. (eds), *Crime and Justice: An Annual Review of Research*, Vol. 7. London and Chicago, University of Chicago Press.

29 Pease, K. (in press) Predicting the Future: the Roles of Routine Activity and Rational Choice Theory, In Newman, G. Clarke, R.V. and Shoham, S.G. (eds), *Rational Choice and Situational Crime Prevention: Theoretical Foundations*. Aldershot: Dartmouth.

30 Some of these strategic ideas have also been put forward, from a slightly different angle, by Cohen, Vila and Malachek (op cit), who also suggest 'crime method surveillance' analagous to the surveillance that is now set up to monitor new diseases.

31 The 'Red Queen Hypothesis' was first put forward in van Valen, L. (1973) A New Evolutionary Law. *Evolutionary Theory.* Vol. 1, pp 1-18.

32 For a 'Scientific Realist' discussion of causal mechanisms in a practical crime prevention context see Tilley, op cit.

33 Rolt, L. (1970) *Victorian Engineering*. Harmondsworth: Penguin.

34 *British Standards* for vehicle construction etc favour this approach. Performance standards have to be comprehensible, too, to legitimate users who need to know how much protection they can expect to gain from installing equipment bearing the standard (a point suggested by Martin Gill of Leiceter University).

35 See Walsh, D. (1994) The Obsolescence of Crime Forms. *Crime Prevention Studies 2,* pp 149-164, Monsey, N.Y.: Willow Tree Press. Shover (Op Cit) provides a useful history of safecracking which ends in near-extinction of the trade.

36 A paper by the author, *Gearing Up against Crime (2): Can we make crime prevention adaptive by learning from other evolutionary struggles?*, is in preparation.

37 One excellent example of technology foresight is by Eric Drexler, who looks carefully ahead a few decades to 'nanotechnology' - manipulation of materials at the molecular level, which has already begun. Drexler, K. E. (1996) *Engines of Creation*. London: Fourth Estate. Intriguingly, Drexler identifies the development of self-

replicating and evolving ‘nanotools’ as a major threat as well as an opportunity. His solutions, in terms of developing ‘active shields’ have something in common with our own immune system and indeed with the active, adaptive approach against crime advocated in this paper.

38 A study of attempted replications of the well-known Kirkholt burglary prevention project revealed further examples of the tendency to copy recipes superficially rather than intelligently apply principles to appropriate data on local circumstances. Tilley, N. (1994) *After Kirkholt - Theory, Method and Results of Replication Evaluations*. Crime Prevention Unit Paper 47. London: Home Office.