Eur J Crim Policy Res (2008) 14:61–87
DOI 10.1007/s10610-007-9041-8

What Do You Mean, 'Is It Secure?' Redesigning Language to be Fit for the Task of Assessing the Security of Domestic and Personal Electronic Goods

Paul Ekblom · Aiden Sidebottom

Published online: 27 June 2007

Abstract Project MARC aimed to develop a mechanism to assess the risk of theft of consumer electronic products, and their corresponding security; and to devise an operational scheme for EU level to influence manufacturers to make their products less criminogenic. The project encountered serious difficulties in the assessment process due, among other things, to limitations of concepts and terminology. This paper describes and analyses those limitations; discusses an approach to redesigning language that draws on biological and risk management concepts; proposes a 'basic grammar' of risk and security covering their dual dimensions of probability and harm (underemphasised in crime prevention); focuses on sources of risk centred on the product, based on 'crime scripts' and criminal motivation; and explores wider ecological and evolutionary issues. It makes suggestions for improving any assessment scheme and raises wider issues on how crime science should tighten its terminology and bring together approaches to crime prevention and risk management. The present contribution comprises proposals for discussion and development rather than a perfected schema.

Keywords CRAVED · Crime prevention · Crime science · Crime proofing · Crime scripts · Design against crime · Electronic products · Harm reduction · Hot products · Risk management · Security

Paul Ekblom is co-director of the Design Against Crime Research Centre, Central Saint Martins College of Art & Design, University of the Arts, London, where he works on design, crime futures and conceptual frameworks for knowledge management of good practice in crime prevention. Aiden Sidebottom is a research assistant at UCL Jill Dando Institute of Crime Science, University College London and has recently acquired a master's in crime science from the same institute. He is currently working on various research projects including the evaluation of design-based interventions to reduce theft of bags in bars and cafes.

P. Ekblom (✉)
Design Against Crime Research Centre, Central Saint Martins College of Art & Design,
Southampton Row, London WC1B 4AP, UK
e-mail: p.ekblom@csm.arts.ac.uk

A. Sidebottom
UCL Jill Dando Institute of Crime Science, University College London, London, UK

Introduction: Project MARC

Project MARC aimed to develop a way of assessing the risk of theft, and corresponding security, of consumer electronic products,[1] including laptops, personal digital assistants, MP3 players and digital cameras. The project followed up Clarke and Newman's (2002, 2005a,b) proposals on 'modifying criminogenic products'. The researchers admitted that while their task was vital for preventing crime, it was also daunting, due to policy obstacles and the tension between opportunity reduction and commercial interests.

The MARC approach to risk assessment involved comparing a consumer electronic product's 'vulnerability to theft' with its 'security'. A product at high risk of theft (e.g., through high value) should have a commensurately high level of security (e.g., an effective anchor, identification or access code). Products rated both 'vulnerable and insecure' were self-evidently at greatest risk and should be the subject of appropriate governmental/European action to encourage or require manufacturers to reduce the mismatch - normally by increasing security. This would preferably be done, in anticipation, at the design stage, when options are broader and 'troublesome tradeoffs' (Ekblom 2005a) between security and other desired features, such as user-friendliness or weight, are easier to resolve.

Project MARC aimed to develop an operational 'crime risk assessment mechanism' which should meet the following specification:

> "a) measure both risk and protection (ensuring that the two are commensurate), b) reflect the language of those who would be tasked with implementing it and c) reflect the language of stakeholders from a variety of European states" (Armitage and Pease 2007:[11] (in press)).

The researchers also advocated that the mechanism be developed bottom-up, rather than being imposed on stakeholders. This was to accommodate two audiences: crime control agencies who could alert consumers to risk and provide precautionary advice, and manufacturers/retailers who could modify their products based upon the findings.

