Crime, situational prevention and technology – the nature of opportunity and how it evolves

Paul Ekblom[1]

Ekblom, P. (2017). 'Crime, situational prevention and technology – the nature of opportunity and how it evolves'. In M. McGuire and T. Holt (eds) *The Routledge Handbook of Technology, Crime and Justice.* Milton Park: Routledge, 353-374.

Introduction: the nature of technology and technological change

Situational crime prevention (SCP) takes offenders' motivation for granted – there will always be people with criminal intent. Instead, it seeks to limit their scope for offending (e.g. a brick wall too high to climb), and to influence their perceptions and decisions regarding criminal action. Since prehistory situational methods have drawn on technology for practical purposes, whether against fellow humans raiding hill forts or treasure chests, or mice, grain stores. This trend can only increase as the world in which crime is committed and prevented becomes ever more technologically-based. However, few have attempted to theorise about the role of technology in SCP.

This chapter seeks to fill this gap – to understand what is meant by technology and to relate it to key concepts in SCP. It first considers the nature of technology. It then examines how technology relates to opportunity, problems and solutions. But these concepts themselves needs more development. The chapter therefore covers both traditional frameworks of SCP and a more integrated and detailed counterpart, the Conjunction of Criminal Opportunity. And 'static' opportunity needs extending to address crime dynamics, especially through the concept of scripts. A major section then examines the relationship between crime and technological change, covering adaptations and conflicts over longer timescales, viewed as arms races between offenders and preventers and drawing on ideas from biological and cultural evolution. Then come sections on the practicalities of adopting a deliberately evolutionary approach to prevention, and weaknesses of purely technological approaches. The conclusion reviews the significance of understanding technology for SCP. Throughout, low-tech and hi-tech, material and cyber technology are covered in parallel.

The nature of technology

Technology has been the subject of theoretical and philosophical discussion[2] since Ancient Greek times. Plato (Plato, *Laws* X 899a ff), for example, anticipated biomimetics in describing the origins of invention as imitation of nature, such as derivation of weaving from observation of birds' nests. Aristotle (*Physics* II.3), however, saw technology as sometimes surpassing nature, and went on to distinguish between natural objects and artefacts, the latter uniquely being shaped by human purpose. This ontological distinction remains troublesome, even today – for example the notions of biological and technological *functionality* are still challenging to pin down, and to relate. Both Plato and Aristotle nonetheless drew on technological imagery for explicating their views of the rationality of the universe. This practice has continued (albeit for applied as well as theoretical ends) through Harvey's 'heart as pump' analogue, to today's 'brain as computer' imagery. The earlier approaches to technology adopted what Mitcham (1994) called the 'humanities' philosophy of technology, exemplified in the extreme in the Marxian focus on the means of production as key to shaping the evolution of class relations and wider society. More recently, another approach has emerged which focuses on technology in itself rather than as a 'black box' influence on society; and which aims to understand both the process of designing and creating artifacts, and the product. This perspective has more in common with the analytical tradition in modern philosophy and in particular the fields of the philosophy of action and decision-making; it also connects with the philosophy of science.

[1] I'm grateful to the Editor for useful and interesting comments.

[2] This paragraph draws heavily, but not exclusively, on the excellent entry on the Philosophy of Technology in the *Stanford Encyclopedia of Philosophy*, 2013 revision, http://plato.stanford.edu/entries/technology/ accessed 21 January 2016.

Here, there are many resonances with the field of applied criminology now self-identified as *crime science* (e.g. Junger et al. 2012). This seeks to focus scientific understanding, experimentation and methodological rigour on the proximal causes and processes of criminal events with a view to situational intervention and criminal investigation. It has a practical, functional approach and a preference for the discourse of Scientific Realism, both to uncover underlying 'causal mechanisms' of criminal events, and more particularly to generate context-fitting interventions based on principles which themselves are abstracted mechanisms, such as deterrence (e.g. see Pawson and Tilley 1997; Pawson 2006). 'Mechanism' in itself is arguably a continuation of the technological imagery already mentioned, originating in the 'clockwork' era. And of course, Rational Choice approaches to *criminal* decision-making (Cornish and Clarke 1986) and an interest in *criminal* action through Modus Operandi and scripts (Cornish 1994) are central to SCP. None of this implies denial by crime science of the importance of psychological, social and cultural influences on crime and their significance in its prevention; indeed, many originators of crime science trained as psychologists, engineers being more recent arrivals. But crime science has an affinity with the modern, analytic philosophy of technology in its willingness to embrace hardware and software solutions (discriminatingly and in a context-appropriate way, ideally through careful design that takes full account of human/cultural factors), and to draw not just on social science but on natural science and engineering. It is therefore this perspective that is primarily adopted here, albeit extended to embrace concepts from biological and cultural evolution.

Among recent theorists of technology, Mitcham (1979) identified 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, innovation), and volition (ethics, technology as social construction). Arthur's recent (2009) 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 scales 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) existing independently in nature. Technology is organised around central principles – the application of one or more phenomena for some purpose; principles in turn are expressed through physical or informational components which are combined, often hierarchically, to meet that purpose. Technological domains are toolboxes of potential, clustered around some common set of phenomena or applied principles such as movement of mechanical parts, or of electrons.

