DESIGN AGAINST CRIME
Research Centre

Gearing up Against Crime

January 2008

Prof. Paul Ekblom

University of the Arts London
Central Saint Martins

5Is, CCO, CLAIMED and definitions in depth of partnership, crime prevention and community safety are all covered in Crime Prevention, Security and Community Safety Using the 5Is Framework, by Paul Ekblom (Basingstoke: Palgrave Macmillan 2011). See **www.palgrave.com/products/title.aspx?pid=296569** and author's blog at **http://5isframework.wordpress.com/.**

Gearing up Against Crime

Prof. Paul Ekblom

Gearing up against crime (GUAC) is an evolutionary framework for understanding, and coping with, the crime and crime-prevention implications of social and technological change and adaptive/innovative offenders. The central idea is that what works against crime now, may in the future become irrelevant (because crimes change as a function of technological, ecological and social change, and criminal innovation) or obsolete (criminals eventually find ways to defeat individual preventive methods).

This adds a whole new level to the strategy of crime prevention: rather than simply attempting to cover the ground once ('ok, we've reduced car crime, now let's tackle burglary') we have to do it again and again. In fact, we are in an arms race (or several subsidiary arms races in specialized areas, e.g. cybercrime, terrorism, car theft) in which the long-term crime rate is determined by which side, preventers or offenders, is innovating and deploying the faster. (Analogy: the level of water in a bath is the resultant of how fast it is pouring in from the taps versus draining out through the plughole.)

It follows that understanding arms races and how they work, and being prepared to invest in innovative capacity (quality of theory and research, training and orientation of scientists, technologists/engineers and designers) are high-level strategic requirements for crime prevention. Medium-level requirements are development of specific strategies covering how to run arms races or avoid them. Many of these are set out in the two publications downloadable from this page – for example the importance of fostering variety rather than uniformity in preventive interventions; and the utility of drawing on experience from other arms races such as the military, or antibiotics versus bacteria.

The themes inaugurated in these two papers continue to unfold in later work – for example in From the Source to the Mainstream is Uphill (Ekblom 2002 – see the 5Is framework), How to Police the Future (Ekblom 2005 – see Misdeeds and Security Framework) and Designing Products against Crime (Ekblom 2005).

Origin and Background

In 1995 the UK Home Office's 'Crime Reduction Agency' (in fact a policy unit in all but name) set up a subunit of its governing board to focus on 'crime futures'. Encouraged by board member Ken Pease, Paul Ekblom submitted a paper which was eventually published as Gearing up against Crime (1997). In 1999 a follow-up paper was published.

Both these papers fed into the crime futures projects within the UK Foresight programme www.foresight.gov.uk (Foresight Crime Prevention Panel and Cyber Trust and Crime Prevention) and imparted a crime flavour to others (Intelligent Infrastructure).

The main paper setting out GUAC is:
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,* 2/4: 249-265. Although some aspects of the paper are outdated, the main ideas on arms races are still valid.

Abstract

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.*

Download 'Gearing Up Against Crime'

The follow-up paper is:
Ekblom, P (1999) 'Can we Make Crime Prevention Adaptive by Learning from other Evolutionary Struggles?', *Studies on Crime and Crime Prevention,* 8/1: 27-51.

Abstract

Crime prevention faces a perpetual struggle to keep up with changing opportunities for crime and adaptable offenders. To avoid obsolescence, it has to become adaptive itself. The task of keeping prevention up to date resembles other evolutionary struggles such as biological co-evolution between predator and prey (eg continually sharper teeth versus continually tougher hide), or military arms races (eg more powerful guns versus heavier armour). These are both examples of protracted co-evolution of conflicting parties against a background of incidental disturbances which from time to time give the edge to offenders or to defenders. The disturbances in question originate from natural processes or human ones (such as the arrival of new technology). This paper explores the lessons for crime prevention which might be drawn from the other struggles at several levels: technology/ engineering, generic new methods of prevention and strategic concepts in prevention. An extremely wide range of possible lessons is identified which can take crime prevention a long way up the learning curve, but caution and consolidation are advised. Some ways of achieving this consolidation through systematic mapping are considered but not yet attempted.

