Technology, opportunity, crime and crime prevention – current and evolutionary perspectives

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

DOI 10.1007/978-3-319-27793-6 ISBN 978-3-319-27791-2 ISBN 978-3-319-27793-6 (eBook)

……………………………………….

Paul Ekblom[1]

Professor of Design Against Crime, Design Against Crime Research Centre, Central Saint Martins, University of the Arts London; visiting professor, Department of Security and Crime Science, UCL; visiting professor, Applied Criminology Centre, University of Huddersfield.

p.ekblom@csm.arts.ac.uk +44 7906 434891

Abstract: This chapter seeks to link technology and crime science, including situational crime prevention. It starts by briefly considering the nature of technology. It then looks at the relationship between technology, opportunity, problems and solutions. But opportunity is a more subtle concept than many in the field assume, needing further development for present purposes. It is therefore discussed in relation to both traditional frameworks of crime science and to a more integrated and detailed counterpart, the Conjunction of Criminal Opportunity. But all the opportunity frameworks need supplementing by an account of the dynamics of crime, especially through the concepts of scripts and script clashes. A major section then examines the relationship between crime and technological *change*, covering adaptations and clashes over longer timescales, in the shape of co-evolutionary arms races between offenders and preventers. This spans both biological and cultural evolution. Then come sections on the practicalities of adopting a deliberately evolutionary approach to prevention – gearing up against crime, innovation and design – and finally some weaknesses of purely technological approaches to crime prevention. The conclusion reviews the significance of understanding technology for crime science. This enhanced understanding of how changing technology can both create and block opportunity for crime, nuisance and terrorism (henceforth, crime) is needed to help us anticipate, detect and respond to the many changes in the crime and security world we can expect to encounter during the rest of the 21st Century.

Keywords: Crime, Crime Prevention, Situational Prevention, Problem-Oriented Policing, Technology, Design, Arms races, Criminal adaptation.

Introduction: the nature of technology and technological change

The world of crime science and situational crime prevention (SCP) has often drawn on technology for practical purposes. This will increase as the world in which crime is committed and prevented becomes ever more technologically-based. However, with some notable exceptions, there has been little attempt to explicitly theorise about the role of technology in SCP. This chapter seeks to correct this deficiency – to relate technology to key concepts in SCP, with the aim of giving us a more self-aware and detached view of what technology is, and how it fits with crime science.

[1] I'm grateful to Benoit Leclerc for his helpful editing, Richard Wortley and anonymous reviewers for their inputs to this chapter.

This chapter starts by briefly considering the nature of technology. It then looks at the relationship between technology, opportunity, problems and solutions. But opportunity is a more subtle concept than many in the field assume, needing further development for present purposes. Opportunity is therefore discussed in relation to both traditional frameworks of crime science and to a more integrated and detailed counterpart, the Conjunction of Criminal Opportunity. But all the opportunity frameworks need supplementing by an account of the dynamics of crime, especially through the concepts of scripts and script clashes. A major section then examines the relationship between crime and technological *change*, covering adaptations and clashes over longer timescales, in the shape of co-evolutionary arms races between offenders and preventers. This spans both biological and cultural evolution. Then come sections on the practicalities of adopting a deliberately evolutionary approach to prevention – gearing up against crime, innovation and design – and finally some weaknesses of purely technological approaches to crime prevention. The conclusion reviews the significance of understanding technology for crime science. This enhanced understanding of how changing technology can both create and block opportunity for crime, nuisance and terrorism (henceforth, crime) is needed to help us anticipate, detect and respond to the many changes in the crime and security world we can expect to encounter during the rest of the 21st Century.

Throughout, low-tech and hi-tech, material and cyber technology are covered in parallel. Co-evolutionary processes intertwine the crime and crime prevention sides and introduce significant symmetry, so a proper understanding of the past, present and future role of technology in the security field can only be achieved by considering them together.

The nature of technology

Although technology is a rich and complex aspect of human life, somewhat surprisingly, until recently the field has had few theorists of its own. But Mitcham (1979) identifies four dimensions: *artefact* (tools, manufactured products etc.), *knowledge* (scientific, engineering, technological know-how, plus insight from social and physical sciences), *process* (problem-solving, research and development, invention, innovation), and *volition* (ethics, technology as social construction). Arthur's recent (2009) seminal attempt to provide a theory of technology, characterises it on different scales: as a means to fulfil a particular human purpose; an assemblage of practices and purposes; and the entire collection of devices and engineering practices available to a culture. These levels interact with each other and the entire economy: 'As the collective technology builds, it creates a structure within which decisions and activities and flows of goods and services takes place.' (p194)

For Arthur, technology starts with *phenomena* – natural effects (e.g. gravitation or electricity) that exist independently in nature. Technology is organised around central *principles*, which are the application of one or more phenomena for some purpose; principles in turn are expressed in the form of physical or informational components which are combined, often hierarchically, to meet that purpose. Technological *domains* are toolboxes of potential, which are clustered around some common set of phenomena or applied principles such as movement of mechanical parts, or of electrons.

These frameworks equally apply to technology in the field of *crime and crime prevention*, but need particularisation. Mitcham's volitional dimension for example could include the social institution of crime and the social forces of conflict between individuals, or between individuals and wider social groups like the state. Arthur refers to multiple purposes; extending these to the multiple stakeholders that hold them is especially important in the case of criminal conflicts. As will be seen, these extensions bestow special qualities on technology in crime and its prevention.

A focus on opportunity

Crime science centres on the immediate causes of criminal events and views opportunity in terms of two related perspectives. In the Rational Choice agenda (Cornish and Clarke, 1986), an opportunity emerges when the offender perceives risk and effort as low and reward high. Complementing this psychological approach is the ecological Routine Activities perspective (Cohen and Felson, 1979) of likely offender encountering a suitable target in the absence of capable guardians. At a higher ecological level is the *opportunity structure* (Clarke and Newman 2006) – the entire pattern of available opportunities for crime.

At this level there are obvious affinities with Arthur's 'decisions and activities and flows of goods and services' quoted above. But crime science's familiar theoretical perspectives require some extension and integration to fully and efficiently engage with technology. Here we discuss 'static' aspects of these perspectives; dynamic and change-related aspects are addressed in later sections.

Rational Choice does not cover prevention that works simply by defeating the offender[2] (e.g. with a massive concrete barrier), or completely designing out the crime target (e.g. the disappearance of the vehicle tax disc in the UK in 2014 and its replacement by electronic means of controlling revenue totally obliterated the crime of forging these discs). Here, any choice has to be exercised at a more strategic level ('How else can I make some money?').

Tools and weapons are considered 'crime facilitators', and 'control tools/weapons' appears under 'Increase the effort' in the 25 Techniques of SCP (e.g. Clarke and Eck 2003). However, a direct and explicit theoretical treatment of technology is lacking.

In the 'Hot Products' approach (Clarke 1999) to identification of risk factors for becoming targets of theft, some of these factors are directly-related to technology – in particular Concealable, Removable, Enjoyable and Disposable. (The same applies to protective factors, for example those reducing the risk of theft of cellphones (Whitehead et al. 2008.) Attempts to apply the Hot Products approach in a practical exercise in crime-proofing of new personal electronic items such as cameras and phones (Armitage 2012) revealed difficulties of linking up terms and concepts in technology and crime science (Ekblom and Sidebottom 2008).

Within the core Routine Activities model, the *capability* of guardians is an obvious conceptual peg for *preventive* technology. This applies equally to the other 'crime preventer' roles that were introduced later (Clarke and Eck 2003), namely place managers (e.g. surveillance and access control technology) and handlers of offenders (e.g. electronic tagging used to monitor curfew of convicted offenders). At first sight, however, there is little that explicitly covers technology for *offending*. Cohen and Felson (1979) did originally include offender *capacity* under 'likely' but this has got lost in recent years and unfortunately most writers now refer, too narrowly, to the 'motivated' offender.