These frameworks readily apply to technology in the field of crime and its prevention. Mitcham's volitional dimension, say, could include the social institution of crime and the social forces of conflict between individuals, between individuals and wider social groups, or between either of these and the state. Arthur refers to multiple purposes; extending these to the multiple stakeholders that hold them is central to criminal conflicts.

Opportunity

As said, SCP centres on the immediate causes of criminal events; these are usually conceptualised as *opportunity*. In the Rational Choice perspective (Cornish and Clarke, 1986), an opportunity emerges when the offender perceives risk and effort as low and reward high. These considerations are used among others to structure an assemblage of (25) generic techniques (e.g. Clarke and Eck 2003). Complementing this psychological approach is the ecological Routine Activities perspective (Cohen and Felson, 1979), where a likely offender encounters 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 of abstraction there are affinities with Arthur's 'decisions and activities and flows of goods and services' quoted above. But SCP's familiar theoretical perspectives require extension and integration to properly link to technology.

Tools and weapons are considered 'crime facilitators', and 'control tools/weapons' appears under 'Increase the effort' in the 25 Techniques of SCP. But there is no theoretical treatment of technology. Both 'technology'

and ‘techniques’ derive from Greek tekhne, art and craft; some techniques involve the use of particular technologies.

Within the Routine Activities model, the capability of guardians is an obvious conceptual peg for preventive technology. While there is little explicitly covering technology for offending, Cohen and Felson (1979) did originally include offender capacity under ‘likely’ but most writers nowadays 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/) seeks to integrate the Rational Choice and Routine Activities approaches plus others on the situational and offender side, providing 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 elaborated to cover technology more comprehensively.

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. 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 deliberate or inadvertent promoters. When these preconditions are perceived to be met the offender decides to proceed. When they are blocked, weakened or diverted by a security intervention, the offender either cannot so act, or decides that the perceived reward is not worth the effort and risk.

Mapping technological opportunity and prevention: CCO

Mapping opportunity systematically and in detail enables us to focus on the particularities of the relationship of technology and opportunity: by considering each element of CCO and their interactions we can develop a ‘gazeteer’ of the huge variety of technological connections for both commission and prevention of crime. We start with the elements on the crime situation side, and finish with those relating to offenders. Both material and cyber examples are used.

Targets of crime

Arguably since the Neolithic and then the Industrial revolution set in train an accelerating trend to property ownership, technology has come to supply most of the material targets for crime (cf. Felson and Eckert 2015): new things of value from pots to jewellery to smartphones; also commodities such as copper from power or signalling cables (Sidebottom et al. 2014). This trend has extended to cover information-related value starting, perhaps, with coins (shortly after silver coins were devised in ancient Greece in about 600 BC, someone produced a silver-plated bronze forgery (James and Thorpe 1994)); and ending, for the present, with bitcoins and identity- or finance-related data. Here, ‘legitimate’ trading in personal data and information by banks and large corporations is accompanied by increasingly sophisticated attempts to steal or manipulate such information.

Through bad or good design, technology can render those targets vulnerable, attractive or provocative to offenders; or resistant, unattractive and inoffensive, inextricably integrated, distributed (as with in-car entertainment components), invisible or non-existent. Security technologies have a long history, and not just in terms of defensive weaponry. For example, Archimedes’ principle, a way of checking the density of complex shapes like crowns, was invented to counter deliberate dilution of gold by base-metals. And microscopic marks were incorporated in early coins to validate them against counterfeiting.

Mass production, as a long-term trend, has stripped the inherent individual identity from material items. This had to be reinstated artificially, by technological means, e.g. with inbuilt or added-on marking of some kind. Since digital – as opposed to analogue – encodings are easily replicated, so too are the items they encode easy to copy whilst preserving value, whether they comprise music, images, or 3D representations stored on computers for purposes of design and manufacture. As another major trend, therefore, the inherent

copiability of information products, plus the development of appropriate copying technologies, has radically changed the domain of Intellectual Property and its theft and counterfeiting.

A range of material and informational properties can render targets at high risk of theft, for example. Relevant risk factors have been documented by Clarke's (1999) CRAVED acronym for 'hot products': Concealable, Removable, Available, Valuable, Enjoyable and Disposable. Many of these have a technological dimension. Protective factors for mobile phones were identified by Whitehead et al. (2008) as IN SAFE HANDS: Identifiable, Neutral, Seen, Attached, Findable, Executable, Hidden, Automatic, Necessary, Detectable, and Secure. Ekblom and Sidebottom (2008) developed a suite of technical definitions for aspects of product security.

