Terrorism - lessons from natural and human co-evolutionary arms races

Paul Ekblom

Central Saint Martins, University of the Arts London

Prepublication version – may contain errors – to appear in

Ekblom, P. (2016). 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. www.routledge.com/books/details/9781138774582/

Introduction: Why take a co-evolutionary perspective on terrorism and counter-terrorism?

The potential for violent, destructive and threatening behaviour against fellow humans seems to be inherent in our psychological and anatomical nature (the latter arguably evidenced by special adaptations of our fists, and fist-resistant faces (Morgan and Carrier, 2013; Carrier and Morgan, 2014)). This is true whether that behaviour concerns an argument over an insult, careless driving, domestic relations, religious beliefs and practices, or who governs Eastern Ukraine. The kinds of tactics and strategies classed, at times, as acts of terrorism, fall within this set. Fortunately equally inherent in us are cooperation, empathy and altruism, although in a conflict these can be selectively applied to one's own side, even by terrorists.

As chapter x notes (Ekblom, Sidebottom and Wortley), we can look to our evolutionary origins to help understand, and hopefully to influence, what turns us – as individuals and groups – on and off violent conflict, who we target, over what moral/political causes and under what circumstances. This is the domain of beliefs, identities, ideologies and motivation.

But we can also take another perspective, which is *how* conflicts tactically and strategically unfold, and how this process can be influenced for the differential benefit of the 'good side'. The 'how' essentially concerns the process of *adaptation*, whereby organisms as individuals, groups or species change over some relevant timescale to become better fitted to survival, flourishing and reproduction in their habitual environment. Adaptation for potentially violent and destructive conflict such as carrying out terrorism or defending against it is the core concern of this chapter, although adaptation for cooperation and straightforward foraging with or without violence also play a part. The aim of the chapter as a whole is to explore the lessons for counter-terrorism from evolutionary studies of adaptation in both human and natural domains. This is partly to come up with some practical suggestions at tactical and strategic levels; but partly also to foster a distinctive and, I will argue, promising way of thinking among policymakers, security services, engineers, planners and designers.

From bacteria to buffalo, conflict is an ecological fact of life. In most animals conflict is driven by scarcity of resources such as food and living space, or mating opportunities, and can range from tussles over food, say, to outright predation, where the conflict is over the fleshly assets of the prey. In humans, conflict extends to cover purely culturally-mediated issues of ideology, belief and conformity to particular ways of doing things. In all cases, conflict can lead to violent behaviour although in certain circumstances, injury avoidance or minimisation strategies have evolved such as ritualised combat between the males of certain species (e.g. stags), though even here fights to the death occur. Sport arguably plays a similar role in human culture. (This prompts speculation that a more civilised outlet for terrorist motives might be for the groups to enter teams in the Olympics rather than shoot the other competitors up; religiously-motivated teams, anticipating divine help towards gold, should expect the effort rewarding.)

In most animals, conflict evolves slowly, as changes in anatomy and physiology (sharp fangs and claws, and powerful muscles versus armoured hide and rapid healing of wounds). Among more advanced animals evolution of *cognitive* contributions to conflict (e.g. ambush behaviour, vigilance, knowledge of opponent's moves and capabilities) proceeds faster as there are fewer constraints and trade-offs at the information-processing level. This is especially so if the animal has already evolved the capacity to learn at an individual level during its lifetime rather than the species learning at a genetic level over many generations. With certain limited exceptions, humans are the only species where cognition and our wider evolutionary psychology has led to extreme adaptability and *cultural* evolution.

Although intelligence has evolved in stages from the Cambrian Revolution (530my BP) to date, the increase in cognitive powers in hominins (the subfamily of ancestral human species that split from the other great apes) accelerated markedly in the evolutionarily recent past. Whiten and Erdal (2012) note the tripling of human brain size over the last 2.5 million years – a remarkable development, especially for an organ so expensive to grow and maintain, vulnerable to damage and hazardous in childbirth. They ask how it was possible for a moderately-sized ape lacking the formidable anatomical adaptations of competing professional hunters like lions to compete over the same prey. Earlier authors (e.g. Tooby and DeVore 1987) have focused on explanations in terms of the elaboration of a new cognitive niche based on intelligence and technology (for example the advanced inferential reasoning in tracking prey—how many, whether wounded, how long ago they passed; and the refinement of composite weapons for the kill). Whiten and Erdal argue, however, that cognition alone is insufficient. They present evidence that a fuller answer 'lies in 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.' (p2119). Whiten (2006) termed the complex 'deep social mind' to emphasise the core features of mental interpenetration and adjustment of individual to group-level goals. The consequent fitness benefits, and positive feedback between the elements just described, are claimed to underlie our exploding brain size.

Whether evolution proceeds at an anatomical, cognitive or cultural level (or as a mixture), certain influences act as potent accelerants, channelling and speeding the processes of change. These influences include *rapid environmental fluctuation* (as wet and dry conditions repeatedly alternated in our ancestral East African habitat, demanding hyper-adaptability to survive – Anton et al., 2014); *sexual selection* (as in the creation of the male peacock's tail) and the more general case of *co-evolution*. All three of these still involve a given species adapting to survive, prosper and reproduce in its environment. But in the last two categories particularly, a key regularity of that other environment is *other organisms* in conflictual or competitive ecological relationships and the mutual feedback between those organisms over various timescales ranging from the evolutionary (over many generations) to the individual lifetime.

Co-evolutionary pairings can be mutually beneficial, as with meerkats and ground hornbills keeping a look out for each other, but those with a conflictual or at least a competitive dimension range from mates versus mates, predators versus prey, mothers and foetuses not just in collaboration on mutual survival but in competition over nutrition and energy, and parasites/pathogens versus hosts. Co-evolution can result in what appear to be equilibria between the two conflicting parties but in reality these are provisional, more like temporary standoffs until one party invents (in human culture) or 'invents' (in biological evolution) some new weapon, tool, poison, claw-sharpening process or similar, that for the time being at least, prevails over the other's kit or repertoire. Co-evolution, e.g. between predators and prey, is also considered to drive the formation of new species. In all these cases, individual species are locked into a *complex adaptive system*, where attempts by any one party to anticipate and control the course of adaptation and counter-adaptation are extremely challenging (Chapman, 2004).

Humans have evolved as intensely social animals, as described above: from early primate ancestors onward, the environments we have adapted to through biological and, increasingly, cultural evolution have always been made up to a significant degree by our conspecifics – nowadays, fellow humans. As populations have grown in historical times, and various technological revolutions such as agriculture have allowed for ever-denser living culminating in urbanisation, phase-changes in social structure have meant that we humans, and our buildings, comprise an ever-higher proportion of our own environment. We are thus in a position of having to adapt ever better to living with, and unfortunately conflicting with, each other.

We have also had to adapt *to*, as well as *through*, changes in our own technology and consequent changes in our wider society and culture. Higher primates and certain bird groups have evolved the use and even the design and manufacture of tools (e.g. chimpanzees and termite-fishing sticks). Earlier human species like Homo habilis made slow technological progress. The 'Oldowan' flint-stones they shaped as flake tools and weapons kept the same form for 700,000 years. Only with the arrival of more advanced species did the capacity for design, development and improvement take off, marked by the emergence of sophisticated Acheulian core tools such as hand-axes and cleavers some 1.7 million years ago. And with the arrival of Homo sapiens development took place at an accelerating pace with only a few minor setbacks (such as the fall of the Roman Empire) up to the present day, where we routinely talk of 'future shock' (Toffler 1970). New technology is disruptive: it perturbs human cultural, and natural ecosystems and upsets the provisional equilibria of conflict described above. It contributes to the 'disturbed ground' of rapidly-changing habitat of the kind claimed to have driven the evolution of our intelligence and generic adaptability (in natural disturbed ground we encounter aggressively adaptive, generalist species like rats, and rapidly-growing and breeding weeds). Thus change begets change: ever more adaptive cultures, or species, create the very conditions for further adaptability, opportunism and change.

Terrorist movements seek to violently impose change on fellow humans, or to reverse others' changes they do not like. The movements may be engendered by exogenous disruptions, may exploit them strategically and tactically, and may cause further disruptions in their turn. Terrorists, as individuals, are presumably no more adaptive than the rest of us (indeed some terrorist movements are in many ways highly conservative and internally conformist, though that constraint unfortunately seems not to apply to their innovativeness in technology or technique). But as groups, organisations, networks and movements they collectively possess some distinct adaptive properties which compare favourably (from their perspective), say, with organised crime and common-or-garden criminals. (Lone-wolf terrorists may either possess some of these properties as individuals or free-ride on those of others.) They are highly motivated to work hard to achieve strategic goals and intermediate ones such as the acquisition of logistical resources and weaponry, and the pursuit of innovative means. They may be persistent and consistent over years or even generations, unlike casual criminals, who are rarely displaced from immediate, easy opportunities to ones that are a bit harder, more risky and less rewarding (Guerette and Bowers, 2009). Terrorists may value risk and danger as a badge of commitment, or an emblem of intimidation. Their belief system (and system of self-justification) can overcome a range of psychological or societal constraints including the finality of death, and the deservingness of enemy groups for empathy, respect and humane treatment. They may develop such a level of fellow-feeling, centred on nationalism, religion or some other ideology, that interpersonal trust can flourish. These characteristics can give them adaptive advantages over everyday society.