In practice the researchers developed two quantitative checklists measuring a product's vulnerability to theft, and security against theft. Vulnerability was measured using Clarke's (1999) CRAVED model for identifying a product's risk factors to theft in terms of how concealable, removable, available, valuable, enjoyable and disposable the tested product was rated. Security was assessed through issues such as customer education, authentication of a product and the additional cost of security inclusion to the manufacturer. A combined score indicated an electronic product's resultant risk of theft.

The two checklists were appraised by various experts, revised and finally applied by 21 judges from numerous sectors (e.g., insurance, law enforcement) and several European states, to estimate the vulnerability and security of 15 products from five classes.

Project MARC finished in 2006 with a multidisciplinary conference and a report (Armitage et al. 2006; summarised in Armitage and Pease 2007 (in press)) whose recommendations covered research, practice, delivery and policy.

Aim and Structure of Paper

This paper seeks a deeper understanding of the conceptual problems faced in Project MARC; to develop an approach for resolving them; and to apply that approach to generate

[1] For brevity hereafter 'products'.

initial proposals for new terms and concepts that are fitter for purpose than those the MARC team had available. Our proposals will not be definitive; indeed, we identify issues to be resolved before the complexity of crime-proofing can be terminologically tamed, and a practical risk/security assessment scheme created. But we hope our approach, and its fruits so far, generate debate within crime science. This should cover both the specific task of crime-proofing products against theft, and more widely, the relationship between crime prevention and security/risk management.

After identifying conceptual/terminological problems in MARC, we discuss an approach to redesigning language; propose a 'basic grammar' of risk and security covering their dual dimensions of probability and harm; focus on sources of risk centred on the product; and explore wider ecological and evolutionary issues; and suggest improvements to product assessment schemes. In the conclusion we revisit issues raised in Project MARC and consider wider implications.

Conceptual/Terminological Problems in Project Marc

In developing an operational crime-proofing system MARC encountered various conceptual, terminological and methodological problems. At the *outset* of the study, the authors readily acknowledged the issue of terminological imprecision.

During the *course* of the study several challenging issues emerged in rating vulnerability and security. Concerns arose over the lack of flexibility imposed by using *quantitative* measurements. Judging *vulnerability* raised issues of clarity and subjectivity. Here, people were having to make many, and maybe diverse, assumptions about how and where products were exposed to risk of theft: for example whether the product is anchored or easily movable, whether the offender can easily identify the product or whether there exists a limited window of opportunity for the offender to locate the product. Problems with the *security* checklist were more specific, with many respondents suggesting this would be difficult to complete without detailed product information. A divergence of language also emerged. While the security checklist used a *functional* language ('*unique identification of product; anchor*'), respondents when explaining their judgements often used more *technical* language ('*BIOS password; cable-lock*'). The effort of translation may have made the task harder work and prone to misinterpretation.

Various remedial measures were taken including adding open-ended questions, and changing from criminological language to that of manufacturers. These apart, at the project's conclusion the researchers faced unresolved problems which left them equivocal about a two-scale (vulnerability and security) rating approach:

- Product scores varied little across the *vulnerability* dimension. This could stem from offenders targeting, say, homes or handbags and indiscriminately grabbing whatever electronic items lay within, including those with no value to them[2]
- *Individual raters*' judgements on each product's vulnerability were significantly negatively correlated with those on security (e.g., high vulnerability was associated with low security), leading the authors to suspect a flaw in their approach. Theoretically the scores should have been independent, but the raters may have been confounding the underlying concepts.

[2] 'Bycatch' in sea-fishing circles.