Targeting of human individuals can also be technologically mediated ~~be affected too~~, via physical assaults with weapons, identity theft or the verbal onslaughts of cyber-bullying. At the extreme but not implausible end of the scale, future microbiologically-based attacks on individuals, communities or members of particular ethnic/genetic groups are unfortunately in prospect following advances in biotechnology and dramatic increases in the cheapness, portability and ease of use of techniques like genetic modification of pathogens (www.newstatesman.com/sci-tech/2014/11/martin-rees-world-2050-and-beyond).

Target enclosures

Enclosures are a major domain of technology. They may contain targets for crime but can also be targets themselves (e.g. theft from car, theft of car). They range from handbags to safes, vehicles, buildings, compounds and firewall-protected ICT systems. Locks give differential access to the legitimate key-holder. Their technology is millennia old, with lock-picking maybe several days younger. Enclosures can be resistant, or vulnerable, to attack and the defence or the attack can involve technology of one or other kind, e.g. a cutting torch, or handbags whose materials resist slashing (see e.g. the Karrysafe range by VexedGeneration, www.designagainstcrime.com/projects/karrysafe/). Offenders, too can create or exploit enclosures (Atlas' 1991 concept of 'offensible space'). Relevant technology ranges from the simple, like the sliding peephole hatch of the Prohibition-era speakeasy, to the sophisticated, such as the movement detectors protecting a Bond villain's hideout. Conflict-avoiding technology exists in the form, for example, of noise insulation between apartments.

Wider environments

Wider environments have two kinds of properties, often shared with enclosures. The motivational dimension relates to the wealth of targets an environment contains, territoriality it arouses or conflicts generated/avoided. More significant here is the tactical/logistical dimension: how the layout, design and construction of the built environment favours offenders over preventers, or vice-versa. Some modifications of the environment, like artificial lighting or mirrors, may be used/misused by either party equally; others, like CCTV cameras, especially if shrouded to conceal where they are pointing, offer asymmetrical advantage. Online networks and systems serve as entire environments for doing crime and crime prevention, where physical constraints, like proximity and inertia, are supplanted by far more mutable ones.

Crime preventers

The crime preventer role is about agents, who either by sheer presence or deliberate action, reduce the risk of criminal events. More specific and familiar preventer roles in the Problem Analysis Triangle include guardians of targets, managers of places and handlers of offenders (Clarke and Eck 2003). Other background roles not catered for in the original, narrow formulation include the technologists who design, produce and install security equipment. There is, now, a vast range of technological aids to empower preventers, including sensors (e.g. for detecting movement) and responders (e.g. for activating barriers). These embody the 'force multiplier' concept which becomes especially important as financial stringency shrinks human resources. (Offender tagging is a multiplier for handlers.) As advances in ICT integrate these functions the technology becomes an active agency, independently undertaking a preventer role, sensing actions and events, making decisions and taking action. An early example is the automatic detection and blocking of suspicious bank card transactions. The perennial problem of false alarms in automated systems/devices can be met by careful design. This can draw on the fusion of information from multiple sensors, plus knowledge of legitimate behaviour and routines which could either be pre-programmed in, or learned in-situ.

Remote prevention is now a familiar part of the everyday world, from telegraphing ahead about horseback bank-robbers to satellite surveillance, and now deactivation of stolen laptops and phones. Media reports of 'kill-switches' (e.g. www.bbc.co.uk/news/technology-31416846) claim 25-40% reductions in iPhone robberies in various cities since introduction; for recent evidence, see Behavioural Insights Team (2014).

Crime promoters

Crime promoters are roles that make crime more likely or harmful, whether innocently (e.g. inventor of the paint spray-can), carelessly (e.g. forgetting to log off when leaving the office) or deliberately (e.g. supplying tools/weapons for crime, or technical services like unlocking stolen phones). ICT extends the range and reach of agency, with, for example, home computers enslaved in botnets actively delivering distributed denial of service attacks on target organisations. We will undoubtedly see more sophisticated software-based crime promoter agents in future. Where human promoters are inadvertent or careless, technology can help mobilise them to cease promoting and perhaps to start preventing. Automatic reminders to lock vehicles, homes or computer terminals are now widespread. Technology can substitute for human intervention (as with remembering to lock away the telescopic car aerials of yesteryear) or design-out the target altogether. Offenders, for their part, have developed 'social engineering' methods to bypass technological security (e.g. phishing attacks on ICT systems) by homing in on the weaker, human components, to manipulate and exploit people as promoters. This may even involve threatening or corrupting technicians (e.g. those who maintain stand-alone ATMs are apparently being persuaded to install criminals' card-skimming devices – Krebs 2015).