When cultural or biological co-evolutionary struggles persist, they may develop into an *arms race*, where each party tries to out-evolve the other over some extended period (in biological evolution, 'tries' is of course used as shorthand for those parties that manage to out-evolve their enemies, and hence win out in survival and reproduction). In the natural world such races may continue for aeons (for example, between bacteriophage viruses and bacteria). In the human world it is rare that we can keep specific intergroup conflicts going in a consistent direction for more than a few decades. The Hundred Years' war between England and France is thus named as a rarity (and was, in fact, intermittent); the 19th/20th century naval arms race between Britain and Germany endured only a few decades; but a more generic race, between defensive and offensive arms manufacturers now continues on an indefinite basis in the global weapons market. Crime and its control have been described in arms race terms for some while (e.g. Ekblom, 1997, 1999; Sagarin and Taylor, 2008). The classic example is the safe (Shover, 1996). Here, the succession of moves and countermoves, against the background of emerging disruptive technologies like thermic lances and diamond-tipped drills on the one side, and manganese steel, copper laminates to conduct away heat and intelligent/internet-connected alarms on the other, has meant that what works for offence or defence at one point in time may cease working in future. Terrorist arms races include, for example, concealment versus detection of hand weapons and explosives, penetration versus resistance of physical barriers, concealment and booby-trapping of IEDs, and hacking versus security of IT systems and controls.

How, then, does legitimate society handle terrorists, who undoubtedly have a strong capacity and motivation to adapt and evolve? Until relatively recently, the consensus among evolutionary-minded commentators on security (whether crime or terrorism control) was summed up by Cohen et al. (1995:216) who argued that 'contemporary crime control policies are hopelessly static'; by Ekblom (1997, 1999) in similar terms; and more recently by Dietl (2008) who argued that we need frameworks that do not 'freeze' change. And society's conventional legalistic response is notorious for being slow moving, although this is for quite understandable reasons: attempts to rush in legislation to address particular criminal or terrorist problems have tended to misfire and to have adverse and unforeseen side-effects, such is the complexity of the corpus of laws and of human lives they are intended to regulate. In fairness, there has been progress, particularly on the cybercrime front (where evolution of both attack and defence can be rapid). The 2010 UK National Security Strategy (UK Cabinet Office, 2010), for example, proposes that because 'we cannot prevent every risk as they are inherently unpredictable', there is a need to 'remain adaptable for the uncertain future' and to 'identify threats and opportunities at the earliest possible stage'. (2010: 18-25) Situational Crime Prevention has been sensitive to the accusation of vulnerability to displacement from one well-protected place or target to another less so. Arguably, this has blocked any sustained interest beyond the short term – when displacement is uncommon – to the longer term, when adaptation is more likely (e.g. Ekblom, 2008).

So, society is in a tactical co-evolutionary arms race with terrorists, against a wider backdrop of technological and social change that continually perturbs any balances of advantage that temporarily benefit one or other party, offering new opportunities for offence (weapons, tools and targets) and defence. How best, then, can society cope over the medium-to-longer term? Not by winning individual security battles, important though these are – indeed, some approaches that confer short-term gains in power and influence may be inconsistent with longer-term strategies of survival (Vermeij, 2008). Instead, we have *to gear up against terrorism* by playing the terrorists at their own game: through strategic, co-evolutionary thinking about arms races and how to run or sidestep them. This necessitates a closer look at evolution itself.

Vermeij (2008), like Roach and Pease (2013) suggests that lessons from biology and palaeontology have been overlooked by policymakers due to the widely-held notion that human nature differs fundamentally from the adaptations of other life forms, not least because the problems faced by humans do not apply to other living things. He contends, by contrast, that humans have faced the *same* problems of limited resources and vagaries of climatic and geological upheaval and that 'the distinctive attributes of human individuals and groups are subject to the same rules of competition and cooperation that have governed the adaptation and evolution of organisms always and everywhere.' (p26). He goes on to say (p27) that 'This fundamental identity of human nature with the natures of other life forms opens the door wide to the principles and major findings of disciplines dealing with life's evolution in a challenging world. At the very least, this approach can help us identify solutions that have worked in the past for many forms of life over the long run, as well as point to responses that have proved less effective.' This neatly articulates the line taken in this chapter.

In the rest of the chapter, I first backtrack a little to summarise the key features of the process of biological evolution, and co-evolution. (A useful alternative account, with a discussion of how evolution and social science-based criminology can and should mix rather than mutually repel, is in Roach and Pease, 2013; an excellent account from the security world is in Schneier, 2012; and coming from biology to security is the book *Natural Security*, edited by Taylor and Sagarin, 2008.) Then, I show how closely-related evolutionary processes apply to cultural (including technological) change, opening the knowledge-transfer process up to a range of natural, and human, co-evolutionary struggles. Following that, I show how such a widened perspective can apply to terrorism and counterterrorism in particular. Before concluding, I discuss a range of lessons for how to run terrorist arms races, drawing heavily on those most human of culturally-evolved adaptive processes, design, research, theory and evaluation.

To avoid later disappointment, I should declare that adopting an evolutionary approach confers no clear ability to predict in detail what terrorists will do next (or what preventive measures will emerge). As Dietl (2008) states, the historically contingent nature of selection cannot be overemphasised. However, Vermeij (1999) holds that while the precise time course of history and the nature of the participants remain unpredictable, some universal rules governing participants and their actions enable us to discern underlying temporal patterns that *are* predictable and scientifically testable. He also (2008) contributes useful ideas on how organisms themselves have evolved to handle unpredictability in their lives and across generations. And abstract approaches to conceptualising innovation in engineering can also offer some encouraging possibilities, as will be seen.

It is possible to undertake a completely detached and disinterested analysis of political and religious violence, and a significant degree of distancing from everyday perceptions, feelings and values is needed for social science to make an appropriate contribution. But where that contribution is a practical one, there is an inescapable value-choice, namely to come down on our own side – albeit in full acknowledgement of the difficult issues in defining crime and terrorism (Bassiouni, 2002; Ekblom, 2012a) and the troublesome tradeoffs between, say, controlling terrorism and promoting privacy.

Evolution: key features

In this section I aim to cover first, the basics of evolution, and second, some more elaborated themes with relevance to co-evolution of terrorism and security.

The basics

As Darwin first proposed, and others have since developed, the basic process of evolution is threefold: *variation* (in some anatomical, physiological or behavioural trait of individual members of a living species); *selection* (differential survival and reproduction of the fittest, i.e. best-adapted variants of that species); and *transmission or inheritance* of the successful variations to successive generations. Given a consistent selection pressure, say for taller individuals, operating in the habitat of a particular species, the population of that species

will come, over generations, to be dominated by the variants best adapted to that selection pressure. From time to time, a single species will split into two or more descendants.
The mechanisms of variation and inheritance are intimately linked – through the replication and storage of information mainly in the DNA of our genes. Variations come about through several kinds of error in copying the information from one generation to the next, and from the mixing of diverse contributions from both parents in sexual reproduction. Occasionally *symbiosis* will bring together more radically divergent sources of information/ experience of how to survive, and this seems to have engendered major leaps forward in the success of the life-forms combining in this way. For example, the incorporation by certain primitive single-celled organisms of oxygen-burning bacteria – ancestral mitochondria – provided a huge boost in the energy supply for what became our eukaryote forebears (eukaryotes being complex cells with nuclei and other organelles, contrasting with the simpler prokaryotes, namely Bacteria and Archaea). Without this facility, advanced life-forms would not exist.

Selection may be the 'vanilla' version of hazards and challenges like climate change, meteorite impact, an unlucky local landslip, or invading species that are simply better-adapted to outcompete; or it may be specifically driven by sexual preference or wider co-evolutionary processes. Typically an organism must simultaneously contend with diverse selection pressures, so the result is usually some kind of compromise in 'fitness space'. This is a multi-dimensional manifold of possible variations characterised by peaks, plains and valleys. Dawkins' book 'climbing Mount Improbable' (1996) describes how variation and adaptive advantage in relation to selection pressures can, through gradual steps, ratchet a species up to a pinnacle of fitness. In nature, however, the variation is blind and in the unbroken chain of living generations, every single heritable variation must either convey some immediate adaptive benefit or at least be neutral. Thus an organism may be marooned on a local peak and unable to move to a higher one just across the plain because to do so would require entering an intermediate state of maladaptation, hence diminished reproductive chances relative to predators, competing conspecifics etc. Leaps directly across space from one peak to another through 'lucky' mutations or other copying errors are extremely rare, but inter-species sharing of DNA (e.g. via viruses) can occasionally produce otherwise impossible advances, as can inheritable forms of symbiosis, as described.