- Worse, when individual raters' scores were aggregated, the correlation between vulnerability and security was no longer statistically significant, suggesting perhaps that there was little common basis of judgement between individuals.
- The researchers discovered that vulnerability had little relationship with the product's weight and price. CRAVED, although more complicated, seemed to capture a broader, more valid, view, but they were concerned at the constraints CRAVED imposed.
- Problems with CRAVED itself were raised, for example whether 'concealable' should always refer to the thief pocketing the product, or whether it could also apply *defensively* to the owner hiding the product from the thief.
- Armitage and Pease's summary of project MARC highlights linguistic discrepancies and a need for interpretation when trying to fit respondent language into the CRAVED framework. "Does 'high quality specifications' stand proxy for expensive? Is 'good brand name' a marker for expensive, enjoyable, disposable, or none of these?" (2007:[25]). Are key aspects lost in translation?
- Examination of judges' justifications for security ratings led the researchers to view security features as more product-specific and less amenable to a universal rating scale than originally envisaged. They indicated that somehow conducting a product-by-product holistic judgement and applying the original '25 techniques' of situational prevention (Clarke and Eck 2003) could better handle this richness than a checklist; but did not suggest how this could be done in practice, standardised or quality-assured.

The Project MARC researchers bravely wrestled with these difficulties and devised various solutions, including those mentioned above. However, the paper gives the impression that there is still far to go in both research and theorising before arriving at a risk assessment mechanism that is fit for purpose.

Our own view is that these problems stem mainly from the terminological/conceptual imprecision that the authors rightly bemoan, but do not fully address. In fact, the Project MARC report (Armitage et al. 2006), largely echoed in Armitage and Pease (2007), introduces imprecisions of its own:

- The abstract describes a 'crime *risk* assessment mechanism' which measures both '*risk and protection*'. It then describes rating a variety of electronic products in terms of both '*vulnerability and security*'. Vulnerability is equated here with risk (and protection with security).
- S1.9 is headed 'The Measurement of Crime *Risk*' and refers to "a mechanism to measure the *factors which make certain products vulnerable to crime* [as being] a relevant tool to enable the *prediction of risk*". Here, vulnerability is a causal factor *underlying* risk.
- The heading of S1.10 contains "Draft Crime *Risk* Assessment Mechanism", but the text refers to assessing a "product's *vulnerability* to theft in terms of how concealable, available, valuable, enjoyable and disposable a product is." Here, it is unclear whether vulnerability is equated to risk per se or to causal/correlational factors that underlie it.
- The text of S1.10 then describes how the second checklist assesses the product's security features: for example, whether it contains technology to negate its financial value if stolen. Finally, and perplexingly, it then states that "*Vulnerability* to theft is indexed by *the relationship between scores on the two indices*." In other words, vulnerability is simultaneously used in two senses - a) as risk or risk factor, and b) as relationship between risk and protection.

- S1.10 then uses an entirely different term for risk by referring to "Products [having] high *vulnerability*/low security [being] particularly *prone* to theft."

How significant are these terminological problems? After all, English prose is well-known for its capacity, and stylistic preference, for saying the same thing in different ways.[3]

We suggest these problems are potentially an insuperable obstacle to the proposed crime-proofing of products. Such imprecision and ambiguity can limit the achievements of multidisciplinary and practical projects through confusing important conceptual distinctions; allow drift of meaning to deny us firm procedural foundations; diminish common ground for discourse between different stakeholders; and inhibit international communication. These problems are not, of course, confined to Project MARC. Gill (2006) notes that there are major definitional problems with the term 'security' that remain to be solved, with different disciplines according it quite different meanings, and little cross-referencing within those disciplines. Villagrán (2006) expresses similar concern in the disaster relief field.

We now seek to tease apart the distinctions and to redesign the terms and concepts that articulate risk, vulnerability, security and related ideas. The intention is to provide a more consistent and usable linguistic platform from which the considerable achievements of Project MARC can be taken forward practically, empirically and theoretically.

How to Redesign a Language: Tackling Marc's Terminological and Conceptual Problems

How to re-design terms and concepts? The language we require should be both constraining to give precision, consistency, efficient communication and sharp criticism; and enabling, to allow people to imagine, design and articulate diverse possibilities of theory and practice with disciplined creativity.