Offender presence in situation

Offenders must either be physically present in the crime situation, hugely aided by transportation technology; or, like preventers just discussed, able to exert their influence remotely. ICT has vastly expanded the possibilities for malevolent telepresence, beginning with threatening/obscene phone calls and moving on to various forms of cyber-bullying, computer virus attacks, and (at a chemical plant near you) interfering with control systems. The awareness space of offenders (Brantingham and Brantingham 2008) has greatly increased, with remote viewing possibilities for hostile reconnaissance, whether via online site maps, webcams or hacking into private cameras (www.bbc.co.uk/news/technology-30121159). The mass-dissemination possibilities of the internet mean that for little effort, offenders can, through phishing messages, reach thousands of potential human targets of fraud and identity theft, greatly altering the balance of effort to reward. More generally, with the Internet of Things, targets themselves may have a presence extending beyond the house, office or factory, in which they are effectively exposed to risk. From the widest perspective, the boundaries between what is a target product or place, a physical environment and a network have become blurred with the advent of wireless internet connectivity so the rules of convergence of offender, target and absent guardians need continual reconfiguration, even though the underlying principle remains valid. Beyond 'pure' ICT, remote-controlled drones can take offenders' ability to reconnoitre, and to execute crimes, to new heights, and to previously inaccessible or well-guarded locations. This emergent tool is generating many criminal applications. One such is the delivery of drugs (www.bbc.co.uk/news/technology-30932395), in which apparently the craft could be sent to a particular place via the GPS location – the risky, line-of-sight presence of the human controller being unnecessary. Drones support prevention too, e.g. being used to patrol Polish railways against coal theft (http://dronelife.com/2015/09/10/drones-deter-polish-railway-thieves/).

Once inside an enclosure, whether a building or an ICT system, offenders may find its internal environment furnishes increased opportunities for crime. Insider threats (Nurse et al. 2014) are a growing concern. Many of these are facilitated by the scale and complexity of company networks and systems. These make crime opportunities hard to detect and block for security staff, but perhaps salient to those employees in particular roles who acquire intimate knowledge of a labyrinthine system, combined with automated access privileges. Automated monitoring for suspicious behaviour patterns is now possible but this raises ethical and staff relations issues.

From the preventive side, technology has significantly increased the risk to offenders via the trackability and traceability of their persons and their communications, way beyond the scope of fingerprints and footprints. Unfortunately, criminals are also misusing a remote-wiping facility intended to protect owners against information theft, to clear incriminating data from phones seized by the police (www.bbc.co.uk/news/technology-29464889).

Offender perception and anticipation

Moving further into the offender side, the perception of risk, effort and reward can be influenced by the technological dimension, for example through deterrence (perceived risk of harm relative to reward) and discouragement (perceived effort relative to reward). Alarms, CCTV, chemical tracing or radio/internet trackers, for example, may all increase objective/subjective risk; they will require either increased risk toleration or greater effort to reduce it, whether technological or behavioural. Uncertainty about the capabilities of some new technological application may augment deterrence; presumably offenders will habituate once they discover its scope and limitations but a stream of new and varied approaches can maintain the pressure.

Resources for offending

Resources for offending are diverse (Ekblom and Tilley 2000; Gill 2005), including the criminal's 'native' properties like courage or strength. Unless we include amphetamines or alcoholic fermentation, these are currently uninfluenced by technology; but performance enhancement and mood control are under constant development in military and sporting contexts and we can expect criminals to exploit them. Of more widespread significance are the resources which offenders can find on arrival (such as scaffolding poles), modify in-situ (e.g. smashing beer-bottles to create weapons), or bring to crime situations (weapons, hardware tools like centre-punches for unobtrusively breaking car windows, or previously-acquired pass-codes). Tools must usually be concealable or have plausibly legitimate uses if the bearer is challenged by the police. Disguised sabotage weapons were widely-developed in WW2 (www.bbc.com/news/uk-34399018). Clarke and Newman (2006) have developed the acronym MURDEROUS to characterise terrorist weapons – Multipurpose, Undetectable, Removable, Destructive, Enjoyable, Reliable, Obtainable, Uncomplicated and Safe. Unfortunately, technological advances mean that many more products are becoming versatile, miniaturised, portable, self-powered and easy-to-(mis)use. Even the easy-to-fly aircraft and easy-to-learn-from flight simulator can make significant contributions. Biotechnology adds another dimension – terrorist threats of engineered diseases apart, apparently it is considered likely that yeasts genetically-modified to produce morphine will become available in the next few years (www.newscientist.com/article/dn27546-homebrew-heroin-soon-anyone-will-be-able-to-make-illegal-drugs.html?full=true#.VVpCSkaMlpo). Apart from direct increases in criminal opportunity the disruptive-technology effect on organised drug producers, traffickers and dealers could be immense, doubtless with resultant violence.

Besides boosting their own resources, preventers can try to restrict those of offenders. Interventions include, for example, designing photocopiers to detect, and block, efforts to copy banknotes; legislating against possession of code-cracking software and hardware for rendering stolen mobile phones re-usable (Ekblom 2002); and 'capture-proofing' police firearms e.g. via fingerprint-activation.

Readiness to offend

Readiness to offend represents the motivational/emotional side of crime causation. Such causes can occur in-situ, as with situational provocations and pressures (Wortley 2008). They can also happen further 'upstream', for example a stressful commute may leave a passenger ready to assault ticket inspectors. Further still, persistent sleepless nights from traffic noise or false car alarms may impair self-control, as, perhaps, can shift-work. Social media can amplify intergroup conflicts. Technology can also be the author of its own destruction, as with faulty ticket dispensers that provoke 'machine rage'. The chemical technology of alcohol and other drugs of course can disinhibit the tendencies normally kept in check by the brain's executive function.