The Conjunction of Criminal Opportunity (CCO – Ekblom, 2010, 2011 and https://5isframework.wordpress.com/conjunction-of-criminal-opportunity/ accessed 17 June 2015) remedies some of these limitations. It seeks to integrate the Rational Choice and Routine Activities approaches together with others on both the situational and offender side, and to provide a consistent and all-encompassing conceptual framework and a unified terminology. CCO explicitly includes offenders' resources for committing crime (Ekblom and Tilley 2000; Gill 2005) and can be readily extended to cover resources for the familiar preventer roles discussed above (plus many more with its more flexible role concept, including 'engineer' or 'designer').

In brief, CCO offers twin perspectives: 1) on the proximal *causes* of criminal events; and 2) on *interventions* in those causes to reduce the events' likelihood and/or harm. CCO comprises *agents* (offenders, crime preventers and crime promoters, who inadvertently, carelessly or deliberately make crime more likely or harmful, including those engineers who ignore crime risks); and *entities* (material or human target; target enclosure; wider environment; and the criminal's psychological, social and material resources both for offending, and for avoiding offending). Under CCO, a criminal event happens when an offender who is predisposed, ready and equipped to offend (and lacking the resources to avoid offending) encounters, seeks or creates a situation containing a target that is vulnerable, attractive or provocative, in an enclosure and/or wider environment that is tactically insecure and perhaps motivating in some way, facilitated by the absence of ready and able preventers and perhaps too by the presence of promoters. When these preconditions are met (and perceived to be met) the offender decides to proceed, and acts. When they are blocked, weakened or diverted by a security intervention, or by natural circumstances, the offender either cannot so act; is not provoked or prompted to act (Wortley, 2008); or decides on balance that the perceived reward is not worth the effort and risk.

---

[2] Thanks to Richard Wortley for this point. But it is worth noting that the capabilities technology brings mean that defeat may rarely be absolute. This is illustrated by the jewel thieves who drilled through a metre of concrete to reach the safe deposit boxes of London's Hatton Garden diamond dealers in 2015 – ironically using diamond-tipped cutters.

This ability to map systematically and in detail offers a fuller view of proximal criminogenic mechanisms, and the criminocclusive mechanisms that deliberately block, weaken or divert them (Pawson and Tilley 1997; Ekblom 2011). Although space is lacking here, each of the 11 elements of CCO can be focused on in turn (and perhaps in combination) to examine the diverse roles technology, both material and informational, can play in contributing to the causes of criminal events, and to interventions in these causes. For example, offender presence in an enclosure can be controlled through automated access control (keeping them out) or electronic tagging (keeping them in). Intelligent software can act in a preventer role (e.g. making decisions and acting on suspicious financial transactions) or even, with automated fraud, as an offender.

The explicit incorporation in CCO of resources for offending allows another insight. In SCP, opportunity is typically considered an attribute of the situation. But this is incomplete. An open window three floors up is only an opportunity to an offender with the resources of agility, courage and/or climbing technology such as a ladder. Opportunity is thus an *ecological interaction* between situation and offender.

Additionally, the concept of opportunity makes no sense without specifying 'to do what' – i.e. there must be some *purpose*, which ultimately stems from an agent's predisposition, whether that agent is offender, preventer or promoter. Thus, we can define opportunity as an *ecological concept, relating to how agents encounter, seek or create a set of circumstances in which their resources enable them to cope with the hazards and exploit the possibilities in order to achieve their multiple goals*. The goals of course can be positive (getting the money…) or 'hygiene' related (…whilst avoiding arrest or injury).

Opportunities and problems

Another conceptual element to consider is the relationship between opportunities and *problems*. SCP methods are usually selected, implemented and evaluated through a problem-oriented approach (e.g. Goldstein 1990; Clarke and Eck 2003). But criminals have problems too, and there is a payoff for crime prevention in general, and for discussing technology specifically, from highlighting a symmetry of circumstance between offenders and preventers. With criminal conflict, problems and opportunities are intimately entangled: one party's opportunity will invariably be another's, or the state's, problem.

From a neutral position, *a problem is some set of environmental circumstances that hinders an agent (or agents), equipped with a certain set of resources, from immediately achieving a particular goal or goals.* 'Goals' is usually plural because often the difficulty is in resolving some conflict between positive and hygiene goals – burgle the house *without* getting caught; having tranquil enjoyment of a house *without* expensive and unsightly fortification; tackling a burglary hotspot without restricting pedestrian movement. In this sense, *a problem is what stops achieving an opportunity from being child's play*.

We can visualise the problem-opportunity relationship (Figure 1a-e) as a circle broken by an arc of 'preconditions that need to be met before the opportunity can be realised and the goal achieved'.[3] The arc is of a greater or lesser angle representing how demanding of effort and resources the problem is to solve with an acceptable level of risk of harm, and of failure. If there are several problems we could envisage multiple breaks; and we could represent multiple, conflicting goals as intersecting circles with a common break. Beyond individual instances, we can envisage *fields of opportunity* for crime and its prevention, the initial problem being where to discern a circle of opportunity; this is equivalent to (legitimate) entrepreneurs scanning the field to discern just where they might be able to make some money.

[3] Alternative imagery for problems/solutions includes that of 'glass half-full versus glass half-empty'; for multiple ones Arthur uses chains.

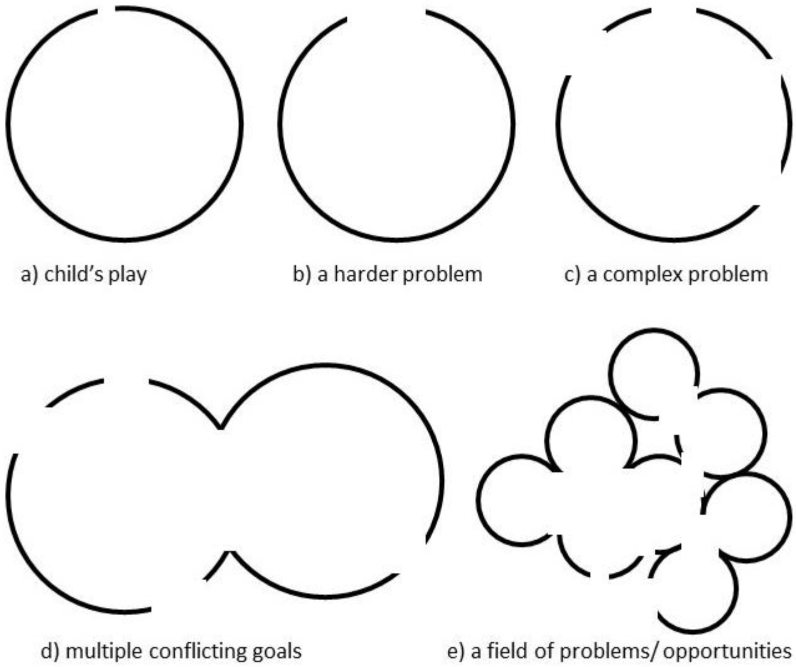

Figure 1. Opportunities and problems

Technology, opportunities and problems

How, then, does technology fit with opportunity, opportunity reduction and problem-solving?

On the opportunity side, the resources and circumstances can obviously include technological elements. But technology can be quite fundamental to defining opportunity. This is partly because it extends human capability to cope and exploit, and partly because (following Arthur 2009), it always has a purpose. Indeed, offenders may have purposes for the technology other than those intended by the engineer/designer – for example misusing or misappropriating it as discussed below.