By this simple and mindless process of variation, selection and transmission, nature generates 'endless forms most beautiful' (Darwin, 1859: 489) – and some pretty ugly ones too. Several elaborations deserve mention, which are now, or may be in future, useful for thinking about terrorism in co-evolutionary terms.

Evolution as learning and hypothesising
Evolution has been described as a kind of *learning* process at the species level, wherein genetic variations can be viewed as 'hypotheses' about predictable elements of an organism's customary environment including dangers and risks, and of what works to enable an organism to survive and reproduce there (Vermeij, 2008). (An earlier and related formulation is Campbell's (1974) concept of 'evolutionary epistemology', where our academic theories are tested by practical implementation to see if they achieve the anticipated and desired changes in the real world.) The knowledge accumulated is not only about how to survive, but also by extension about the nature of the 'environment of

evolutionary adaptedness' (Bowlby, 1969) itself. Thus for example our genes have come to 'know' that we live on a planet with a certain strength of gravity, an oxygen atmosphere, dangerous predators, poisonous snakes etc.

Niche construction and the 'extended phenotype'

A new basic evolutionary process, *niche construction*, has recently come to the fore (e.g. Laland et al., 2009). This takes account of the fact that many species, perhaps most, do not simply adapt to their environment as it is, but in one way or another *shape* that environment. This may initially be accidental – for example some herbivores may graze plants down so only certain species survive (the familiar example being grass, adapted to being chopped off from above by growing from the base rather than the tips) so the landscape they occupy actually becomes a more suitable niche for their talents to exploit. (The grass example also exemplifies positive co-evolution.) Humans are, of course, the arch niche-constructors, whether those niches are in the material or social world, or both.

Evolution of evolvability

Co-evolution was earlier described as an accelerant of evolution. Another accelerant is the *evolution of evolvability* (Dawkins, 2003). This refers to the fact that some organisms, generally the more complex ones, evolve sets of genes that facilitate the 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 will be more likely to harm than help, but variants that have a good chance of survival and possibly of conferring benefit. Kirschner and Gerhart (2005) describe how vertebrates and other advanced animals have a well-organised suite of genetic switches (certain DNA sequences which turn genes on and off during development to guide the formation of limbs, body segments etc). This is in effect a high-level computer language of structural design and development which sits on top of the fundamental code in 0s and 1s (or in DNA terms, codons of AAC, GTC etc). The upshot is that the organism in possession of such suites of genes and gene switches, can through mutation and sexual recombination of genes generate *orderly* variety of, say, limb length, shell shape, or neck musculature: candidates for adaptation that ab initio fit as a workable proposition with the rest of the body, rather than just a limp and squidgy mess. Kirschner and Gerhart entitle their book *The Plausibility of Life*, referring to the fact that the new proposals (or hypotheses) for survival are not nonsense strings but eminently sensible. A metaphorical way of looking at this is to consider how Mozart, even in his first drafts of pieces, could come up with beautiful music straight from the fingertips: he had the capacity to generate musically plausible variety.

Handling unpredictability

If biological evolution is about genetic learning, it can only learn about those aspects of the environment that stay constant over a long enough timescale to supply consistent selection pressures to shape the genes. Crude facts about the environment (such as the presence of gravity and the need to respect it by not falling out of tall trees) will be learned within a generation or two; subtler facts, or those which are stochastic and involve a lot of good or bad luck (such as how strong particular branches on particular types of tree are) will take longer. But however much invariance-knowledge the genes can extract from the environment, there will be sufficient 'slings and arrows of outrageous fortune' for the world to remain a very unpredictable place from the gene's eye view. *Cognitive* learning evolved to extract local invariances that remain valid for periods *less* than a generation – for example, that the trees around here (which grew rapidly in exceptionally warm conditions) are *not* to be relied on despite the superficially-reassuring girth of their branches. Unsurprisingly, those species that invest in building and maintaining brains capable of supporting cognitive learning tend to live longer. But again, there is no escaping the huge amount of unpredictability that remains to challenge the chances of any individual, or species, surviving and reproducing. Some of this unpredictability revolves around 'known unknowns', such as whether there is a lion around the next rock (or an IED under the next culvert), where the prey can, through inductive learning at a cognitive or genetic level, estimate some prior probability; some will be nonlinear 'unknown unknowns', like the outbreak of an entirely new disease, or the arrival of a new predator species with exceptional night vision. In an arms race context, the co-evolutionary feedback between, say, predator and prey means that one source of unpredictability is how the predator will respond to one's own new defence. The implications of unpredictability for terrorism are pretty self-evident and will be revisited in detail below.

With certain rare exceptions, humans are the only species that has evolved the capacity to go beyond inductive learning to explicitly *anticipate* hazards including those that originate from enemy action (and indeed, from enemy countermoves to one's own first moves). Two facilities underlie this capacity: perception and modelling of *causation*, and *theory of mind* (e.g. Whiten, 2006) – involving the perception of other people's point of view and specifically of their intentions. More generally, humans can imagine their own actions and their consequences both regarding the material world; and the reactions of other people and groups (not that they always get it right). As Popper put it (1972), we humans can let our ideas die in our stead – in other words, we discover the flaws in some action by imagining doing it and seeing how it could go wrong, rather than always having to learn the hard way.

Humans, too, have evolved to be unpredictable predators par excellence. Tooby and DeVore (1987) argue that the evolution of human intelligence allows us to mount evolutionary 'surprise attacks' which escalate the arms race against prey, such that the latter cannot keep up through their own biologically-evolving counter-adaptations which are more limited in scope and slower to emerge. When we try this against our human enemies, of course, the tactical advantage of surprise is still a potent one, but the enemy may be on the alert, may have anticipated some such move, and may have some surprises of their own in store.

The units of evolution

Terrorism and security are predominantly group-related activities. A major, unresolved argument in evolutionary science is over the existence of group-level selection. Early assumptions about particular adaptations being 'good for the *species*' were revealed as nebulous, a trend culminating in the perspective of adaptations being 'good for the selfish *genes*' (Dawkins, 1976). But authors including sociobiologist Edward O. Wilson (1975) argue for an independent, additional influence of group-level selection especially, but not exclusively, with reference to 'eusocial' species such as ants or humans where major manifestations of altruism seem to occur. Indeed, the more recent concept of multi-level selection (e.g. Okasha, 2006) covers not just evolution at the level of groups but incorporates a whole hierarchy of potential genetic/evolutionary units including also the intense symbiosis between the once-independent-living cellular components of eukaryote organisms (mitochondria and chloroplasts), and the functional interdependence of groups of genes. (To illustrate, the genes enabling perception and those enabling response are useless without one another, both being needed for their mutual survival and replication). Recent arguments on the status of multi-level selection are at http://edge.org/conversation/the-false-allure-of-group-selection and by D. Sloan Wilson (2012). Whether or not it is profitable to apply multi-level selection within biological evolution, the case for it is rather clearer with cultural evolution, to which we shortly turn.

The evolutionary algorithm – universal Darwinism

Dennett (1995) describes the variation-selection-inheritance process as the *evolutionary algorithm*; and like all such abstractions, suggests it can be applied, in pretty much the same form, to understand a wide range of other 'substrate' processes including the functioning of the immune system, thinking processes in the brain and instrumental (trial and error) learning. The perspective now known as 'Universal Darwinism' (e.g. Dawkins, 1983; Dietl, 2008) addresses the wider applicability of the algorithm. Cultural evolution is one such extension. But such is the power of the concept that we can even see explicit, recursive uses *within* human scientific/technological culture, in the form of genetic algorithms for finding the best combinations of new materials out of vast numbers of alternatives, and for coming up with solutions to complex mathematical and practical problems that cannot be directly computed. Some of these may even end up in the service of counter-terrorism, as with developing armour and optimising patrol/surveillance schedules.

'Darwinising culture'

Human culture is an evolutionary invention which has transformed our evolutionary capabilities – an example of the evolution of evolvability at many levels (including the example just given). As a concept, culture itself is notoriously hard to define (Spencer-Oatey, 2012). However, Richerson and Boyd (2005:5) offer a definition sufficiently generic and abstract to handle the diversity of human culture whilst meaningfully connecting with evolutionary concepts by: 'Culture is information capable of affecting individuals' behavior that they acquire from other members of their species through teaching, imitation, and other forms of social transmission. By information, we mean any kind of mental state, conscious or not, that is acquired or modified by social learning, and affects behavior.' Transmission of information through culture can occur both vertically – as an extra-genetic storage-and-retrieval system for knowledge accumulated over generations – and horizontally – as in peer-to-peer sharing. The transmission process may differ in significant ways from the standard biological model – for example, we may well envisage Lamarckian inheritance of acquired characteristics. Verbal encoding of knowledge has meant that the inheritance of such information has progressed from the low-fidelity reproduction of photocopies-of-photocopies, which rapidly become a blur, to a digital level of precision (just like DNA).This is particularly so, when know-how is represented as instructional procedures (Blackmore, 1999), for example in *how to make* an origami boat rather than, say, a *description* of the end product.