Resources to avoid offending, and Predisposition to offend

Our ability to earn an honest living is often dependent on, or disrupted by, technology, though this is outside the present focus on proximal causation and intervention. But technology can intervene on the preventive side. Examples are psychopharmacological, neurosurgical and cognitive interventions which are intended to reduce the readiness to offend, or even to alter the predisposition. Examples of the latter used historically but now understandably abandoned were prefrontal lobotomy and chemical castration. More widely acceptable nowadays is the search for means of removing drug addiction by targeting relevant brain centres pharmacologically or via immune-system responses. Pharmacological intervention, transcranial electrical

stimulation, surgical implantation and who knows what other kinds of intervention may emerge in the future and will pose serious ethical challenges before they can be applied for crime prevention purposes, if ever.

Extending the concept of opportunity

The detail with which CCO deconstructs opportunity allows further insight. In SCP, opportunity is typically considered an attribute of the situation. But an open window three floors up, say, is only an opportunity to an offender with the resources of agility, courage and/or climbing aids such as a ladder. Opportunity is thus an ecological interaction between situation and offender, and this is often technologically mediated.

Nor does opportunity make sense without specifying 'to do what' – there must be some purpose, ultimately stemming from an agent's predisposition. 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.

Technology, opportunities and problems

Another issue to consider is how opportunities relate to problems. SCP methods are usually selected, implemented and evaluated through a problem-oriented approach (e.g. Goldstein 1990; Clarke and Eck 2003; Bullock et al. 2006). 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 is always 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. So, a problem is an obstacle stopping an opportunity from being instantly achievable.

Enter technology

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, as discussed below.

On the problem side, technology can contribute to solutions by bridging gaps in 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 new round of problem and opportunity – as with the arrival of CCTV – monitoring misbehaviour, or spying on changing rooms. Besides prevention, technology can halt an ongoing criminal attack (for example 'smokecloaks' to obscure vision www.smokecloak.co.uk/en/), or mitigate the adverse consequences of crime – whether a backup of data on a stolen phone, or supporting business continuity after a terrorist attack.

And technology can resolve design contradictions (Ekblom 2012a) or trade-offs between security and, a range of values including safety, profitability or privacy. An example of the last is the millimetre-wave airport body scanner that aids security but reduces privacy: here a technological resolution is the substitution of a personal body image on the operator's screen with a generic, computer-generated outline that still displays suspicious items. In solving problems, therefore, technology enables rapid adaptation of the good or the bad party to the challenges posed by their material and social habitat to the pursuit of their various goals.

Cyberspace creates a new technological domain for opportunities and problems, but it is debatable whether recently-emerged crimes in silico are always merely reconfigurations of familiar clashes in vivo, with physical constraints removed, or entirely new ones. Certainly identity and trust in online transactions have become

huge issues. Applying CCO to cyberspace, Collins and Mansell (2004:64) noted how trust fits into the framework. '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.'

Together, technological extensions of human capabilities, and the technologically-modified situations in which those capabilities are exercised, engender many opportunities both for crime and 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 and perhaps neutralising the benefits (Tenner 1996).

The dynamics of crime: technology, scripts and script clashes

The coming-together of proximal circumstances to generate criminal events may result from influences at levels ranging from the individual offender *creating* the opportunity – which is not a Routine Activity – to emergent societal influences including market forces. For its part, Rational Choice does not cover the *actions* carrying out and linking successive decisions. A complete picture of crime as opportunity must incorporate a dynamic view. This is especially true with more complex crimes involving sequences of action.

Cornish (1994) developed this perspective 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 script analyses can be better woven into the opportunity/problem perspective presented here if they more explicitly attend to goals, plans and resources ((Ekblom and Gill 2015).

Being instrumental, scripts can be influenced by technology as problems are solved and opportunities realised. Problems come in hierarchies or clusters, e.g. a subsidiary, yet prior, problem to obtaining cash by burglary could be acquiring a crowbar. In this sense, problems equate to necessary subsidiary goals whose potential means of achievement, i.e. solutions, are not yet determined. (Actual achievements are only finally reached via successful attempts.) Offenders 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 eliminate traces on them such as from DNA or electronic usage data. An approach from accident prevention (Reason 1990) compares complex security systems to a stack of slices of Swiss cheese – in which the succession of holes cover for each other, unless aligned by accident …or by intent. We can envisage the latter being achieved by executing a crime script, which aligns an entire *opportunity path* through successive obstacles.

The available 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 subtleties. For example, the Concealable factor in 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, at the target-seeking stage.

The procedural analysis of behaviour applies to preventers as well as offenders (Leclerc and Reynald 2015) covering all the above considerations. The preventer's script may overlap with 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

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 which designers of prevention must address in arranging 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 (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 decades made them more suitable 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 from historical population movement into cities. Related arguments were previously set out by McIntosh (1971), covering interactions between changes in the technology and organisation of crime prevention, and those in the organisation, level and type of fraud.