On the problem side, technology can contribute to solutions by bridging gaps in the circle of opportunity – for example, how to stop car alarms going off as intended (problem for offenders), or inappropriately (problem for car owners and their neighbours). It can even start an entirely fresh circle, opening the doors to new rounds of problem and opportunity – as with the arrival of CCTV – monitoring misbehaviour, or spying on changing rooms. Technology can help either party adapt to contextual conditions necessary for offending or preventive mechanisms to be triggered (Tilley 1993). Besides the social and architectural context these may include the prevailing weather conditions such as sun, rain or snow. Likewise, the weather can cause technology to fail, as anyone whose car alarm has been set off by the wind will attest. Besides prevention, technology can halt a criminal attack that has been launched (for example personal attack alarms or 'smokecloaks' to obscure vision), and *mitigate* the adverse consequences of crime – whether backing up the data on a stolen cellphone, or providing for business continuity after a terrorist attack.[4]

And technology can resolve design contradictions (Ekblom 2012a) or trade-offs between security and, say, safety or profitability. An example is the millimetre-wave airport body scanner that aids security but reduces privacy, where one resolution is the substitution of a *personal* (point-and-laugh) body image on the operator's screen with a *generic*, computer-generated outline that still displays suspicious items. In solving problems, technology thus enables rapid adaptation of the good or the bad party to the challenges posed by its material and social habitat, to the pursuit of its goals. But finding technological solutions that enable opportunities may not always be straightforward. To quote Arthur, 'At one end of the chain is the need or purpose to be fulfilled;

[4] Thanks to Benoit Leclerc for these ideas.

at the other is the base effect that will be harnessed to meet it. Linking the two is the overall solution, the new principle, or concept of the effect used to accomplish that purpose. But getting the principle to work properly raises challenges, and these call for their own means of solution, usually in the form of the systems or assemblies that make the solution possible.' (2009: 110) And one might add that technology can also *obstruct* achievement of purposes when it fails the user, engenders a vulnerability to attack, or is difficult to obtain without extra cost and risk; and sometimes too when the opponent's technology succeeds.

Cyberspace creates a new technological domain for opportunities and problems, but whether recently-emerged crimes *in silico* are merely always reconfigurations of familiar clashes *in vivo*, with certain constraints removed (such as spatial conjunctions, inertia, conservation of mass etc.), or entirely new ones is debatable. Certainly the question of *identity* and *trust* in online transactions have become huge issues. Applying CCO to cyberspace, Collins and Mansell (2004:64) noted that trust fits into the framework in several ways. 'An Internet shopper who is too trusting may act as a careless or negligent crime promoter, as may a system designer. Conversely, being an effective crime preventer means being equipped with appropriate applications and systems. Offenders exploit misplaced trust, sometimes to an expert degree and are aided by software and hardware based resources, for example, "skimming" devices fitted into cash machines to clone cards.'

Taking the broader view, technological extensions of human agents' capabilities, and the technologically-modified situations in which those capabilities are exercised, combine to engender a range of opportunities for crime, and likewise for crime prevention. The combinations range from simple to complex; and from direct routes to indirect, roundabout ones such as the mediating effect of technology on people's routine movements which lead them to crime-generating situations (Brantingham and Brantingham 2008). And there are always knock-on and interaction effects between technologies and with other social and physical circumstances generating unforeseen consequences (e.g. see Tenner 1996).

The dynamics of crime: technology, scripts and script clashes

Criminal events are unlike chemical reactions, where the ingredients are simply brought together and in a single step reliably produce a brightly-coloured precipitate or nasty smell. The coming-together of proximal criminal ingredients may result from influences at levels ranging from the individual offender creating the opportunity – which is not a Routine Activity – to emergent societal influences such as market forces. For its part, Rational *Choice* does not cover the *actions* linking successive decisions. A complete picture of crime as opportunity therefore cannot be developed without incorporating a dynamic view.

Cornish (1994) developed the dynamic dimension with his seminal article on *crime scripts*, boosting understanding of the procedure of crime commission, and promising identification of particular *pinch points* in the script where interventions might be targeted for maximum effect. But scripts can be better woven into the opportunity/problem perspective presented here if they give more explicit attention to goals, plans and resources.

Being instrumental, scripts can be influenced by technology in various ways as problems are solved and opportunities realised. Problems come in hierarchies or clusters – much as goals do in means-end relationships – e.g. a subsidiary problem to breaking into the house could be the lack of a crowbar. Offenders must learn to bypass alarms or pick locks. They must often take extra steps to obtain tools or weapons; perhaps also to learn how they work, how they can be used, or even hacked; and maybe to safely dispose of them or eliminate traces on them such as from DNA or electronic usage data.

The tools themselves can shape or constrain criminal behaviour. Designers refer to 'persuasive technology' (Lockton et al. 2008), and the idea that devices (e.g. cash machines) have scripts 'expected' of their users (Latour 1992). Certainly the properties of knives, locks or network routers influence the kinds of action offenders can contemplate undertaking, and their performance during the event itself. Material items are often misused, sometimes created, as props for con-tricks or ambushes which may involve more or less elaborate scripting. The gay hookup facility Grindr has for example been used to lure victims to robberies.

Applying the procedural dimension to risk factors reveals glossed-over subtleties. For example, the Concealable factor in CRAVED hot products (Clarke 1999) may be criminogenic at the getaway stage when it is the *thief* who pockets the stolen smartphone; but the same factor may *protect* the phone, safely in the owner's pocket or bag, at the target-seeking stage.

The procedural analysis of behaviour applies to preventers as well as offenders, covering all the above considerations. The preventer's script may be quite closely interrelated to the offender's script, for example in collecting money from a cash machine, and stealing or robbing it. Especially significant for technology is the concept of the *script clash* (Ekblom 2012a). This is where the offender's script engages with the preventer's in such issues as:

- Surveill v conceal
- Exclude v permit entry
- Wield force v resist
- Conceal v detect criminal intent
- Challenge suspect v give plausible response
- Surprise/ambush v warning
- Trap v elude
- Pursue v escape
- Foster trust v become suspicious
- Constrain v circumvent[5]

Technology can favour one side over the other, creating an opportunity either for crime, or for prevention, variously relating to targets (e.g. resistant or vulnerable, concealable or detectable), enclosures (hardened or vulnerable, excluding or permitting entry), environments (e.g. illuminated evenly so as to minimise scope for ambush, or with deep shadows) and resources for offending (e.g. tools with ambiguous or clearcut criminal purpose).

Clashes are the fulcrums on which prevention must be designed. The security design task is to arrange the situation to favour preventers over offenders. Discriminant technologies are often crucial – for example the swing-down fire escapes enabling residents to flee a burning building, but hindering offenders from entering; and the 'what you know, what you have and what you are' discriminators in ICT security (respectively, passwords, tokens and biometrics).

Technological change

The original Routine Activities article (Cohen and Felson 1979) theorised how *changes* in the weight/bulk of items like TV sets over several decades made them more suitable as targets for theft. But we can view such changes over greater timescales – indeed Felson and Eckert (2015) argue that technological change is of major importance in understanding longer-term trends in the crime and crime prevention field, illustrating the point with, for example, crime impacts over history of the adoption of horse transport, and the move into towns and cities.

Although early technologies (such as Acheulian stone hand-axes introduced by Homo erectus) endured for hundreds of thousands of years, under Homo sapiens technological change has become the norm. Ogburn (1922), an early historian of technology, saw technological change as the primary driver of social change. In understanding change processes, subsequent debates have occurred over the relative predominance of technological or resource *push* versus market or demand *pull* (see Arthur 2009; and Sten 2014 for a thorough review of the development of thought in this area). The current view seems to be that of a system of mutual influence and feedback loops between supply and demand for technology, albeit with technology taking a significant and often-leading role. Technologically-induced changes diffuse through the wider society at differential rates, leading to cultural *lags* in adjustment (Ogburn 1922). Many commentators (e.g. Arthur 2009)

[5] Thanks to Benoit Leclerc for this clash.

have noted that the rate of technological change has been accelerating, which can only amplify such lags and any negative consequences, e.g. from crime prevention techniques trailing those of crime commission.