Download 'Evolutionary Struggles'

References

Ekblom, P. (2002). 'From the Source to the Mainstream is Uphill: The Challenge of Transferring Knowledge of Crime Prevention Through Replication, Innovation and Anticipation.' In: N. Tilley (ed.) *Analysis for Crime Prevention, Crime Prevention Studies* 13: 131-203. Monsey, N.Y.: Criminal Justice Press/ Devon, UK: Willan Publishing.

Ekblom, P. (2005). 'Designing Products against Crime' in N. Tilley (ed.), *Handbook of Crime Prevention and Community Safety* . Cullompton: Willan.

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 M. Smith and N. Tilley (eds.), *Crime Science: New Approaches to Preventing and Detecting Crime.* Cullompton: Willan.

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

Summary of GUAC Tactics and Strategies

Some of these are further developed in Evolutionary Struggles.

Design Tactics

- During design, consider the *causal mechanisms* 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?

- *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?).

- *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. Designers should perhaps build in the potential for upgrading security if this subsequently becomes necessary.

- 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. 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 (see Evolutionary Struggles below) 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* (e.g. ‘the lock must be able to withstand 20 kg of force and to resist expert picking for 20 minutes’). 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* - e.g. 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 (e.g. ‘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 Criminal Opportunity framework could be developed further to serve this latter purpose [see Conjunction of Criminal Opportunity – Dynamic]

- Learn from the *extinction* of crimes – which ones have fallen into disuse, 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 (subsequently developed by Felson 2006).

- Learn the methods of, and cautiously use the predictions of, sophisticated attempts at *technology foresight.*

- Examine the *legal context* - can laws or the rules of evidence be made more helpful to prevention in particular circumstances - e.g. 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.

- 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.

Other Evolutionary Struggles

Realm	Struggle	Description and possible crime equivalent
The natural world	Prey v predators	(confronters, trappers, dupers), mainly resembling crimes against the person - assault, robbery, homicide
	Plant v herbivore	grazing- taking stored energy and materials from plants, resembling theft
	Host v parasite	parasitism by insects, tapeworms etc - resembling theft
	Host immune system v pathogen	infection by bacteria etc resembling robbery (overcoming host's defences)
	Host immune system v viral pathogen	infection by viruses, resembling fraud or embezzlement in misappropriation of resources for and control of production; computer hacking (breaking access and control codes), and computer viruses themselves
	Natural 'theft or robbery'	within or between species - eg birds taking each others' nest sticks, or robbing others' food in midair attacks
	Natural 'fraud'	birds taking nectar by pecking a hole in the side of the flower to avoid the effort required to pass on pollen, orchids pretending to be female wasps and cheating males of reproductive effort and opportunity.
	Natural 'threat, assault' or killing	conflict over territory, mates, food.
Humanity versus nature	Disease control	hygiene, public health, innoculation, vaccination, antibiotics - resembling prevention of theft/robbery
	Pest control	rats etc spoiling/ stealing crops or livestock, spreading human diseases, acting offensively - resembling prevention of theft /damage, disorder/ nuisance
The human world	Military arms races and (counter) terrorism	arms versus armour, missiles versus electronic countermeasures, manoeuvrability - resembling assault and prevention of assault, homicide, disorder, theft of property, coercion, control of production
	War-games	military training; evolution of new strategies in chess; computer-games of tactics and strategy
	Economic warfare	outgrowing the enemy or disrupting their economy (shading into real crimes like forgery or extortion)
	Hacking	shading into serious computer crime
	Espionage	military/ industrial, to steal information on resources, products, tactics and strategy, shading into theft of information/ obtaining it in preparation for crime