Human culture is of course the substrate for evolution of both terrorist-type ideologies and motives and their antagonists, and the tactics of attack and defence that are the subject of this chapter. Human culture has undoubtedly *itself* been evolving, and authors (e.g.

Richerson and Boyd, 2005) make the convincing case that the same evolutionary algorithm is at work (Aunger, 2002 entitles his anthology *Darwinizing Culture*). We can readily see processes of variation, selection and inheritance on scales ranging from catchy tunes, to designs for weapons, to religions. The concept of *memes* (Dawkins, 1976; Blackmore, 1999) treats such items and complexes of knowledge as replicators similar to genes, with ourselves and our technologies of information storage and dissemination as vehicles. From a meme's eye-view, we humans are their means of replication and memes are in competition with one another for brain-space and airtime. Sometimes, as with rival scientific hypotheses or extreme political ideologies memes are in conflict. Mechanisms of cultural replication are diverse and operate on different scales: Godfrey-Smith (2012) distinguishes imitative selection from the population of intra-cultural variants of behaviour (i.e. individuals choosing what/who to copy); cumulative cultural adaptation (e.g. adjustments to climate change); and the most macro-level, 'cultural phylogenetic change'. The last, for example, comprises radical discontinuities like the Neolithic revolution shifting societies from hunting/gathering to farming; and industrialisation.

The most recent such cultural phylogenetic change has arguably been the emergence of information technology, starting first with writing, moving on to printing, then to telecommunications, to computing and finally to the combined culmination of all these in the form of the Internet and other distributed systems. IT acts as a significant accelerant, in facilitating the development and dissemination of knowledge of terrorist and counter-terrorist practice in the material world – for example, how to anonymously move funds, or obtain assets such as explosives or detonators online. It also is inherently faster to evolve, since what is changing is code and code-based systems, with far fewer constraints than the material world imposes. Both terrorists and security can swiftly upgrade their software or hardware.

A diversity of arms races

Extending the scope of the co-evolutionary process from biological to cultural domains enables us to consider, and learn from, adaptive strategies and tactics in a range of natural, human and mixed arms races. These are listed in Box 1.

Box 1 A diversity of arms races

The natural world

Prey versus predators (confronters, trappers, dupers), mainly resembling crimes against the person – assault, robbery, homicide

Plant versus herbivore grazing- taking stored energy and materials from plants, resembling theft

Host versus parasite parasitism by insects, tapeworms etc – resembling theft

Host immune system infection by bacteria etc resembling robbery *versus pathogen* (overcoming host's defences)

Host immune system versus viral pathogen infection by viruses, resembling fraud or embezzlement in misappropriation of resources for and control of production; computer hacking (breaking access and control codes), and computer viruses themselves

Natural 'theft or robbery' within or between species – eg birds taking each others' nest sticks, or seizing others' food in mid-air attacks

Natural 'fraud' birds taking nectar by pecking a hole in the side of the flower to avoid the effort required to pass on pollen, orchids pretending to be female wasps and cheating males of reproductive effort and opportunity

Natural 'threat, assault' or killing - conflict over territory, mates, food

Humanity versus nature

Disease control hygiene, public health, inoculation, vaccination, antibiotics – resembling prevention of theft/robbery

Pest control rats etc spoiling/stealing crops or livestock, spreading human diseases, acting offensively – resembling prevention of theft/damage, disorder/nuisance

The human world

Military arms races and (counter)terrorism - arms versus armour, missiles versus electronic countermeasures, manoeuvrability – resembling assault and prevention of assault, homicide, disorder, theft of property, coercion, control of production

War-games and other simulation military training; evolution of new strategies in chess; computer-games of tactics and strategy

Economic warfare outgrowing the enemy or disrupting their economy (shading into real crimes like forgery or extortion)

Hacking

Espionage military/industrial, to steal information on resources, products, tactics and strategy, shading into theft of information/obtaining it in preparation for crime

Adapted from Ekblom, 1999

Military arms races demonstrate many examples of castles versus cannon, tanks versus bazookas, planes with electronic countermeasures versus missiles with counter-countermeasures. The military has only had a few millennia to evolve equipment and tactics but natural arms races rather longer. Co-evolution between predator and prey has at least 600 million years of experience to offer. The long struggle between pathogens and immune system has resulted in dynamic and adaptive strategies on each side. This has culminated in such sophisticated attackers as the HIV and smallpox viruses. Smallpox (Dunlop et al., 2003) has over 80 genes that interact with human defence mechanisms. In fact it has evolved counter-countermeasures to cope for example with a ‘virus alert’ chemical produced by infected cells, whose function is to warn nearby uninfected cells to activate their defences against virus attack. At some stage the smallpox virus ‘stole’ a length of DNA from the human host, which coded for the host cells’ receptor molecules for the virus alert chemical. When the smallpox virus invades a host cell it can therefore direct the cell to produce bogus receptor molecules which blot up the alert chemical. This masks the alarm signal so uninfected host cells are unprepared to resist the virus. It is ironic – but perhaps no coincidence – that one threat seriously considered by security services is that terrorists may acquire smallpox viruses from scientific repositories, the disease having been eradicated in the wild. Another interesting cross-link is the ‘infection’ model of the transmission of terrorist ideology or memes (Lafferty et al., 2008).

Vermeij (2008), quoted at the beginning of this chapter, argues that there is enough in common to these co-evolutionary struggles for human security to learn many useful lessons. But what, exactly, is ‘common’? Protracted competition and conflict between agencies which vary in their characteristics, adapt, differentially survive and replicate inherited or otherwise cumulatively developed characteristics. All the struggles (whether they are mediated by gene-based evolution or some other process such as rational thought) are pursued through development in tactics, strategy, and evolution of design. All involve exploitation of disturbances on one side and sufferance of their consequences on the other. The fundamental problem faced by the participants in each struggle is identical: (i) how to maximise positive consequences and minimise negative ones using the minimum of resources, (ii) when enemies or rivals are doing the same, (iii) against a background of disturbances which may favour, and/or be exploited, by one side or the other.

Co-evolution and terrorism

It’s now time to connect the basics and the details of evolution as just described, to terrorism and security, drawing on the insights of both genetic and culturally-mediated processes.

Beyond immediate survival

Arms races can seem an exercise in futility, an endless spiral of adaptation and counter-adaptation with first one party, then the other, gaining momentary advantage. Indeed, biological arms races have been described as a ‘Red Queen’s Game’ (from Lewis Carroll’s *Alice through the Looking Glass*), in which you must keep running merely to remain in the same place (van Valen, 1973; see also Schneier, 2012 for a detailed exploration of security implications). As Vermeij (2008) notes, in biology those lineages that cannot adapt to the latest weapons of predators are ecologically marginalised, though rarely completely extinguished (typically finding themselves modest niches as insectivores or bottom-feeders). A similar fate may await those societies that cannot, or will not, keep up in the arms race. At present, this may seem unlikely in Western industrial nations (although the rise of fascist dictatorships and communism in the 20th Century came close to eclipsing democracy) but in the long-term, who knows? And some human conflicts differ from natural ones in the deliberate pursuit of extermination of cultures or ethnic groups.

Unpredictability

According to Vermeij (2008) the greatest challenge to security, and the hardest to adapt to, is uncertainty. Terrorists readily exploit unpredictability in both their tactics and their strategic goals. That unpredictability relates to both 'known' and 'unknown' unknowns (respectively, for example, the time and place of the next AK47 attack, versus flying a passenger plane into a tall building). However, given the rapid horizontal spread of information among human groups the 'surprise attacks' rapidly cease to be surprising –silver bullets turn to lead. I previously referred to such episodes as 'breakouts with transient advantage' (Ekblom, 1999), like the invention of the tank in World War 1. In a related fashion, security measures also become obsolescent. The rate of obsolescence will depend on the kinds of offenders involved, their resources, and the kinds of social and technological changes that occur.

Variation, acceleration and the evolution of evolvability

Human ingenuity in generating variations, say, of methods of attack and defence is boundless. The 'dark side of creativity' is explored by Cropley et al., 2010; Cropley and Cropley, 2013). As in biological evolution, certain human inventions boost adaptive potential. Ekblom and Pease (2014) discuss this concept further in relation to adaptive criminals, citing for example 'script kiddies' (software kits enabling amateurs to generate effective computer viruses). Because of this acceleration in technologically-induced change the breathing space we get from a new preventive method before it is bypassed, is tending to diminish. Other cultural phylogenetic changes coming up which are potentially equally momentous are in artificial intelligence/robotics and biotechnology/genetic engineering. Taylor (2008) notes that DNA synthesis became more than 500 times faster between 1990-2000; it also became more automated and black-boxed so progressively less tacit knowledge is needed to employ the technology of synthetic genomics, which could be misused, say, in producing crop-destroying or ethnically-targeted pathogens.