Cultural and biological evolutionary perspectives

Accounts of the change process have usually drawn on *evolutionary* themes, and this will be adopted here. The pattern of technological evolution has been variously seen as slow and cumulative (as with Gilfillan's (1935) account of the development of ships through many individual inventions), or operating on a range of saltatory scales. According to Arthur (2009) these range from small 'standard engineering' advances or tweaks, to more radical innovations (such as the leap from steam to electrical propulsion of locomotives) and those that transform whole industries and beyond (such as ICT). The pressures shaping technological evolution variously relate to market forces, networking and both physical and social constraints.

It is self-evident that viewing technological evolution as a subset of cultural evolution can give useful insights. But by combining this with conventional, biological evolution we can go beyond the human and ecological factors than the 'vanilla' version of crime science supplies, gaining insight from fresh concepts and a certain detachment from conventional viewpoints.

Early attempts to draw on biological evolution to understand technology include Samuel Butler's idea of 'Darwin amongst the Machines' (1863) but these resembled superficial analogies (with curious visions of coupling steam engines!). Later attempts have been more penetrating. Biological and cultural evolution have previously been viewed as rivals for explaining human behaviour (e.g. see Roach and Pease 2013), but the scope for fundamental tie-ups between them has increased (e.g. Godfrey-Smith 2012). In fact, 'Universal Darwinism' (Nelson 2007) envisages a common 'evolutionary algorithm' (Dennett 1995) comprising *variation* of individual organisms, practices or products; *selection* on the basis of adaptation to some natural, social or commercial environment; and *replication or transmission* whether through genes, blueprints or imitating/copying the product.

Detailed differences are, however, instructive. For example, Arthur (2009) notes the relative rarity of combinatorial mechanisms in biological evolution (such as the symbiotic coming together of various bacteria and archaea to generate the great leap forward of eukaryotic cells, supporting all advanced life forms). This contrasts with its pervasiveness in technological evolution, where variety is commonly generated by bringing together new assemblages of components or principles: the jet engine, for example, does not result from a gradual modification of piston/propeller engines.

To focus on *biology*, most tools and weapons evolved by animals are simply *grown* as part of their anatomy (e.g. shells) or physiology (venom). But spiders manufacture webs to trap insects, and termites build protective mounds. Technology therefore doesn't require a large brain to create and exploit it, but it does need a research and development process. Humans apart, this is not undertaken by conscious engineers and designers over years but mediated over millennia by the gene-based evolutionary process in countless generations of individuals. Those spiders which, by virtue of their genes, reliably and blindly produce web variants better-adapted to serve their own foraging agenda in the immediate environment (catch prey, avoid being eaten in turn, economise on effort and materials) survive, reproduce and pass those genes on so they come to predominate in the spider population.

Dawkins (1999) refers to the reach of genes to reliably generate structures and behaviours beyond the body of their owner as the 'extended phenotype' (the phenotype being the mature body, the result of protracted interactions between genes and environment during the course of individual development). Humans do have inbuilt tools and weapons – arguably, our *hands.* (Morgan and Carrier (2013) controversially claim that fists have anatomically evolved as a specialised fighting structure.) But with the possible exception of implements for throwing (see below), we have little in the way of fixed phenotypic extensions. The knuckle-duster weapon, for example, is not produced by specific 'build knuckle-duster' genes. Rather, through our generic 'ability to build tool/weapon' and 'understand causality' genes conferring the manipulative rather than pugilistic aspects of our hands, and associated brainpower to operate them purposively.

At the most general level our capacity to support *cultural* evolution, has itself biologically evolved. Whiten and Erdal (2012) ponder the tripling of human brain size in the last 2.5 million years, and explain it in terms of 'the evolution of a new socio-cognitive niche, the principal components of which include forms of cooperation, egalitarianism, mindreading (also known as "theory of mind"), language and cultural transmission, that go far beyond the most comparable phenomena in other primates. This cognitive and behavioural complex allows a human hunter-gatherer band to function as a unique and highly competitive predatory organism.' [2119]

The evolution of technology has been a significant part of this process (although the technological history literature seems to have paid scant attention to the wider cultural evolution material). The anatomy and fine neurological control of the hand, and the construction and use of tools, together constitute a powerful example of *genetic/cultural co-evolution* (Tocheri et al. 2008), a process whereby cultural and biological changes amplify and channel one another. Elsewhere on the body, paleontological and comparative studies (e.g. Roach et al. 2013) suggest that the unique weapon-throwing capacity of humans involved feedback between changes to arm, shoulder and back anatomy and the development of projectiles, a process which may have begun with Homo erectus some 2 million years ago.

From a broader perspective Godfrey-Smith (2012) identifies macro-level, 'cultural phylogenetic changes' such as the Neolithic Revolution's shift from hunting/gathering to farming. These are comparable to Arthur's (2009) suggestion that major, transformative leaps in technological ability occur when we switch to a new domain, e.g. from mechanical to cyber. The cultural/technological evolution of farming introduced a phase-change in human existence. It increased population density, led to ownership of fixed parcels of land and other property, plus the development of written recording of that ownership; fostered emergence of hierarchies; and enabled the development of societal roles with specialist skills unrelated to subsistence. In turn, these ultimately technologically-induced changes together with a cascade of others including the invention of mass transportation, can be said to have drastically and progressively reshaped the routine activities of society (Cohen and Felson 1979; Felson and Eckert 2015); the places the activities occur in and the journeys between them (Brantingham and Brantingham 2008); and the nature and supply of targets, tools and weapons. Such changes have generated both readiness to offend (for example via more sources of conflict), and made possible many more criminal opportunities leading to more frequent, and more diverse, criminal events. And major phase changes continue to unfold – we are in the midst of those stemming from the emergence of ICT, bioengineering and climate change.

Farming, fire, and the axe, in enabling forest clearance in favour of grassland, illustrate a further evolutionary concept: *niche construction*. This fundamental, but only recently recognised process (Laland et al., 2009), is where a given species pervasively shapes its own environment to its own advantage and simultaneously adapts to survive within it, as with corals building entire reefs out of their limestone skeletons. We humans have come to constitute and determine our own environment in both social and technological terms, for better and for worse.

Biological lag

To Ogburn's cultural lag, we may add *biological* lag. Evolutionary psychology (e.g. see Roach and Pease 2013; Ekblom et al. 2015) explores the possibility that human genes, including those influencing our perceptions and behaviour, remain adapted to life in the Pleistocene epoch (which ended some 11000 years BP), when we were hunter-gatherers living in small mobile bands with limited weapons and tools. The remarkable human capacity for cooperation described above evolved in this period, creating the backdrop against which crime must be understood. But unfortunately we are also pretty accomplished at conflict between individuals, and between groups; and in inventing, using and improving tools and weapons in both cooperation and conflict. Behavioural tendencies appropriate for the Pleistocene circumstances – where time, space, materials and local population size provided natural constraints on conflict, differential wealth, things to steal and violence – are now inappropriate where weapons of easy, stand-off killing and mass destruction are available together with a cornucopia of portable high-value goods. Inappropriate, too, when we are enclosed in vehicles where lack of natural empathic signals between conflicting individuals can perhaps unleash road rage. Cultural evolution has largely been able to compensate for inadequate psychological/ecological controls, including through the development of social controls relating to reputation; and societal institutions such as law, criminalisation and enforcement. But because these remain imperfect, direct interventions to improve security remain necessary (Schneier 2012).