In developing our language we will attempt to respect, and build on, the MARC specification for the crime risk assessment mechanism, and where possible use existing terminology from CRAVED in particular, and situational crime prevention in general. However, some change may be necessary. CRAVED was derived mainly empirically from statistics of products at risk of theft. It therefore combines quite diverse factors. Although this was a valid approach when the purpose was to rapidly and memorably communicate the concept of 'hot products' to diverse stakeholders, the 'slogan' style may have revealed its limitations in trying to apply it in a rigorous, practical context as in Project MARC. We will, therefore, work on concepts from bottom up and then revisit CRAVED to see if it is still the best way of identifying risk factors; and if not, what the alternative might be. The 'bottom' in question centres on generic principles of risk and harm, taken in combination with concepts from crime and its prevention - primarily focusing on theft, but always with an eye to the more general.

One particular concern we have in developing terms and concepts (pursuing a theme long followed by Ekblom 1994, 1997, 2002a,b) is to ensure that all definitions *interlock* in a single, consistent *conceptual system*. In other words, if **a** means **b/c** then **c** consistently means **b/a** and so on. Ensuring reciprocity of meaning within an entire suite of terms is vital for orderly and efficient research and development in any academic and practical field that has progressed beyond the 'Wild West' stage.

[3]See George Orwell's (1946) essay 'Politics and the English Language' for his exposition of "mental vices" and the "slovenliness" of language.

One framework that has attempted to develop interlocking definitions in this way is the Conjunction of Criminal Opportunity (CCO) (Ekblom 2000, 2001, http://www.designagainstcrime.com/web/crimeframeworks). This is an integrated, analytic model of the immediate causes of criminal events which draws together familiar criminological theories in a single language; and a corresponding map of the principles underlying preventive intervention. Various terms from this framework (such as crime preventers and promoters, target enclosures and offenders' readiness to offend) will be used in our reconstruction.

We think it important for those professionally involved in crime-proofing and secure design to be conversant with both *technical* and *functional* perspectives. Functional language confers generality and economy of description. While manufacturers will focus on technical matters, designers should be capable of moving easily from one discourse to the other as their work progresses. (Whitehead et al. (2007, in press) use similar dual discourses.) Crime prevention practitioners, if they are following a problem-oriented approach and/or a design-like approach to intervention (as advocated by Ekblom 2005a) should equally be encouraged to move between function and form, or generic principle and practical method. This last duality is of wider importance in crime prevention in the process of intelligent, context-sensitive replication of good practice (Tilley 1993; Ekblom 2002a,b, 2005b).

In seeking new terms and concepts we, like others (Cohen et al. 1995; Ekblom 1999, 2005a; Farrell 2001; Felson 2006), will use *biological* perspectives, especially ecological ones. *Foraging* (e.g., Johnson and Bowers 2004; Felson 2006) comprises the behavioural tactics and strategy for exploiting the benefits of the environment and coping with the risks of harm and wasted effort. *Adaptation* ecologically links the design of an organism, or product, to its environment and the hazards that environment holds. A complementary concept is the *risk environment*: the environment of a particular product (or other entity), which contains sources of criminal risk to that product. *Evolution* covers the dynamic *process* of adaptation. Of course, biological perspectives do not supplant rational, utility-based perspectives such as rational choice theory (Cornish and Clarke 1986) but enrich them.

We also consider concepts for addressing risk in non-criminological domains such as accident prevention, public health and disaster management. However, this requires care because common terms such as 'vulnerability' have quite diverse meanings.

The main terms developed below appear in the Appendix.

Basic Grammar - Disentangling Key Terms and Concepts

We begin our attempt to disentangle key terms and concepts with surely the most fundamental, namely *risk*. Project MARC was primarily an exercise in *risk assessment*, in the service of *risk management* at European level. While this is clear as stated, various problems attended the use of 'risk' in the project, and also in situational prevention more generally.