Change is now the norm. Technologically-induced changes diffuse through society at differential rates, leading to cultural lags in adjustment (Ogburn 1922). Many (e.g. Arthur 2009) note how technological change has been accelerating. This amplifies such lags and their negative consequences, as for example when crime prevention techniques trail those of crime commission.

Cultural and biological evolutionary perspectives

Accounts of the change process usually draw on evolutionary themes. 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 at diverse 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 disrupt or transform whole industries and beyond (such as ICT). The pressures shaping technological evolution variously relate to market forces, networking, and physical and social constraints.

Viewing technological evolution as a subset of cultural evolution can give useful insights. But by combining both with biological evolution we can gain fresh concepts and some detachment from conventional viewpoints. Biological and cultural evolution have previously been considered rivals for explaining human behaviour (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.

The differences are, however, instructive. For example, Arthur (2009) notes the relative rarity of combinatorial mechanisms in biological evolution (such as the symbiotic merging of 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 engines.

It seems that the ability to develop relatively complex tools required a surge in brain size (Faisal et al. 2010). Moreover, human hand bones appear to have evolved special features to enable tools to be grasped and wielded (Ward et al. 2014). The anatomy and fine neurological control of the hand, plus the construction and use of tools 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 technological development of projectiles, a process which may have begun with Homo erectus some 2 million years ago. The relevance of tool/weapon wielding for both instrumental and expressive crime is clear, whether the use of our hands is in direct combat or more remotely-connected action.

From a cultural evolutionary 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 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 plus many others including the invention of mass transportation, are claimed 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; 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 anthropogenic climate/sea-level 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., 2015), is where a given species pervasively shapes its own environment to its advantage and simultaneously adapts to survive within it, as with corals building entire reefs out of their limestone skeletons. We humans have come to hugely constitute and determine our own environment in both social and technological terms, for better and for worse. In the extreme, some ecologists consider we are creating an entire new geological epoch, the Anthropocene (Williams et al. 2015).

Biological lag

To Ogburn's concept of 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 (e.g. Nowak and Highfield 2011) evolved in this period. Beyond the breathtaking cooperative technological effort of developing global ICT systems or putting people on the moon, cooperation also creates the backdrop (rather neglected by criminologists) against which crime, as a failure in cooperation, 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 – where time, space,

materials and local population size provided natural constraints on conflict, differential wealth, things to steal and violence – are now inappropriate. Weapons of easy, stand-off killing and mass destruction are available together with a cornucopia of portable high-value goods; vehicles and computer terminals insulate us against natural empathic signals between conflicting individuals and may unleash road rage or online trolling. Cultural evolution e.g. of institutions such as the law has helped to compensate for inadequate psychological/ecological controls, but direct interventions to improve security remain necessary (Schneier 2012).

Perturbation, co-evolution and arms races

Thwarted commercial burglars can simply return to attack a security fence with more powerful bolt-cutters – 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 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 of power supply, and the break between appearance and functionality, will all keep shifting the balance between offenders and preventers.

Change can be exogenous (driven by external forces like the emergence of motor vehicles, acting as crime resource and target par excellence, or as police patrol car), or endogenous, by the playing out of script clashes involving adaptation and counter-adaptation of criminals and preventers to one another's tools, techniques and weapons. However, the nature of perturbation, and the interactions between multiple 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 channels. A compact 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 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 depart'; the first bike theft script 'see unattended bike, get on and depart'. 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, often engendering 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; Ekblom 2015). These are 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). Classic examples are the evolution of locks/lockpicking (Churchill 2015), the safe (Shover 1996), coins and banknotes, and more recent means of payment such as online purchases. Once started, arms races may proceed at an irregular pace. 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 and, for a while, overwhelms the opposition's defences. One example is the recent emergence of kits for converting drones to carry graffiti spray cans (www.icarusone.com/home/). And imagine, more strategically, the devastating effect on cyber security if someone discovered how to identify the huge 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 that the 'security hypothesis' (Farrell et al. 2011) – sustained technological and procedural improvements in the security of homes, vehicles, shops etc. – accounts for the striking crime drop 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). 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.

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. 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). And from a carelessly-displayed online photo, US Transportation Security Administration master-keys to open every air traveller's luggage were engineered, and converted to 3D printer instructions available online (www.theguardian.com/technology/2015/sep/10/3d-printed-tsa-master-keys-put-travellers-luggage-at-risk). This acceleration/replication capacity is far 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/). 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). This will surely 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, otherwise win individual battles, but lose campaigns. 'Gearing up against crime' approaches (Ekblom 1997) suggest how. Some are lessons transferred from a range of other evolutionary struggles including 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 and Taylor. 2008). Practically speaking, running arms races (Ekblom 1997, 1999, 2015) 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 slots into place.