Technology, disruption, co-evolution and arms races

Thwarted commercial burglars can simply return to attack a fence with a more powerful bolt-cutter – an example of tactical displacement. But the offensive or defensive tools themselves may change, and the balance of technological advantage between offenders and preventers alters over time. Technological historians have long identified perturbations and disruptions of a more general nature (Ogburn 1922; Christensen and Raynor 2003). Disruptive trends like automation, remote monitoring and operation, self-design and production, mass customisation, miniaturisation, portability including power supply, and the break between appearance and functionality, will all keep perturbing the balance between offenders and preventers.

Change can be exogenous (driven by external forces like the arrival of the motor vehicle, acting as crime resource and target par excellence, or police patrol car); endogenous, by the playing out of script clashes involving the adaptation and counter-adaptation of criminals and preventers to one another's tools, techniques and weapons; or more usually, a combination in which exogenous changes perturb the endogenous ones. However, the nature of that perturbation, and the interactions between different perturbations, can only be resolved at the level of the fine detail of particularities and perhaps only in retrospect. An example is the digital TV set-top box, intended to allow existing analogue TV sets to receive digital stations. A compact (and for a few years, widely-available) object initially costing around £100, we might have expected the box to become a hot product – until the TV service providers decided to subsidise the cost and instead make their money from the service charge.

Co-evolutionary struggles

In the short term one can imagine the mutual adaptation of conflicting scripts – the first bicycle-parking script might have been 'cycle to cake shop, leave bike outside, buy cake, return, mount bike and pedal off'; the first bike theft script 'see unattended bike, get on and pedal off'. Soon these would be followed by various elaborations such as 'lock bike', 'break bike lock' etc. In the medium term come 'crime harvests' Pease (2001), in which some product, say the mobile phone, is designed and developed in a way that is naïvely vulnerable to crime and attractive to offenders (a failure to 'think thief' – Ekblom 1997). Soon after coming on the market it becomes both a popular purchase and a popular steal. This is usually followed by desperate commercial or governmental measures to retrofit security which often result in clunky, user-unfriendly or unreliable products.

In the longer term, such adaptations and counteradaptations can extend into prolonged co-evolutionary struggles (Ekblom 1999; Sagarin and Taylor 2008). These are also known as arms races or 'Red Queen's games', where you have to keep running merely to stay in the same place (from *Alice Through the Looking Glass* – see van Valen 1973, and Dawkins and Krebs 1979). Classic examples are the evolution of the safe (Shover 1996), coins and banknotes, and more recent means of payment such as online purchases. Once started, arms races may unfold at an irregular pace (perhaps resembling the biological 'punctuated equilibrium' of Gould and Eldredge (1972)). At any point in such a criminal co-evolutionary sequence, we may encounter further harvests in the form of breakouts or 'evolutionary surprise attacks' (Tooby and DeVore 1987), where a new tactic, tool or weapon becomes available or is invented out of the blue and, for a while at least, overwhelms the opposition's defences. Imagine, for example, the devastating effect on cyber security if someone discovered how to predict/identify the very large prime numbers relied on in most security protocols.

Historical changes, and co-evolution especially, mean that knowledge of what works, including technological solutions to crime problems, is a wasting asset that needs continual replenishment by new sources of variety. A contemporary example here is what happens when the automotive industry rests on its laurels. A convincing case can be made (see Chapter by Farrell and Tilley) that the 'security hypothesis' – sustained technological and procedural improvements in the security of homes, vehicles, shops etc. – accounts for the striking crime drop seen over the last two decades. A significant contributor to these improvements has been the inclusion (e.g. mandated by EU Directive) of immobilisers in vehicles; Brown (2013) thoroughly reviews the evidence. Recently, however, and as Brown anticipated, car thieves have managed to circumvent the security of keyless top-end models such as the Land Rover Evoque (www.bbc.co.uk/news/technology-29786320 accessed 20 February 2015). These are currently disappearing into shipping containers and heading abroad so fast that insurers are declining cover unless, say, cars are parked off-street and primitive security devices like add-on steering wheel locks fitted. A similar reversion to past technology is evidenced (www.theguardian.com/world/2013/jul/11/russia-reverts-paper-nsa-leaks accessed 20 February 2015) by the

Russian Federal Guard Service. Following the Snowden affair, they have purchased old-fashioned typewriters in order to deter leaks, by the traceability of individual machines' key imprints. In asymmetrical warfare, insurgents sometimes gain advantage by reversion to old-fashioned weapons or means of communication.

Accelerants

Co-evolution through conflict, as just described, constitutes a powerful accelerant of technological change in both criminal and military arenas since the two opposing sides focus sharply, consistently and persistently on countering one another's resources and capabilities. But co-evolution unfolds against a background of further accelerants. Ogburn (1922) and later technological historians (see Sten 2014) have identified factors including increased population size enabling more people to invent things; a greater stock of pre-existing technologies to combine; and communications media enabling recording and dissemination of inventions and techniques (including lock-picking sites on the Internet (Ekblom 2014b), and capitalistic competition. Arthur (2009) additionally sees a qualitative change, with the human economy becoming increasingly generative – shifting from optimising fixed operations, towards creating new and flexible combinations and offerings for the market.

The last relates to the biological concept of the *evolution of evolvability* (Dawkins, 2003). This refers to the fact that some organisms evolve sets of body-plan genes that facilitate the orderly and efficient generation of variety. Moreover this is not just random variety, where the chances are that such a spanner dropped into the works of a complex machine would be more likely to harm than help, but *plausible* variants (Kirschner and Gerhart 2005) with a good chance of survival and possibly of conferring benefit.

The same process can be seen with cultural and especially technological evolution, and in fact we can see processes of combination, co-evolution, modularity and evolution of evolvability coming together. In crime, facilities like *script kiddies* enable less-accomplished programmers to generate computer viruses. *3D printers*, originally design prototyping tools, have been used to boost criminals' own capacity in, say, manufacturing accurately-fitting and realistic-looking scanning mouthpieces for ATMs to read/transmit customers' card details; and in rapidly updating the shapes as soon as the bank security team modify the ATM front panel (Krebs 2011). This aspect is more significant than the printers' claimed ability to produce working firearms (e.g. www.wired.com/2014/11/atlas-314-3-d-printed-guns-bullets/ accessed 3 March 2015). 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 accessed 3 March 2015). One imagines this will interest terrorists and other criminals.

Gearing up against crime

In the face of co-evolution, accelerants, and the background of dramatic changes in technologies and their applications, the appropriate strategic response for professional preventers is to try to *out-innovate* adaptive offenders. Anything less risks winning battles, but losing campaigns. 'Gearing up against crime' approaches (Ekblom 1997) suggest ways of doing this. Some are lessons transferred from a range of other evolutionary struggles such as arms races in the military domain, human versus nature (e.g. antibiotics versus resistant bacteria, pests versus pesticides) or the purely natural (e.g. predator versus prey, immune system versus pathogens) (Sagarin et al. 2008). Practically speaking, running arms races (more fully covered in Ekblom 1997, 1999, 2015 and below on innovation) involves generating plausible variety of responses by relying on theory and interchangeable practical elements; building in the capacity for security upgrades, especially 'broadcastable' ones as with Windows security patches; and developing security 'pipelines', as with bank cards and satellite TV decoders, such that as soon as offenders crack one, a new one is slotted into place.