Niche construction

Vermeij (2004) notes that all scales of economic life, from cells to ecosystems, from firms to states, influence their own evolution by being both the object of selection and the creator of the conditions of that selection. Terrorists and security organisations alike seek to foster supportive environments – whether this is for the ready provision of safe houses and moral support and the recruitment or corruption of security officials, or (on the opposing side) the public/political acceptance of intrusive surveillance.

Lessons from co-evolution

We are now in a position to draw together some lessons for how to handle the co-evolutionary nature of terrorism. As I previously observed (Ekblom, 1997, 1999) regarding crime in general, a perusal of natural history sources (and a long history of watching wildlife programmes by David Attenborough and others with a 'security affordance' mindset) revealed the difficulty of coming up with specific, tangible interventions from nature that humans had not already culturally re-invented for themselves. The classic example here is the lizard's detachable tail (e.g. see www.youtube.com/watch?v=rQkWn4jodbY), designed to distract predators: British police uniform ties detach at the neck to avoid strangulation by criminals.

More promising are lessons of biological and human design and engineering relating to use of materials, structures and mechanisms, and how to trade off the conflicting requirements between security and, say, effort in foraging or in constructing convenient but defensible buildings. These are explored below.

But the main theme of this chapter, and the most promising level of approach, is at the level of campaigns, not individual battles – where victories are soon eroded by adaptive terrorists and/or technological game-changers – by running or avoiding arms races.

Running arms races

The following list of suggestions developed from my own earlier thinking (Ekblom, 1997, 1999) significantly supplemented by other authors. Inevitably there is some overlap between the headings. In all that follows, similar opportunities and constraints apply to the terrorists and to the security sides: hence, we will be flipping perspectives quite often.

Before proceeding, I should emphasise that each human or human/nature struggle from which lessons may be drawn has its own ethical issues – what is acceptable in war, espionage or pest control is not necessarily appropriate for civil security. Application of transferred knowledge must therefore be sensitively done.

Handling unpredictability of terrorists

Terrorists have made a thing of unpredictability, both for good tactical reasons, and also for wider strategic benefit to convey an image of superiority. How does biological evolution handle unpredictability? Vermeij (2008: 30-35), drawing on an encyclopaedic view of evolutionary strategies, lists the following, with my own interpretations in brackets:

- Passive tolerance
- Active engagement with the enemy
- Striving to increase predictability by observing the habitat over longer periods and wider spatial tracts, and investing in the intelligence to analyse a greater proportion of invariance (Likewise, the security side can limit observation of its own defensive tactics and assets. Users of online banking are familiar with the technique of partial use of passwords as in 'enter the 3rd and 6th digits'.)
- Being unpredictable oneself (as with rarity, dispersal, the zigzag flights of moths aiming to confuse bats, or Hannibal Lecter's observation on the locations of the serial killer's victims in *The Silence of the Lambs* movie 'Clarice, doesn't this random scattering of sites seem *desperately* random?'). The accumulation of a diverse stock of 'silver bullets' on the security side may be useful here. The development of military counterparts by Lockheed's 'Skunk Works' design facility is described by Rich and Janos (1994).)
- Quarantine, isolation and starvation (e.g. Russia's scorched earth strategy against Napoleon's invading army, and 'hearts-and-minds' campaigns to deny terrorists support)
- Redundancy

- Adaptability, for example through semi-autonomous components under weak central authority, flexibility and rapid communication between parts, and combinatorial generation of variety

Prescott (2008) also suggests the importance of developing *flexible responses* which do not fire every time with consequent cost and disruption (thinking for example of the feed-or-flee choice that suspends foraging birds on a knife edge of decision-making between breadcrumbs and lurking cat). Also, of developing adaptive/security responses which are *generalised*, so they are less likely than a specialised defence, to be caught out by a new one-off attack (an example being our generalised 'innate immune system' which complements the highly-specific antibody-based one that must learn about each individual pathogen).

Madin and Johnston (2008) note that *insurance* is an approach to mitigation of unpredictable disasters. In biological terms this is a form of 'preadaptation' to novel threats. In human terms, insurance can be both individualistic (e.g. storing food in case of an electricity disruption) or mutual. With the latter, however, insurance companies strongly prefer to cater only for those risks where past actuarial data is available, often excluding coverage of terrorist attack and leaving any compensation to governments.

Anticipation

Despite the challenging nature of terrorist unpredictability, 'investing in intelligence' enables humans to undertake some modest anticipation. Anticipation can cover both terrorists' first moves and their countermeasures, i.e. adaptations to the security response. It can also cover forecasting what might come up on the preventive side.

- The methods of foresight/horizon scanning (e.g. see DTI (2000) and Collins and Mansell (2004) can be applied to terrorism and its control. Experience from that field indicates the risk of betting on very specific predictions; instead, the approach is to identify a wide envelope of possible futures and ensure security plans are valid across them all.

- Techniques like *technology road-mapping* can identify upcoming inventions, and the steps that still need to be taken before some tool or weapon becomes a practical proposition for terrorists or security. (The same applies to anticipating new viral infections – where health researchers have determined, say, that a particular pig-hosted virus strain is only two mutations away from acquiring human-to-human transmissibility.)

- The TRIZ approach to inventive principles, further discussed below, has accumulated a set of evolutionary trends in invention that may be used to identify where, in some specific engineering domain (e.g. armour), new inventions may be expected, and what kind of invention that might be (e.g. move from rigid connection to flexible link).

- *Crime impact statements* can be developed for proposed new tools, trading practices etc, identifying aspects which may supply new opportunities for terrorists and/or render existing preventive measures obsolete. These can be based on crime prevention theory (Ekblom 2002b) or practice principles (Monchuk and Clancey 2013).

- We can encourage a 'think terrorist' mindset to consider their next adaptive moves. The *Misdeeds and Security framework* (Ekblom 2005, 2008) helps to systematically ponder ways in which new technology, systems, procedures etc. can generate opportunities for offending: Misappropriation (theft), Mistreatment (damage or injury), Mishandling (e.g. smuggling), Misbegetting (counterfeit), Misuse (as tool or weapon) and Mistake (e false alarms or wrongful accusation). Counterpart categories enable similar anticipation of emerging opportunities on the security side.

- It is important to identify and block as many terrorist countermeasures as possible, perhaps through the use of 'attack trees' (e.g. Schneier, 1999) which tease out the widest range of alternative methods by which they can realise their attack), but beware diminishing returns and disproportionate 'over-engineering' of solutions.

- We must anticipate that even the best preventive method will have a limited lifespan, the aim being to develop ones slower to become obsolete. Military co-evolution supplies the concept of exploiting momentary advantage, e.g. that afforded by a new kind of fortification: useful for a while, even though it is soon countered by a new projectile.

Coping with the limits of anticipation

- Where anticipation fails, we should gear up for faster response to handle 'crime harvests' (Pease, 2001), by accelerating the learning curve for designers of preventive measures. Setting up learning paths, involving systematic assembly of attack incident information of the right kind (e.g. how the lock was broken/ the security code was obtained/ circumvented), can guide suitable adjustments. In effect this is quickly shutting the stable door before the *next* horse bolts.

- More generally, we should anticipate design failure or obsolescence by incorporating the possibility for remedy, making the inevitable retrofit solution easier, as discussed under design, below.

Adaptation in general

Having the capacity to evolve, learn and upgrade is as important as possessing any individual defensive feature which gives temporary advantage. Since adaptation, and the adaptability of both terrorists and the security side, are central to exploiting (co-)evolutionary perspectives on terrorism, we should understand how it works in some depth. Here are some aspects worth considering:

- Blumstein (2008) maintains that we must develop better understanding of how species respond to novel threats. In particular, do these require truly novel responses, or can we adapt responses that have evolved for some, possibly everyday, purpose (the technical term is 'exaptation)? A similar point is made by Johnson and Madin (2008) who note that those adaptations that can be co-opted to alternative uses, protect against both commonplace and unpredictable threats. Counter-terrorism strategies should likewise seek versatility rather than pared-down specificity to known threats.

- Adaptation often involves knowledge spread, or its equivalent, and the appropriate defence is to minimise opportunities for offenders to learn or pass on that learning. In biological evolution, exchange of plasmids enables bacteria to horizontally swap DNA 'knowledge' including that coding for antibiotic resistance. Whether any bacteriologists have discovered inhibitors of such transfers would be interesting to discover.

- Technology transfer in particular may be prevented by 'capture-proofing' equipment. The equipment is made difficult to operate without training; spares are difficult to obtain; it self-destructs, or stops working without authorisation. This strategy applies to the literal transfer of military weapons to terror attacks. It could also apply to the 'hacking' of everyday equipment and applications which could be converted to terrorist misuse.

- Given that knowledge of target and procedural vulnerabilities, and of methods of attack, once developed, are likely to proliferate rapidly over the Internet, it is necessary, further, to devise preventive measures that are difficult for offenders to overcome, even if they know how they work (some encryption systems rely on offenders not possessing massive computing power and/or infinite time, although quantum computing may invalidate this).