Risk and Vulnerability

As noted, there was some confusion and overlap in usage of the terms 'risk' and 'vulnerability'. The latter was used variously as a *synonym* for risk, as a *cause or source* of risk and as the *resultant of the balance* between risk and protection/security. Our preference is to keep the terms distinct, so they can serve different purposes. Risk becomes more fundamental; vulnerability less so.

Risk Promoted

We think *risk* should follow wider usage in the risk-assessment world beyond crime prevention. Risk has two aspects - the *probability* of a *hazardous event*, theft, happening to the product; and the *harmful consequences* of the event to the product, and more significantly to various parties such as its owner or carrier, the home it is kept in, or some wider institution or system. Practically speaking, knowledge of probability is important for directing attention of crime preventers to the product; knowledge of potential harm, for prioritising preventive action. Knowing what to do about the risk comes from deeper knowledge about causes and interventions, and the people and institutions capable of implementing them.

Sometimes risk is used to cover both probability and consequentiality, sometimes just probability. This duality causes confusion in crime science, but tackling it requires persistence. Here it will be used in the *dual* sense, which is common in 'utility' literature and risk management; where necessary the more specific meaning will be declared.

Vulnerability Demoted

Vulnerability should take just one of the meanings used in the MARC paper. It is not a *state* of risk, but a *cause* of the heightened probability of theft occurring to a product, which resides in a feature/features of the product itself.

As will be developed below, vulnerability is one of several such causes. Together, these can be called that product's *criminogenic* features (Clarke and Newman 2005a; Pease 2001). Other criminogenic features include a product's *value* to the offender.

Harmful Consequences of Theft of Product

Public and political concern about 'the crime problem' typically centres on *numbers* of events. With theft of electronic consumer goods, *consequences* beyond the simple loss of the product itself must be considered. Loss of a PDA or laptop may lead to immense inconvenience from loss of the data contained. Worse, that data could give offenders access to the owner's bank account or identity, or to some wider system such as that of the owner's employer, allowing further, more serious crimes to propagate. And of course, products taken in robbery or burglary may have serious bodily or emotional consequences. Taken together, what happens as a *result* of the criminal event is highly important both practically and politically. And as is widely appreciated, *perception* of risk may have harmful consequences whether or not that perception is valid.

'Consequences' is too clumsy a term to refer to all this. 'Impact' of the occurrence of a hazardous event is often used in the wider risk management field, but in the crime science context this makes for confusion with the evaluative sense of 'impact of intervention on crime'. We will therefore simply call it the *harm* of an event to a product and/or to people, institutions and systems associated with it. This connects to the wider concept of *harm reduction* which, with its links to the quality-of-life notion of *community safety*,[4] is steadily moving up the public agenda.

A concept linked to harm is *hazard*: something *with the potential to cause harm*. Risk, as the probability of harmful events such as theft, rests on the conjunction of one or more

[4]See http://www.designagainstcrime.com/web/crimeframeworks for appropriate definition of community safety focusing on the harmful consequences of crime, complementing the criminal event focus of crime prevention.

hazards and wider facilitating conditions (Clarke and Newman 2006). A hazard originating from malevolent human intent can be called a *threat*. (see also Savona and Di Nicola 2002).

Just as 'criminogenic' describes features of a product that increase the *probability* of theft, we can call a product with the potential to cause *harm* through that theft event, *criminally hazardous*.

What kinds of criminal harm follow from theft or robbery of a product?