It is prudent to establish systems for spotting and quickly reacting to new technologically-enabled or targeted crime. But given the lead time to develop security functionality, *anticipation* plays an important role in prevention. The traditional anticipatory method of the problem-oriented approach to crime prevention – induction of risk and protective factors from past patterns of hotspots etc. – has been applied to 'hot products' (those whose design and exposure render them at greatest risk of theft: Clarke 1999; Armitage 2012). But this struggles with nonlinear changes in technology. However, alternative, foresight- or horizon-scanning-based approaches are applicable: see, for example the UK Government's Foresight Programme activities covering crime in general (DTI 2000) and cybercrime (www.gov.uk/government/publications/cyber-trust-and-crime-prevention accessed 3 March 2015). Technology roadmapping, which seeks to connect future requirements with upcoming trends in technology (e.g. www.technology-roadmaps.co.uk/secure_environment/ accessed 3 March 2015), could be applied to both crime prevention and the misuse of emerging technologies and technological combinations by offenders.

Horizon-scanning can be rendered more systematic and rigorous by various crime science approaches. On causes, the Routine Activities perspective can be used to identify changes in any of its three causal components that might make crime events more likely (Pease 1997). The CCO can prompt more detailed questions along similar lines (Ekblom 2002): what future technological changes might affect offender presence, target vulnerability, offender resources etc.? We might also ask what changes might tip the balance of particular script clashes. On risk and protective factors, a generic approach – the Misdeeds and Security framework (Ekblom 2005) – asks how scientific and technological innovations might generate opportunities for crime through:

- Misappropriation (theft)
- Mistreatment (damage or injury)
- Mishandling (e.g. smuggling, data transfer)
- Misrepresentation (fraud)[6]
- Misbegetting (counterfeit)
- Misuse (as tool or weapon)
- Misbehaviour (for spraying graffiti for example)
- Mistakes (e.g. false alarms)

More specific risk factors for, say, misappropriation of *products* can be developed, as with CRAVED (Clarke 1999). In turn, we can link these factors to generic anticipated trends in technology, including greater miniaturisation and less use of energy, to spot upcoming criminogenic changes.

Equivalent protective factors/opportunities for prevention are:

- Secured against Misappropriation, e.g. vehicles with built-in immobilisers
- Safeguarded against Mistreatment, e.g. street signs that avoid couching regulations in provocative, confrontational terms
- Scam-proofed against Mishandling, Misbegetting and Misrepresentation, e.g. fold-over airline baggage labels concealing holidaymakers' addresses from burglars' touts; or anti-copying functions within DVDs
- Shielded against Misuse, e.g. one-time syringes
- 'Sivilised' against Misbehaviour, e.g. metro station seating shaped to discourage rough sleeping

These factors can be used descriptively; or as a technology requirement specification e.g. by the police (Ekblom 2005) intended to encourage the development of the appropriate preventive capabilities. This last is an instance of market pull rather than technology push.

Technology, innovation and design

Arthur (2009), building on Ogburn (1922), emphasises the importance of *combination* of prior, especially modular, elements of technology in generating new products. With crime prevention, systematically generating plausible variety at the level of *principles* derives from the use of tested theory and what-works evidence (Ekblom and Pease 2014). This is the case whether that theory and research relates to technological or social domains (e.g. how to make wall-penetrating surveillance *work*, and how to *use* it with what effect on offenders). That theory must be in a suitably analytic, integrated and accessible state to generate variety at a sufficient pace to out-innovate adaptive offenders against the backdrop of social and technological change, as noted. Arguably, CCO fits this requirement, being a suite of generative, analytic principles for preventive intervention, which channel more or less complex mechanisms through practical intervention methods. (In this, in itself it resembles Arthur's (2009) account of a domain of technology.) Innovation in prevention can also draw on recombination of modular *practice* elements (e.g. how to mobilise people as preventers) (Ekblom 2011).

[6] Thanks to Benoit Leclerc for Misrepresentation, and Ken Pease for Misbegetting.

However, concepts can only be realised by people. We need professional designers closely working with practice-experts and users for the theory and practical know-how to come together to generate intervention measures that both work in principle and are workable in practice; and moreover which meet a range of other requirements such as cost, aesthetics, durability, a small carbon footprint, business continuity and public safety. This takes design beyond the pure homespun practicality of the police and hard-edged engineers. Recent reviews of design and crime are in Ekblom 2012a, 2014b, and see also www.designagainstcrime.com and www.designingoutcrime.com/.

The design process needs hefty doses of intuition, inspiration and creativity, helped by developing a 'think criminal' mindset, and always being alert to the need to 'reframe' the presenting problem (Lulham et al. 2012). But it must also be systematic, constrained and supported by theoretical and methodological discipline. The use of frameworks like CCO, scripts etc. as discussed, and the more specific situational perspectives behind them, can contribute to this. One approach to feeding crime science into design is the Security Function Framework (Ekblom 2012b; Meyer and Ekblom 2011) for specifying criminocclusive products, i.e. those that reduce the possibility, probability and harm from criminal events. This framework seeks to develop a rationale for secure designs in terms of

- Purpose (what/who are the designs for, i.e. to reduce what crimes, and serve what other goals, for which stakeholders?)
- Niche (how do they fit within the security ecosystem? Inherently *secure* products, dedicated *security* products, or *securing* products which confer protection as a side-benefit to some main function like being a handbag)
- Mechanism (how do they *work*, causally, to serve security and other goals?)
- Technicality (how are they constructed, of what materials, and how are they operated?)

A counterpart framework could be developed for criminals' tools and weapons. Clarke and Newman (2006) have developed the acronym MURDEROUS to describe weapons of choice for terrorists: Multipurpose, Undetectable, Removable, Destructive, Enjoyable, Reliable, Obtainable, Uncomplicated and Safe.

A final approach in the engineering innovation context is TRIZ, the theory of inventive principles (Ekblom 2012a; www.triz-journal.com/ accessed 3 March 2015). In brief, TRIZ facilitates the engineering design process by bulk scrutiny of past inventions and inventive trends. The TRIZ approach has developed a generic set of 40 *inventive principles*, abstracted widely across vast numbers of patents; 39 recurrent *contradiction principles* that routinely face designers seeking to meet conflicting user requirements, or technical tradeoffs such as strength versus weight. Contradictions and tradeoffs are inherent in crime prevention: there is the central contradiction between 'offender wants the item' versus 'owner wants the item'; and in practice there are specific script clashes, as previously described. There are also contradictions *within* security, such as 'higher fence keeps intruders out' versus 'blocks natural surveillance'; and 'lighting means more security but greater carbon footprint' (cf. Armitage and Monchuk 2009). Each contradiction constitutes a *problem* as previously defined, in terms of an obstacle to someone's achievement of their goals. A central procedure within TRIZ is to identify two principles in conflict, then look up to see what inventive principles were previously used to resolve that contradiction. New technology has always been at the forefront of such resolutions – for example, the arrival of the internal combustion engine relaxing the strength/weight trade-off, so the military tank simultaneously has both armour *and* manoeuvrability, unlike its predecessors the armed knight and the cavalryman, who had one *or* the other.

A final aspect of TRIZ worth mentioning is its identification of a range of *evolutionary trends* in various technological fields (e.g. a trend from fixed links between components, to hinged links, to infinitely variable links like bicycle chains, to electromagnetic fields). Knowing such trends can help us anticipate where the next improvement in some product, process or system might be expected to come from, whether introduced by legitimate engineers or criminal ones. In this respect, TRIZ provides yet another, more technologically particular, evolutionary perspective to those already described.

Beyond the technical side of innovation, designers and those that employ them must consider the business dimension of market forces in spurring development of products and getting them sold. Space precludes further discussion but it is worth briefly noting that *opportunity* relating not to criminal conflict but commercial competition (e.g. Trott 2005; McElwee and Smith 2015), raises interesting theoretical and practical issues. And Arthur (2009) considers demand too limited a concept to depict processes at the level of the economy, preferring to refer to 'opportunity niches' (e.g. p174). There was no specific demand for penicillin, for example, until it was discovered, but there was a broader need for something to be done about bacterial infection. Working this concept into crime science may prove rewarding.