- Security measures should not be specified as fixed construction standards, like incorporating particular types of lock or using particular resistant materials, but to *performance* standards (e.g. 'the lock must withstand 20 Newton force and resist expert picking for 20 minutes'). This slows obsolescence, and frees designers to devise diverse solutions rather than constraining them to a single one whose vulnerabilities can quickly be transmitted among attackers. It also prevents manufacturers from absolving themselves from responsibility by 'designing down' to minimum construction specifications. Terrorists faced with uncertainty about what preventive systems they may find in the next place they reconnoitre or attack, are at a tactical and psychological disadvantage. Ekblom and Hirschfield (2014), in identifying 11 generic mechanisms of influencing terrorists at an attack site, thus distinguish between 'deter-known' and 'deter-unknown'.

- Adaptability also implies avoidance of *phylogenetic constraint* (Raup, 1993). This is where an evolved security or defence system becomes so complex and integrated, that radical redesign is impossible, only minor adjustment. A related issue is developing ways to cope with rapid change. In both cases, we must discover which kinds of security adaptations have preserved flexibility, and which have led to rigidity and constraint (Vermeij, 2004). More generally, we on the security side want to avoid evolutionary blind alleys of prevention; or conversely, exploit those blind alleys by shaping offenders into them, causing them to specialise in ways which are slow and costly to reverse (but we should also beware of *adverse* shaping of terrorists towards more harmful methods of attack).
- Unfortunately, the 'plus ça change' hypothesis (Sheldon, 1996) suggests that the kind of rapidly-changing social/technological environment humans have now created, is more likely to favour generalist rather than specialist adaptive strategies – a lesson that applies to both sides.

- Another constraining factor is *field obsolescence* – that is, where we have developed a new, more secure product or system but it takes time and money for the current, less secure, versions to be replaced. The classic example is the older generation of cars lacking steering locks (Webb, 1994), where the half-life for replacement was about a decade. Tackling this problem can involve a switch from vertical to horizontal transmission of change such as 'broadcast' security upgrades of the kind we get with our software operating systems, or product recalls for cars. With material products like buildings, we can design-in the capacity for easy upgrades such as more secure door fittings. Rather than over-engineering the doors on every school or government office, say, we can design the door frames to swap-out higher-security fittings only where and when necessary, in the light of threat assessments.

- A strategic point on *resources* is made by Johnson and Madin (2008), who argue that adaptations require substantial allocation of energy and time, constraining competing functions under a fixed budget. A complementary strategy to the 'exaptation' of routine security measures to extreme but rare terrorist attacks, mentioned above, is to ensure that security measures designed to address these should also confer more day-to-day benefit in, say, crime control or transportation safety. Another resource management strategy Johnson and Madin identify derives from the immune system's ability to tick over at a low level of energy expenditure until it encounters a threat, when it can rapidly ramp up a highly-targeted response. This fits nicely with attempts to provide graduated 'bronze, silver and gold' responses to repeat victimisation (Chenery et al., 1995). They also note the dangers of inappropriate or over-reaction, where immune responses can drain the organism's resources, with obvious lessons for security and life in general. The balance between active and passive resistance is therefore tricky to determine (Vermeij, 2008).

- Johnson and Madin further state the importance of allocating *rolling budgets*, rather than one-off lump sums, to security. This is part of a wider evolutionary/ecological analysis of the sources of resistance to adaptive change: we humans normally wait for a disaster to trigger significant action rather than anticipate and avoid it. In this connection, Johnson and Madin's contribution deserves close attention if we wish to avoid anticipation failure and/or implementation failure. Rolling budgets support ongoing anticipation, maintenance of expertise and information flows, and perhaps '*pipelines*' of a succession of new security measures ready to put into place in the expectation that current ones are a wasting asset and will soon become outdated. This approach is well-developed in, for example, the domain of credit cards and pay-tv services.

Adaptation: redundancy and resilience

Sagarin and Taylor (2008), Prescott (2008) and especially Vermeij (2008), identify several interlinked principles from evolutionary history which confer resilience. These include redundancy; distributed rather than centralised functions, with diffuse control relying on multiple, semi-autonomous units rather than hierarchy; integration; and flexibility. Likewise

Edwards' (2009) review of resilience calls for society not just to resist and respond to current challenges, but to anticipate and be ready to adapt to, future ones.

Adaptation: the importance of variety
Variety of preventive measures, and the ability to generate *plausible* variations (see next section), is a vital challenge to terrorist tactics. Uniform security systems or devices are often installed for reasons of economy of funds and effort, but – like crop monocultures facing a new mutant fungus – this could be a case of 'crack one security measure, crack them all'. The more genetically *diverse* the potential hosts of disease, the more restricted is the scope for any one type of pathogen to attack them (Wills, 1996; Colinvaux, 1980).

To further exploit variety, it is useful to act on several fronts simultaneously (like multiple antibiotic regimes), e.g. hardening target assets whilst improving surveillance, to introduce some redundancy and/or synergy into security measures.

Adaptation: design, innovation, creativity and anti-creativity
Producing variety equates to innovation. Arms races seek to out-innovate the opposition. Innovation is about the successful exploitation of new ideas; creativity is the generation of new ideas; and design is what links creativity and innovation, shaping ideas to become practical and attractive propositions for users or customers, i.e. creativity deployed to a specific end (HM Treasury 2005:2). We have already seen how natural systems can generate plausible designs, and noted the contribution of theory (specifically, crime science theory) in supplying that plausibility. This is irrespective of whether that theory originates in a human scientific process, or as accumulation of genetic hypotheses about what works for this species in this habitat. We have also acknowledged the significance of the evolution of evolvability: the human capacity to innovate through design is an example of this bootstrapping process, supported by a combination of genetic and culturally-mediated accumulation and transmission of knowledge and know-how.

Unfortunately innovative capacity is as much available to terrorists as to the security side (Ekblom and Pease, 2014). But innovative capacity is best exploited through the consistent employment of the design *process*, not by lifting individual innovations off-the-shelf as products to deploy in individual evolutionary surprise attacks; and here, the security side should be able to gain intellectual advantage if it applies sufficient, sustained attention and resources to design.

In biological evolution, the exploration of fitness space is constrained to the local and the immediately advantageous, as described. Only human learning and cultural evolution are capable of looking, and leaping, across the valley separating a local fitness maximum from a far higher peak. We are able to do this because we can take the generation of variety, and the testing of possible responses, 'offline' from immediate biological survival (a re-phrasing of Popper's point cited above) and into an imaginary and/or otherwise protected world. Here, evolution still operates, with our theory, and our prototype practical realisations, exposed to the selection pressure of searching appraisal and rigorous evaluation; but with a degree of tolerance that allows failures to be resurrected and modified rather than having to be reinvented all over again. Only when such innovations have reached a certain level of plausibility are they deployed in the field and exposed to real-world selection pressures (or not, as the discussion of evaluation reveals, below). Design embedded in a research and development process offers a systematic way of doing this.

Of course, the richer the stock of theoretical principles to draw on, and the more readily these can be accessed and recombined, the better-equipped are designers to generate plausible candidate innovations. This is equivalent to the diversity of genes we enjoy for protection against pathogens – and those they possess against us, as already described for smallpox. Theoretical frameworks, especially those that are comprehensive, integrated and well-articulated, can be useful here. Examples aspiring to these standards are the Conjunction of Terrorist Opportunity on causes and interventions against terrorist events (Roach et al., 2005 and see chapter by Ekblom, Sidebottom and Wortley); the Misdeeds and Security Framework (Ekblom, 2005) for identifying generic crime/terrorism risks involving designed products/technologies; the risk factors approach of terrorist target selection known as EVIL DONE (Clarke and Newman, 2006); and the theoretical/practical Security Function Framework for specifying security designs (Meyer and Ekblom, 2011). Most are summarised in Ekblom (2014).

Many terrorist groups allow themselves a free hand with violence and intrusion on people's lives. But the actions, and defensive equipment, open to the security side to create and deploy, are far more constrained. We must respect diverse 'requirements tradeoffs' between security and human rights, sustainability, aesthetics, economic growth, and avoidance of fear and fortification. The essence of design is to identify and creatively resolve such tradeoffs. (The huge metal 'Arsenal' sign at London's Emirates football stadium is the classic example, being designed to covertly protect against explosive-laden trucks ramming into the stadium.) This echoes a similar process in biological evolution: Prescott (2008) notes that extant organisms are descendants of those that got the balance right between security and other survival priorities. High-performance natural predators like cheetahs must trade off speed against the strength/weight to fend off hyenas wishing to steal their kill. Likewise such tradeoffs routinely occur in commercial and military engineering. Military aircraft require a combination of offensive and defensive capabilities, and face severe and complex tradeoffs of weight/ manoeuvrability/ damage resistance/ damage tolerance/ reliability/ cost.