- Harm to the *product itself* during/after the crime (e.g., laptop damaged when pulled away from anchor, or its cover scratched to obscure serial number). Susceptible features of the product include *fragility, anchorage*, and *marking* that damages the case when removed
- Harm to the *owner or other parties* through the *loss or damage* of the product and its informational contents (e.g., owner loses the only draft of document and fails to meet publication deadline). Hazardous features include: *cost* (mitigated by insurance), *capacity to engender sentimental value, loss of data/cost and effort to recover* (mitigated by backup and retrieval arrangements).
- Harm to the owner or other parties through the *collateral loss of, or damage to*, the *enclosure/carrier* (bag, house) and any *bycatch* of other goods taken and perhaps discarded. These harms are not especially connected to hazardous features of the product, except that the product is *designed to be carried* in a bag or pocket along with other items.
- Harm to the owner/carrier/householder from the *theft or robbery event itself* - shock, injury, humiliation etc.[5] Hazardous features include: design of *carrying straps and grips, anchorage of earphones in ear.*
- *Propagation of further harm* through *misuse* of product (e.g., in identity theft, or defrauding wider system) - in effect, this is now another crime or crimes altogether, and the product, in the wrong hands, has become a *fresh* criminal hazard.[6] Hazardous features include: *accessibility of data, accessibility of service* (e.g., via stolen phone), *utility of data* (e.g., for identity theft and consequent crimes; for using product anonymously in drug dealing/terrorism).

Not all things, people or institutions are equally affected by harm. The *potential to be harmed* by a given criminal event (e.g., an easily-damaged phone, an easily-injured person, or a bank account accessible via a stolen product) could be called *susceptibility* to harm.

Security

We first consider security in relation to the probability side of risk, then incorporate harm.

Security and Probability of Criminal Event

Although risk and security appear to be opposites, using security simply to mean 'at low risk of crime' is not helpful. By this definition something could be secure just because it had no intrinsic value, like the empty box the laptop arrived in. Rather than describing such a *state of absolute low risk* the critical consideration is that, to be secure, some product is *less at risk than expected* by virtue, for example, of its attractiveness to offenders. This

[5]Legally, occurrence of injury may change the classification of the crime or add a new offence, but from a preventive perspective it remains the same event.

[6]That potential for harm through misuse existed even before the theft - it has now just become clearer.

modified risk is hence the *resultant* of the *criminogenic and criminocclusive* (using Felson's (1986) antonym) *influences* raising and lowering the probability of theft. This relativistic understanding of security connects closely (and deliberately) to Project MARC's principle, of making security commensurate with risk.

Security must therefore be defined simultaneously in relation to *risk-enhancing features* of the product[7] and *security-enhancing features*.

Some features, such as the *bulk* of an expensive television, could confer security as an *incidental* property of the product. Other features are deliberately *intended* to confer security - as with a designed-in anchor cable. We think the plain term *security* is better used to refer to something crime preventers *deliberately* do to a product to *make* its risk lower. (This positive meaning connects with the other sense of security, as an active *process* or a *capability* of individuals, organisations or systems.) The qualified term *incidental security* should be used to cover the remaining cases.

In biological discourse, possession of some evolved and distinctive feature which conferred security and had no other apparent function would be considered a security *adaptation*. 'Evolved' is taken to imply that the feature has undergone several iterations of improvement and specialisation, in a consistent direction.

From a quasi-biological angle the key security assessment question becomes '*is the product adapted, through security features, to the risk environment of theft it is likely to face when passing down the supply chain and during end-use?*'

Security and Harm - Making the Product Less Criminally Hazardous

Security, of course, must not only cover the *reduced probability of theft* happening to the product (its criminogenicity), but a *reduced potential for harm*.[8] In the previous section we identified various aspects of harm associated with the theft of a product, and linked these to susceptibility to that harm, and propagation. Here they are repeated, with our suggested generic security equivalents for limiting/mitigating the harm.