Weaknesses of technology

Technology has its drawbacks for crime prevention as much as in any other domain of application. Solution- or supply-driven approaches to problems can canalise responses, constraining both current interventions and future adaptability. The rush into public-space CCTV surveillance, despite indications of restricted utility (Welsh and Farrington 2008) reflects this. Investment in technology of the rigid, capital-intensive kind can hinder adaptation to changes and enhance the lag behind adaptive criminals – a case of 'field obsolescence'. Techno-fixes can be superficial, of the 'bolt-on, drop-off' kind. However well-designed and constructed, they can also fail at the interface with humans if that part of the preventive system is inadequately integrated or updated. One example is the Grippa Clip (Ekblom et al. 2012), a carefully-designed and-trialled clip for preventing theft of customers' bags by anchoring them to pub/café tables. Despite plaudits from customers, police and bar staff, and successful utilisation by customers in bars in Barcelona and a café at a London station, in one UK bar chain they were ignored. Indications were that utilisation depended on the crime climate (serious enough in Barcelona for bar staff to not be shy about alerting customers to these security aids), and on staff motivation and commitment (in the UK bars this seemed lacking, but was firmly present in the London café, which 'nurtured' its personnel and established mutual commitment with the company).

Technology can make things worse, with false burglar or car alarms wasting police time and annoying neighbours. It can also be self-defeating: clunky password-based security systems overload the memory and exceed an employee's 'compliance budget' (Beautement et al. 2008) – that proportion of their work time and effort they are willing to dedicate to security procedures (beyond which they cut corners, like writing passwords down).

But none of these failings are inherent limitations of technology – only technology that is over-relied upon in isolation from human/system considerations; poorly designed (e.g. to be abuser-unfriendly without being simultaneously user-friendly; and note the DAPPER acronym in Tilley and Farrell's chapter in this volume); rigid and constraining in the face of the messy complexity of real life; and incapable of being adapted to changing patterns of risk during its lifetime of use, through material or software upgrades (Ekblom 1997).

A broader issue is complexity. Arms races, human system failures etc. show that technology is often embedded in *complex adaptive systems*, where introducing change at one point is followed by the various agents adjusting to the change, and to each other's new stance (a theme inaugurated by Ogburn 1922). Add to this the complexity of interactions between technologies (think how many technologies came, or were brought, together to enable the attack on the Twin Towers) and we can see how unpredictable the crime (or crime prevention) impact of individual technological developments can be. Crime prevention faces a rich and challenging future in which *sense-making* rather than watertight, orderly explanation and prediction may well play a greater part in practice, as it is doing in the economy as a whole (Arthur 2009).

Conclusion

Technology forms a pervasive and routine part of the human ecosystem, and constitutes the means of individuals and groups to extend their native capabilities to adapt to and exploit that ecosystem, whether for legitimate or illegitimate purposes. It is not an optional bolt-on component to crime science, but is fundamental to concepts of opportunities, problems and solutions.

Technology both creates and solves problems for offenders and crime preventers, and – as the other side of the coin – helps to block or generate opportunities for these parties. It plays many causal roles in the clashing scripts of offenders and preventers: in the language of CCO it can produce or modify targets, enclosures and wider built environments; enable or restrict presence in the crime situation; and supply resources for offending, avoiding offending and preventing offending. All of these apply to both material and cybercrime, and to both hi-tech and low-tech products and systems. Since every criminal or preventive action has a potential technological dimension, those seeking to understand and intervene in crime must be technically aware. Since it is so varied – and variable – crime scientists must understand technology's fundamental nature, as shown e.g. by Arthur, and be able to grasp the specifics of technologies in particular crime situations, scripts and script clashes, both functionally and …technically.

One underlying theme of this chapter has been the symmetry between problems and solutions facing offenders, and the solutions and problems facing preventers. But the point having being made, it may be worth exploring what asymmetries remain, and their significance for prevention. To a certain degree, professional developers of preventive technologies work in an *intensive* way, with considerable investment and application of know-how, time and other resources in coming up with solutions. This may also happen with organised or networked crime and terrorism, but in many cases the development process may be *extensive*, with thousands of offenders 'trying it on' in modest ways to develop ways to circumvent particular locks, or surveillance cameras, or find loopholes in financial systems. The extensive process resembles all those bacteria mutating away in their billions, with a few coming up with just the right change in their metabolic repertoire to overcome the latest antibiotic.

Technologies interact with one another and with social and environmental contexts, generating challenging levels of complexity and unpredictability. And technology evolves, under the drivers and constraints of market forces, societal requirements, the material laws of physics and chemistry, the logical rules and conventions of ICT, the ingenuity and innovativeness of engineers and designers, a never-ending succession of technologically-induced opportunities and problems and in some cases, the co-evolutionary arms race between offenders and preventers. This evolution unfolds in biological, cultural and specifically technological domains. (Interestingly, Arthur (2009) points out how technology itself is developing ever increasing resemblance to biology in its complexity, adaptability and integration/ communication between parts.)

For the foreseeable future, technology will be a significant influence in both generating and reducing crime. However, successful crime prevention through technology cannot be based on some narrow and linear technological determinism but must be undertaken through the understanding of and influence upon complex social/ physical/ informational systems. The design of technology must thread its way between diverse requirements and in particular to intelligently discriminate in favour of rightful owners/users over criminal abusers and misusers. While a purely technological approach to crime prevention has notable weaknesses and limitations, technology that is carefully designed in line with the tested theories of crime science, developed, updateable and updated on an appropriate timescale, and that is well-integrated with the human parts of a security system, can make a significant contribution to the well-being of individuals, organisations and society.

But criminals are forever seeking opportunities to misappropriate, mistreat, misuse and misbehave with technology as they adapt to the changing socio-technological environment, attempting to cope with its hazards and exploit its vulnerabilities. The Red Queen's game will doubtless continue to run throughout the remainder of the 21st century and beyond. Only strategic, evolutionary and innovative thinking based on plausible theory and empirical research and development can stop the nice guys finishing last. But it seems (www.bbc.co.uk/news/technology-31416838 accessed 5 March 2015) they will have to contend with 3D-printed knuckledusters!

References

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

Armitage, R. & Monchuk, L. (2009). Reconciling security with sustainability: the challenge for eco-homes. Built Environment, 35(3), 308—327.

Arthur, W. B. (2009). The Nature of Technology. What it is and How it Evolves. London: Allen Lane.

Beautement, A., Sasse, M. A., Wonham, M. (2008.) The compliance budget: managing security behaviour in organisations. In NSPW'08: Proceedings of the 2008 workshop on new security paradigms workshop (pp. 47—58). Association for Computing Machinery.

Brantingham, P. & P. Brantingham (2008). Crime Pattern Theory. In R. Wortley and L. Mazerolle (Eds.) Environmental Criminology and Crime Analysis. Cullompton: Willan.

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

Butler, S. (1863). To the Editor of The Press, Christchurch, New Zealand, 13 June. Wellington: Victoria University.

Christensen, C. & Raynor, M. (2003). The innovator's solution. Harvard: Harvard Business Press.

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

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. (2006). Outsmarting the Terrorists. London: Praeger Security International.

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

Collins, B. & Mansell, R. (2004). Cyber Trust and Crime Prevention: A Synthesis of the State-of-the-Art Science Reviews. London: Department for Business, Innovation and Science. www.foresight.gov.uk/Cyber/Synthesis of the science reviews.pdf accessed 21 January 2015.

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

Cornish, D. & Clarke, R. (Eds.) (1986). The Reasoning Criminal: Rational Choice Perspectives on Offending. New York: Springer-Verlag.