It is prudent to establish systems for detecting and reacting to new technologically-enabled crimes. But given the lead-time to develop security functionality, anticipation is important. The traditional anticipatory method of the problem-oriented approach to crime prevention – induction of risk and protective factors from past patterns of hotspots, hot products etc. is unsuited to handle nonlinear changes in technology. Luckily, alternative, 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). Technology roadmapping, which seeks to connect future requirements with emerging trends in technology (e.g. www.technology-roadmaps.co.uk/secure_environment/), could be applied to both crime prevention and the misuse of new technologies and technological combinations by offenders.

Horizon-scanning can be rendered more systematic and rigorous by incorporating SCP approaches. Routine Activities 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 – as with Hot Products)
Mistreatment (damage or injury)
Mishandling (e.g. smuggling, data transfer)
Misrepresentation (fraud)
Misbegetting (counterfeit)
Misuse (as tool or weapon)
Misbehaviour (for spraying graffiti for example)
Mistakes (e.g. false alarms)

In turn, we can link these generic factors to more specific crimes and/or particular anticipated trends in technology, 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 stating regulations in 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) to encourage technologists to develop the appropriate preventive capabilities.

Technology, innovation and design

Arthur (2009) emphasises the importance of combination of prior elements of technology in generating new products. With crime prevention, systematically generating plausible variety at the level of principles comes from tested theory and what-works evidence (Ekblom and Pease 2014). That theory must be in a suitably analytic, integrated and accessible form, as noted. Again, CCO can be claimed to support this requirement, being a suite of generative, analytic preventive principles, which channel causal mechanisms through practical intervention methods.

But concepts can only be realised by people. We need professional designers closely working with practice-experts and users for the theory and know-how to combine to generate intervention measures that work in principle and in practice; and which meet diverse other requirements including cost, aesthetics, durability, a small carbon footprint, business continuity and public safety. This takes design beyond the homespun practicality of the police and hard-edged engineers. Recent reviews of design and crime are in Ekblom 2012a, 2014b; 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 readiness to 'reframe' the presenting problem (Lulham et al. 2012). But it must also be systematic, constrained and supported by theoretical and methodological discipline (cf Dorst 2015). The use of frameworks like CCO, scripts etc. as discussed, and the more specific situational perspectives behind them, can facilitate this. One approach to feeding crime science into design is the Security Function Framework (Ekblom

2012b; Meyer and Ekblom 2011) for specifying products 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, and how are they operated?)

Weaknesses of technology for crime prevention

Solution-driven approaches to crime 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) epitomises this. Investment in rigid, capital-intensive kinds of technology can hinder adaptation to changes and lengthen the lag behind adaptive criminals. Techno-fixes can be superficial, 'bolt-on, drop-off' efforts. However well-designed and constructed, they can also fail at the interface with humans if that part of the preventive system is inadequately integrated. 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 praise 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 (pervasive enough in Barcelona for bar staff to readily alert customers to these security aids), and on staff motivation and commitment (in the UK bars this seemed lacking, but was firmly present in the café, which 'nurtured' its personnel and established mutual commitment with the company).

Extending such specific evaluations to the contribution of technology as a whole to crime prevention probably poses too great a challenge for the coffers and perhaps the techniques of social research. But the 'security hypothesis' research (Farrell et al. 2011) does suggest that security equipment and procedures together have made a substantive difference.

Preventive technology can do harm, with false burglar/car alarms wasting police time and annoying neighbours. It can also be self-defeating: password-based security systems overload the memory and exceed an employee's 'compliance budget' (Beautement et al. 2008) – how much of their work effort they are willing to dedicate to security procedures. Beyond this level 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); 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 causes the various agents to adjust to that change, and to each other's new stance. Add the complexity of interactions between technologies (how many technologies together enabled the 9/11 attack?) and we can appreciate the unpredictability of the crime (or preventive) impact of individual developments. Crime prevention faces a rich and challenging future, but one where sense-making (Kurtz and Snowden 2003) rather than watertight, orderly explanation and prediction play a greater part, as in the wider economy (Arthur 2009).

Conclusion

Technology pervades the human ecosystem. It constitutes the means of individuals and groups to extend their native capabilities to adapt to and exploit that ecosystem, whether for legitimate purposes or – as noted by Brey (2016, in this volume) – illegitimate ones. It is central to SCP concepts of opportunities, problems and solutions.

Technology both creates and solves problems, and helps to block or generate opportunities for offenders and crime preventers alike. 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 equally to material and cybercrime, and to hi-tech and low-tech products, places 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 preventers must understand technology's fundamental nature; grasp the functional and technical specifics in particular crime situations, scripts and script clashes; and their be alert to their tactical and strategic advantages and drawbacks.

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 innovativeness of engineers and designers, an endless succession of technologically-induced opportunities and problems and sometimes, arms races between offenders and preventers. This evolution unfolds in biological, cultural and specifically technological domains. As with medical science, ethical dilemmas and power/control issues are increasingly likely, but as medicine has shown, these can be addressed.