Articulating and resolving tradeoffs is highly-developed in engineering design, for example through TRIZ, the theory of inventive principles (Ekblom 2012b; and see www.triz-journal.com/triz-what-is-triz/). This has identified some 39 generic 'contradictions,' and 40 'inventive principles' previously used to resolve them; and through 'optimisation algorithms' (e.g. Science Daily, 2015). The identification of 'script clashes' (Ekblom, 2012b), generic procedural conflicts between offenders and preventers (e.g. pursue versus escape, conceal versus reveal, ambush versus alert) is another potentially useful approach for focusing design.

One specific way design can address the need to favour the good guys over the bad is in making products, places and procedures capable of *differentiation* – i.e. 'user-friendly, abuser-unfriendly'. The capture-proofing of weapons, previously described, is one such instance. The most strategic differentiation of all is to find ways of making it hard for terrorists to undertake design and innovation without putting brakes on the security designers and indeed those aiming to design for the rest of civil society. Space precludes coverage of how to block the dark side of creativity (e.g. see Dolnik, 2011) but essentially the strategy is to differentially throw into reverse, all those aspects of business and society that encourage and support design.

Design, however, goes beyond the steady generation and improvement of plausible ideas – important though this is – and rather than make do with compromise makes intuitive, ingenious leaps out of the initial frame of thinking to overcome requirements conflicts and bypass or relax tradeoffs. Sometimes this draws on new technology. An example is the arrival of the internal combustion engine, which enabled warfare to be conducted using armour *and* mobility combined (the tank), whereas in the horse-powered era it was one *or* the other. A 'jumping' strategy that occasionally occurs in the natural world is, as mentioned, through new symbiotic relationships that radically improve the resources available to a duo of species. Partnerships in the human world, of course, also bring together diverse resources and we must foster those on the security side whilst seeking to disrupt those on the terrorist side, for example by sowing distrust.

Designers also tend to question the assumptions behind the problem as put to them, by the clients. They advocate *reframing* of problems and solutions (see Lulham et al., 2012 on reframing the anti-terrorist litter bin). This is related to the 'system operator/ nine windows' technique within TRIZ that encourages engineers to look beyond the immediate problem domain to consider intervening at an earlier or later point in time, up a level to a super-system or down to a subsystem. At a strategic level, we might wish to avoid becoming locked into a pointless competitive loop of design and counter-design, for example in surveillance, counter-surveillance, counter-counter-surveillance… Therefore, we should prepare to deliberately jump out of the loop. Where technology currently favours terrorists, deliberate switching of security effort to conventional investigative security/law enforcement, manguarding and offender-oriented approaches may be more appropriate until the balance of power reverts.

A last point about design is the utility of investing in the *infrastructure* of design against terrorism and crime. This involves creating an environment of theory, knowledge gathering and dissemination, understanding, and perhaps, even, the law which can empower designers more generally to gear up to tackle new problems as they emerge, and hopefully anticipate them too. However, as usual we must beware design infrastructure which offenders can misuse. The 3D printer, originally a design prototyping tool, has 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).

Knowledge and evaluation

Knowledge-related processes play a significant part in the success, or otherwise, of security activity. Variety of response can derive from the richness of generative theory – theory which is plausible because it has been tested across a diversity of contexts. Variation also derives from empirical research, for example on the decision-making, scripts and perpetrator techniques of terrorists and other offenders, and an understanding of the mechanisms of attack and resistance, whether in humans, bacteria or larger pests like rodents. (Integrated frameworks, as discussed above, draw theories together for users and designers.)

A vital domain of knowledge, relevant to anticipation of attack methods and design of preventive measures, is *knowing the terrorists.* This may range from understanding their likely choice of targets, through to the constraints they operate under, to the *resources for offending* (Ekblom and Tilley, 2000; Gill, 2005) that terrorists have access to now or that they may acquire in future. Resources may range from mental (courage, skill and tactical procedures, techniques for 'neutralisation' (Sykes and Matza 1957) of norms or empathic processes) to material (weapons, logistics etc.) and social (moral and material support).

But it is pointless risking the cost and effort we invest in developing, producing, implementing and using security-oriented designs, if their principles are not *evidence-based*. Applied researchers set up their own selection pressures in the form of *evaluation* and evaluation criteria to test the fitness of particular practices (and perhaps of the theories that have generated those practices). Unfortunately, in the 'what works?' literature, a systematic review (Lum et al., 2009) of over 20,000 accounts of anti-terrorist strategies, implemented at some unknown but doubtless enormous total cost, yielded only *seven* moderately rigorous evaluations from which policy-relevant conclusions might be drawn.

Of course, there is unique difficulty in applying traditional social/operational research methods to evaluate interventions intended to block extremely rare events; but there is no escaping that this is shameful neglect. It misses an enormously significant opportunity for exploiting the advantages of the 'big' side in asymmetrical conflict over the 'little' side, namely systematic research and the development of advanced, rational approaches to counter-terrorism, much as science is the only hope we have for keeping up with the evolution of antibiotic resistance. (The significance of that particular arms race, and the need for a sustained and sophisticated drive to implementation, has recently been acknowledged at high level in society in the shape of the £10m 2014 Longitude Prize (www.bbc.co.uk/news/science-environment-28027376).)

It is vital nonetheless to develop alternatives to conventional evaluation. Red teaming and attack testing, including through simulations rather than the (often expensive) field exercise, are important to continue to develop, helping both to identify possible offender countermeasures and to assess the performance of security systems against them. But these tend to be rather atheoretical, so boosting them with crime science theory, attention to the detailed causal mechanisms (Tilley, 2006; Ekblom, 2011) of failure and success, and deep understanding of the tactical procedures and goals of terrorists ('scripts' – Cornish, 1994) is a necessary extension.

Beyond variation, *replication and inheritance* is a difficult issue for preventive knowledge. Even when copying preventive 'success stories' as judged by good-quality evaluations, over-emphasis on *literal* fidelity in replicating the action precisely is actually quite poorly adaptive to new contexts. Unfortunately, this is amply illustrated by the literature on 'implementation failure' in crime prevention (Tilley, 2006; Ekblom, 2002, 2011). Successful replication – and innovation, where there is nothing in the trusted knowledge bank to copy

– depends more on fidelity of generative *principles* of the kind based on theoretical knowledge of causal mechanisms.

As a final point it may well be easier to identify 'What *Doesn't* Work' – certainly every successful terrorist attack (or successful subsidiary step in such an attack) should be as instructive as it is unwelcome for the security side. And bearing in mind the turnover of the arms race we must continually test and weed even those security measures that have worked up to now (Blumstein, 2008).

Conclusion

Threats from lethal, destructive terrorist attacks will never go away, and no adaptations to them can be perfect, nor predictions reliable. The 'War on Terror' can never be won. But however futile the Red Queen's Game seems, we cease to run it at our peril. Studying evolution, and more specifically co-evolution, gives us access to knowledge of generic solutions to conflict and competition that have been tried and tested (and had their limitations and contextual supporting conditions revealed) in the very long run, over a wide range of 'universal' ecological problems faced by natural organisms of all kinds; and recapitulated over a far shorter timescale by humans in conflict with 'nature' and each other. Crime science, engineering science and design together with attention to evaluation of effectiveness, and sophisticated knowledge management, can all contribute to this repertoire through which we can hopefully out-innovate adaptive terrorists whilst preserving our cherished values and serving the widest range of societal priorities in a proportionate way. As noted, studying co-evolution across a range of natural, human and mixed Darwinian struggles may or may not generate specific preventive tactics and strategies. But as a fresh way of thinking about the problem of terrorism and how to combat it in the medium-to-long term, derived from some 600 million years of experience, it is surely worth adopting.

But we must also develop, and exploit, our unique ability to jump out of the loop. Solving intergroup conflicts politically is a strategy probably not found outside the realm of advanced primates. Unlike pretty much all other living creatures, we humans do have another avenue to pursue in parallel to, but not instead of, the counter-terrorism arms race.

References

Anton, S., Potts, R. and Aiello, L. (2014). Evolution of early Homo: An integrated biological perspective. *Science*, 345/6192.

Aunger, R. (ed.) (2000). *Darwinizing Culture. The Status of Memetics as a Science.* Oxford: Oxford University Press.

Bassouni, C. (2002). Legal control of international terrorism: A policy-oriented assessment. *Harvard International Law Journal* 43/1: 83–104.

Blackmore, S. (1999). *The Meme Machine.* Oxford: Oxford University Press.

Blumstein, D. (2008). Fourteen security lessons from antipredator behaviour, in R. Sagarin and T. Taylor (eds.), *Natural Security: A Darwinian approach to a dangerous world*. Berkeley: University of California Press.

Bowlby, J. (1969). *Attachment and Loss*. New York: Basic Books.

Campbell, D. (1974). Evolutionary epistemology, in P. Schlipp (ed.), *The philosophy of Karl Popper*, 413–63. LaSalle, IL: Open Court.

Carrier, D. and Morgan, M. (2014). Protective buttressing of the hominin face. *Biological Reviews* Online first version.

Chapman, J. (2004). *System Failure: Why Governments Must Learn to Think Differently*. London: Demos.