Dawkins, R. (1999). The Extended Phenotype. Oxford: Oxford University Press.

Dawkins, R. (2003). The evolution of evolvability. In S. Kumar and P. Bentley (Eds.), On Growth, Form and Computers. London: Academic Press.

Dawkins, R. & Krebs, J. (1979). 'Arms races between and within species. Proceedings of the Royal society of London B 205 (1161): 489—511. doi:10.1098/rspb.1979.0081

Dennett, D. (1995). Darwin's Dangerous Idea. London: Penguin.

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.

Ekblom, P. (1999.) Can we make crime prevention adaptive by learning from other evolutionary struggles?' Studies on Crime and Crime Prevention, 8, 27—51.

Ekblom, P. (2002). Future imperfect: preparing for the crimes to come. Criminal Justice Matters, 46, 38—40. London: Centre for Crime and Justice Studies, Kings College.

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.

Ekblom. P. (2010). The Conjunction of Criminal Opportunity theory. Sage Encyclopedia of Victimology and Crime Prevention, Vol 1, 139—146.

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 G. Farrell and N. Tilley (Eds.) The Reasoning Criminologist: Essays in Honour of Ronald V. Clarke (pp.163–198). Crime Science series. Cullompton: Willan.

Ekblom, P. (Ed.) (2012b). Design Against Crime: Crime Proofing Everyday Objects. Crime Prevention Studies 27. Boulder, Col.: Lynne Rienner.

Ekblom, P. (2014a). Crime and communication technology. In W. Donsbach (Ed.) The International Encyclopedia of Communication. Oxford: Blackwell Publishing.

Ekblom, P. (2014b). Designing products against crime. In G. Bruinsma, and D. Weisburd (Eds.), Encyclopedia of Criminology and Criminal Justice. New York: Springer Science+Business Media.

Ekblom, P. (2015). Terrorism – lessons from natural and human co-evolutionary arms races. In M. Taylor, J. Roach and K. Pease (Eds.), Evolutionary Psychology and Terrorism. London: Routledge.

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

Ekblom, P. and Sidebottom, A. (2008). What do you mean, 'Is it secure?' Redesigning language to be fit for the task of assessing the security of domestic and personal electronic goods. European Journal on Criminal Policy and Research, 14, 61—87.

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

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

Ekblom, P., Sidebottom, A. and Wortley, R. (2015). Evolutionary psychological influences on the contemporary causes of terrorist events. In M. Taylor, J. Roach and K. Pease (Eds.), Evolutionary Psychology and Terrorism. London: Routledge.

Eldredge, N. & Gould, S. (1972). Punctuated equilibria: an alternative to phyletic gradualism. in T. Schopf (Ed.), Models in Paleobiology. San Francisco: Freeman Cooper.

Felson, M. & Eckert, M. (2015). Crime and Everyday Life (5th edition). London: Sage.

Gibson, J. J. (1950). The perception of the visual world. Boston, MA: Houghton Mifflin.

Gilfillan, S. (1935). Inventing the Ship. Chicago: Follett.

Gill, M. (2005). Reducing the capacity to offend: restricting resources for offending. In N. Tilley (Ed.), Handbook of Crime Prevention and Community Safety. Cullompton: Willan.

Godfrey-Smith, P. (2012). Darwinism and cultural change. Philosophical Transactions of the Royal Society B, 367, 2160—2170.

Goldstein, H. (1990). Problem-Oriented Policing. Philadelphia: Temple University Press.

Kirschner, M. and Gerhart, J. (2005). The Plausibility of Life: Resolving Darwin's Dilemma. New Haven, CT: Yale University Press.

Krebs, B. (2011). http://krebsonsecurity.com/2011/09/gang-used-3d-printers-for-atm-skimmers/ Accessed 22 January 2015.

Laland, K., Odling-Smee, J., Feldman, M., Kendal, J. (2009). Conceptual barriers to progress within evolutionary biology. Foundations of Science 14(3) 195—216.

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In W. Beijker and J. Law (Eds.), Shaping Technology, 205—224. Cambridge, MA, MIT Press.

Lockton, D., Harrison, D., Stanton, N. (2008). Design with intent: persuasive technology in a wider context. In H. Oinas-Kukkonen, P. Hasle, M. Harjumaa, K. Segerståhl, P. Øhrstrøm (Eds.) Persuasive Technology: Third

International Conference, PERSUASIVE 2008, Oulu, Finland, June 4-6, 2008, Proceedings. Series: Lecture Notes in Computer Science, 5033. Berlin: Springer.

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

McElwee, G. & Smith, R. (Eds.) (2015). Exploring Criminal and Illegal Enterprise: New Perspectives on Research, Policy & Practice. London: Emerald Group.

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

Mitcham, C. (1979). Philosophy and the history of technology. In G. Bugliarello (Ed.), The History and Philosophy of Technology, University of Illinois Press, Champaign-Urbana, Illinois, 163—189.

Morgan, M. & Carrier, D. (2013). Protective buttressing of the human fist and the evolution of hominin hands. Journal of Experimental Biology 216, 236—244.

Nelson, R. (2007). Universal Darwinism and evolutionary social science. Biology and Philosophy 22, 73—94.

Ogburn, W. (1922). Social Change With Respect to Culture and Original Nature. New York: B.W. Huebsch Inc.

Pease, K. (1997). Predicting the future: the roles of routine activity and rational choice theory. In G. Newman, R. V. Clarke and S. Shoham (Eds.), Rational choice and situational crime prevention: Theoretical foundations. Aldershot, UK: Dartmouth Press.

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

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

Roach, J. & Pease, K. (2013). Evolution and Crime. London: Routledge.

Roach, N., Venkadesan, M., Rainbow, M., Lieberman, D. (2013). Elastic energy storage in the shoulder and the evolution of high-speed throwing in Homo. Nature, 498, 483—486.

Sagarin, R. & Taylor, T. (Eds.) (2008). Natural Security: A Darwinian Approach to a Dangerous World. Berkeley: University of California Press.

Schneier, B. (2012). Liars and Outliers: Enabling the Trust that Society needs to Thrive. New York: Wiley.

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

Sten, K. (2014). The Emerging Dynamics of Innovation: The case of IT Industry in India. Master's thesis, Copenhagen Business School. http://studenttheses.cbs.dk/bitstream/handle/10417/4797/katri_sten.pdf?sequence=1 Retrieved 25 March 2015.

Taylor, M. & Currie, P. (2012). (Eds.) Terrorism and Affordance. London: Continuum.

Tenner, E. (1996). Why Things Bite Back: Technology and the Revenge of Unintended Consequences. New York: Alfred A. Knopf.

Tilley, N. (1993). Understanding Car Parks, Crime and CCTV: Evaluation Lessons from Safer Cities. Crime Prevention Unit Paper 42. London: Home Office.

Tocheri, M., Orr, C., Jacofsky, M., Marzke, M. (2008). The evolutionary history of the hominin hand since the last common ancestor of Pan and Homo. Journal of Anatomy, 212(4), 544—562.

Tooby, J. & DeVore, I. (1987). The reconstruction of hominid behavioral evolution through strategic modelling, in W. Kinzey (Ed.) The Evolution of Human Behavior: Primate Models, 183—227. New York: SUNY Press.

Trott, P. (2005). Innovation Management and New Product Development, 2005. Upper Saddle River NJ: Prentice Hall.

van Valen, L. (1973). A new evolutionary law. Evolutionary Theory 1, 1—30.

Welsh, B. & Farrington, D. (2008). Effects of closed circuit television surveillance on crime. A systematic review. Oslo: Campbell Collaboration.

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

Whiten, A. and Erdal, D. (2012). The human socio-cognitive niche and its evolutionary origins. Philosophical Transactions of the Royal Society B 367, 2119—29.

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