For the foreseeable future, technology will be a significant shaper, generator and reducer of crime. But successful crime prevention through technology cannot be based on some narrow and linear technological determinism: it requires full awareness of the complexity of social, physical and informational systems. The design of technology must cater for diverse requirements and intelligently discriminate in favour of rightful owners/users over criminal abusers and misusers. While a purely technological approach to crime prevention has weaknesses and limitations, technology that is carefully designed in line with the tested theories of SCP, developed, updateable and updated on an appropriate timescale, and that is well-integrated with the human parts of a security system, can significantly enhance the well-being of individuals, organisations and society.

But criminals too are forever seeking opportunities to exploit new technology, and ways to cope with it. Only strategic, evolutionary and innovative thinking based on plausible theory and empirical research and development can give preventers the edge, a position that will remain perpetually precarious.

References

All web links in references and main text accessed on 30 September 2015 unless stated otherwise.

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.

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

Atlas, R. (1991). The other side of defensible space. Security Management, March, 63—66.

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.

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

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

Brey, P. (2016). Theorizing Technology and Its Role in Crime and Law Enforcement. (This volume)

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

Bullock, K., Erol, R. and Tilley, N. (2006). Problem-Oriented Policing and Partnerships. Implementing an Evidence-Based Approach to Crime Reduction. Cullompton: Willan.

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

Churchill, D. (2015). The Spectacle of Security: Lock-Picking Competitions and the Security Industry in mid-Victorian Britain.

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

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

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

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

Ekblom, P. (1997). Gearing up against crime: a dynamic framework to help designers keep up with the adaptive criminal in a changing world. International Journal of Risk, Security and Crime Prevention, 2, 249—265.

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

Ekblom, P. and 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.

Faisal, A., Stout, D., Apel, J. and Bradley, B. (2010). 'The manipulative complexity of Lower Paleolithic stone toolmaking**.** PLoS ONE, 5 (11): e13718 DOI: 10.1371/journal.pone.0013718**.**

Farrell, G., Tseloni, A., Mailley, J., & Tilley, N. (2011). The Crime Drop and the Security Hypothesis. Journal of Research in Crime and Delinquency, 48, 147–175.

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.

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

Junger, M., Laycock, G., Hartel, P. and Ratcliffe, J. (2012). 'Crime science: editorial statement'. Crime Science, 1, 1—3.

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

Krebs, B. (2015). http://krebsonsecurity.com/all-about-skimmers/.Kurtz, C. and Snowden, D. (2003). 'The new dynamics of strategy: Sense-making in a complex and complicated world". IBM Systems Journal, Volume 42(3), 462.

Laland, K., Uller, T., Feldman, M., Sterelny, K., Müller, G., Moczek, A., Jablonka, E. and Odling-Smee, J. (2015). 'The extended evolutionary synthesis: its structure, assumptions and predictions.' Proceedings of the Royal Society B, 282: 20151019. DOI: 10.1098/rspb.2015.1019.

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.

Leclerc, B. & Reynald, D. (2015). 'When scripts and guardianship unite: A script model to facilitate intervention of capable guardians in public settings.' Security Journal advance online publication. DOI 10.1057/sj.2015.8.

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.

McIntosh, M. (1971). Changes in the organisation of thieving. In S. Cohen (Ed.), Images of Deviance. London: Penguin.

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.

Mitcham, C. (1994). Thinking through technology: the path between engineering and philosophy. Chicago: University of Chicago Press.

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.

Nowak, M. and Highfield, R. (2011). SuperCooperators: Altruism, Evolution and Why We Need Each Other to Succeed. New York: Free Press.

Nurse, J., Buckley, O., Legg, P., Goldsmith, M., Creese, S., Wright, G. and Whitty, M. (2014). 'Understanding insider threat: A framework for characterising attacks'. In Workshop on Research for Insider Threat (WRIT) held as part of the IEEE Computer Society Security and Privacy Workshops (SPW14), in conjunction with the IEEE Symposium on Security and Privacy (SP). London: IEEE. DOI 10.1109/SPW.2014.38.

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

Pawson, R. (2006). Evidence-Based Policy. A Realist Perspective. London: Sage.

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

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.

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

Reason, J. (1990). 'The Contribution of Latent Human Failures to the Breakdown of Complex Systems'. Philosophical Transactions of the Royal Society B, **327** (1241), 475–484.

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.

Sidebottom, A., Ashby, M. & Johnson S.D. (2014). 'Copper Cable Theft: Revisiting the Price-Theft Hypothesis'. Journal of Research in Crime and Delinquency, 51, 684—700.

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.

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.

Ward, C., Tocheri, M. Plavcan, M., Brown, F. and Kyalo Manthif, F. (2014). 'Early Pleistocene third metacarpal from Kenya and the evolution of modern human-like hand morphology'. Proceedings of the National Academy of Science 111(1): 121–124. DOI: 10.1073/pnas.1316014110.

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.

Williams, M., Zalasiewicz, J., Haff, P., Schwägerl, C., Barnosky, A. and Ellis, E. (2015). 'The Anthropocene biosphere'. The Anthropocene Review (online first), 1–24. DOI: 10.1177/2053019615591020.

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