Chenery, S., Holt, J. and Pease, K. (1997). *Biting Back II: Reducing Repeat Victimisation in Huddersfield*. Crime Detection and Prevention Series Paper 82. London: Home Office.

Clarke, R. and Newman, G. (2006). *Outsmarting the Terrorists.* London: Praeger Security International.

Cohen, L., Vila, B. and Machalek, R. (1995). Expropriative crime and crime policy: An evolutionary ecological analysis*. Studies on Crime and Crime Prevention* 4:197–219.

Colinvaux, P. (1980). *Why Big Fierce Animals are Rare*. Harmondsworth: Penguin.

Collins, B. and 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, in R. Clarke (ed.) *Crime Prevention Studies 3.* Monsey NY: Criminal Justice Press.

Cropley, D. and Cropley, A. (2013). *Creativity and Crime: A Psychological Analysis.* Cambridge: *Cambridge University Press.*

Cropley, D., Cropley, A., Kaufman, J., and Runco, M. (2010). *The Dark Side of Creativity.* Cambridge: Cambridge University Press.

Darwin, C. (1859). *On the Origin of Species*. London: John Murray.

Dawkins, R. (1976). *The Selfish Gene*. Oxford: Oxford University Press.

Dawkins, R. (1996). *Climbing Mount Improbable*. New York: Norton.

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.

Dietl, G. (2008). Selection, security and evolutionary international relations, in R. Sagarin and T. Taylor (eds.), *Natural Security: A Darwinian approach to a dangerous world*. Berkeley: University of California Press.

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

Dolnik, A. (2011). *Understanding Terrorist Innovation*. London: Routledge.

Dunlop, L., Oehlberg, K., Reid, J., Avci, D. and Rosengard, A. (2003). Variola virus immune evasion proteins. *Microbes and Infection*, 5/11: 1049–56.

Edwards, C. (2009). *Resilient Nation*. London: Demos.

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* 214: 249–265. www.veilig-ontwerp-beheer.nl/publicaties/gearing-up-against-crime/at_download/file accessed 17 January 2015.

Ekblom, P. (1999). Can we make crime prevention adaptive by learning from other evolutionary struggles? *Studies on Crime and Crime Prevention* 8/1: 27–51. www.veilig-ontwerp-beheer.nl/publicaties/can-we-make-crime-prevention-adaptive-by-learning-from-other-evolutionary-struggles/at_download/file accessed 17 January 2015.

Ekblom, P. (2002a). From the source to the mainstream is uphill: the challenge of transferring knowledge of crime prevention through replication, innovation and anticipation, in N. Tilley (ed.) *Analysis for Crime Prevention,* Crime Prevention Studies 13: 131–203. Monsey, N.Y.: Criminal Justice Press/ Devon, UK: Willan Publishing.

Ekblom, P (2002b). 'Future Imperfect: Preparing for the Crimes to Come.' *Criminal Justice Matters* 46 Winter 2001/02: 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. (2008). Designing Products against Crime, in R. Wortley and L. Mazerolle (eds) *Environmental Criminology and Crime Analysis*. Cullompton: Willan.

Ekblom, P. (2011). *Crime Prevention, Security and Community Safety Using the 5Is Framework.* Basingstoke: Palgrave Macmillan.

Ekblom, P. (2012a). Book review of ‘Liars and Outliers: Enabling the Trust that Society Needs to Thrive’ by Bruce Schneier (Wiley). At *Criminal Law and Criminal Justice Books*, September, retrieved on 19 January 2015 from http://clcjbooks.rutgers.edu/books/liars_and_outliers.html.

Ekblom, P. (2012b). 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,* 163–198. Cullompton: Willan.

Ekblom, P. and Hirschfield, A. (2014). Developing an alternative formulation of SCP principles – the Ds (11 and counting). *Crime Science*, 3: 2.

Ekblom, P. and Pease, K. (2014). Innovation and Crime Prevention, in G. Bruinsma and D. Weisburd (eds), *Encyclopedia of Criminology and Criminal Justice*. New York: Springer.

Ekblom, P. (2014). Design and security, in M. Gill (ed.) *The Handbook of Security (2nd Edn),* 133–156*.* Basingstoke: Palgrave MacMillan.

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

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.

Guerette, R. and Bowers, K. (2009). Assessing the extent of crime displacement and diffusion of benefit: A systematic review of situational crime prevention evaluations. *Criminology*, 47/4:1331–1368.

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

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.

Lafferty, K., Smith, K. and Madin, E. (2008). The infectiousness of terrorist ideology: Insights from ecology and epidemiology, in R. Sagarin and T. Taylor (eds.) *Natural Security: A Darwinian Approach to a Dangerous World*. Berkeley: University of California Press.

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

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

Lum, C., Kennedy, L. and Sherley, A. (2009 update). *The Effectiveness of Counter-Terrorism Strategies: A Campbell Systematic Review.* Oslo: Campbell Collaboration.

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

Monchuk, L. and Clancey, G. (2013). A comparative analysis of crime risk assessments and their application in Greater Manchester and New South Wales. *Built Environment*, 39: 74–91.

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

Okasha, S. (2006). *Evolution and the Levels of Selection*. Oxford: Clarendon.

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

Popper, K. (1972). *Objective Knowledge: An Evolutionary Approach.* Oxford: Clarendon.

Prescott, E. (2008). Corporations and bureaucracies under a biological lens, in R. Sagarin and T. Taylor (eds.) *Natural Security: A Darwinian Approach to a Dangerous World*. Berkeley: University of California Press.

Raup, D. (1993). *Extinction: Bad genes or bad luck?* Oxford: Oxford University Press.

Rich, B. and Janos, L**.** (1994). *Skunk works*. London: Warner Books.

Richerson, P. and Boyd, R. (2005). *Not by Genes Alone: How Culture Transformed Human Evolution*. Chicago: University of Chicago Press.

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

Roach, J., Ekblom, P. and Flynn, R. (2005). The Conjunction of Terrorist Opportunity: A framework for diagnosing and preventing acts of terrorism. *Security Journal* 18/3: 7–25.

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

Schneier, B. (1999). Attack trees. *Dr. Dobb's Journal,* December. www.schneier.com/paper-attacktrees-ddj-ft.html accessed 21 January 2015.

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

Science Daily (2015) Optimizing optimization algorithms: Getting best results when approximating solutions to complex engineering problems. 21 January 2015. www.sciencedaily.com/releases/2015/01/150121155545.htm accessed 22 January 2015.

Sheldon P. (1996). Plus ça change – a model for stasis and evolution in different environments. *Palaeogeography, Palaeoclimatology, Palaeoecology* 127: 209–227.

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

Spencer-Oatey, H. (2012). What is culture? A compilation of quotations. GlobalPAD Core Concepts. Available at GlobalPAD Open House http://go.warwick.ac.uk/globalpadintercultural downloaded 15 January 2015.

Sykes, G. and Matza, D. (1957). Techniques of neutralization. *American Sociological Review,* volume 22, 664-70.

Tilley, N. (2006). Knowing and doing: Guidance and good practice in crime prevention', in J. Knutsson and R. Clarke (eds) *Putting Theory to Work: Implementing Situational Prevention and Problem-Oriented Policing*, Crime Prevention Studies 20. Monsey, New York: Criminal Justice Press.

Toffler, A. (1970). *Future Shock.* New York: Random House.

Tooby, J. and 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.

UK Cabinet Office (2010). *UK National Security Strategy 2010* accessed 15 January 2015 from www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty

van Valen, L. (1973) A New Evolutionary Law. *Evolutionary Theory* 1: 1–18.

Vermeij, G. (1999). Inequality and the directionality of history. *American Naturalist*, 153: 243–253.

Vermeij, G. (2004). *Nature: An Economic History.* Princeton: Princeton University Press.

Vermeij, G. (2008). Security, unpredictability and evolution: Policy and the history of life. In R. Sagarin and T. Taylor (eds.) *Natural Security: A Darwinian Approach to a Dangerous World*. Berkeley: University of California Press.

Webb, B. (1994). Steering column locks and motor vehicle theft: Evaluations from three countries, in R. Clarke (ed.), *Crime Prevention Studies*, 2: 71–89. Monsey, N.Y.: Criminal Justice Press.

Whiten, A. (2006). The place of 'deep social mind' in the evolution of human nature, In M. Jeeves (ed.) *Human Nature*, 207–22. Edinburgh: Royal Society of Edinburgh.

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.

Wills, C. (1996). Safety in diversity. *New Scientist* 23 March: 38–42.

Wilson, D. Sloan (2012). Clash of paradigms: Why proponents of multilevel selection theory and inclusive fitness theory sometimes (but not always) misunderstand each other. Downloaded from http://socialevolutionforum.com/2012/07/13/david-sloan-wilson-clash-of-paradigms-why-proponents-of-multilevel-selection-theory-and-inclusive-fitness-theory-sometimes-but-not-always-misunderstand-each-other/ on 15 January 2015.

Wilson, E. O. (1975). *Sociobiology: The New Synthesis.* Cambridge, Mass.: Harvard University Press.