- Susceptibility *of* product itself to criminal harm during/after the crime. Security equivalent is *product resilience*: the product's potential to *resist, limit or recover from harm*. A simple example is shockproofing.
- Susceptibility of owner, others or wider systems to harm *through the loss/damage* of the product, collateral loss/damage and bycatch. Security equivalent is *system resilience*. This could partly be designed into the product e.g., via data backup and registration/tracking/retrieval systems (which also may be criminocclusive).
- Susceptibility of owner/carrier/householder to harm (e.g., injury) from the *theft or robbery event itself*. While this harm can mostly be reduced by designs for avoidance (i.e., boosting the criminocclusive features of the product), reducing hazard from the product might include designing in 'fuse' straps which break and let the offender escape without using excessive force to snatch the product or turning a snatch into confrontation and assault.
- *Propagation of further harm* through *misuse* of product. Security equivalent is *shielding against misuse* in additional crimes (taken from the Misdeeds and

[7]Multiple features may raise risk additively, or synergistically, e.g., laptops must be both removable and valuable to make theft possible and worthwhile.

[8]We need a term for the harm equivalent of criminocclusive - criminally harmless? Criminally safe?

Security framework (Ekblom 2005a,c) which covers crime risks additional to theft.). This could be achieved through password protection or remotely disabling the product, through product/system design.

There may be 'troublesome tradeoffs' (Ekblom 2005a) between making a product *less criminally hazardous* and *less criminogenic* - because, say, products whose strap breaks to avoid injury, may attract criminals through ease of theft. Maximising both functions poses a challenge for designers.

Taking probability, harm and susceptibility together, and incorporating accident and injury safety perspectives (World Health Organisation 2004),[9] security against product theft can be:

- *Primary* - reduce probability of harmful event - i.e., increase criminocclusiveness of product.
- *Secondary* - if event does happen, limit harm as it unfolds to product, owner and beyond - i.e., increase resilience of product and system.
- *Tertiary* - limit propagation of harm post-event - i.e., increase shielding of product against misuse.

Risk management approaches, including those applied to security, normally include *mitigation* of harm. Mitigation would come under secondary and tertiary security above. Mitigating actions may stem from the product's, owner's or system's own resilience, or may complement them. Mitigation is not preventive per se, because it happens after the harmful event (e.g., victim support action after robbery).[10] *Preventive* mitigation occurs when resilience can be designed in advance into product or system - e.g., an external data-backup facility in a music-player.

Defining a Secure Product[11]

Drawing these definitions together, *a secure product is one whose risk of theft is less than expected on the basis of its criminogenic, susceptible and criminally hazardous features, because it is deliberately adapted to its expected risk environment to be criminocclusive, resilient in itself to harm, designed for incorporation in a resilient system and shielded against misuse. An insecure product is one with strong criminogenic, susceptible and criminally hazardous features, but without effective security adaptations/features to reduce the elevated risk of theft to some acceptable level of probability and harm*.[12]

The *security level* of a product is how far its security features outweigh its criminogenic and criminally hazardous features. In the case of an *insecure* product, they fail to do so.

[9]See also Haddon's matrix (e.g., Haddon 1980) for accidental injury prevention, which divides injury into pre-event, event and post-event phases; and in a second dimension, contributing factors under host, agent or vector and environment.

[10]It can however set the scene for preventing the *next* crimes. This could be within a repeat-victimisation context, or more strategically with the redesign of a product revealed by a 'crime harvest' (Pease 2001; Ekblom 2005a) to be criminogenic or criminally hazardous.

[11]Ekblom (2005a) distinguishes 'secure products' which have inherent security from other fruits of design including add-on 'security products', 'security components' etc. Whitehead et al. (in press) list several dimensions of anti-theft design.

[12]This paragraph hopefully demonstrates how we are starting to write in ways that demonstrate the consistency and reciprocity of meaning of the individual terms in a single conceptual network. An even fuller sentence could be constructed to incorporate all the subsidiary definitions, but that would overload the poor reader, who would no longer be gentle.

Sources of Risk Centred on the Product

Having established the basics of risk and security in our revised language, we can develop further detail. In particular, we can consider the causes of risk of theft that centre on the product. We examine probability in detail below, because crime-preventive experience is plentiful. This cannot be accompanied by equivalent coverage of harm, because this is currently underdeveloped in crime science.

The Criminogenic Product: Product-Centred Causes of Heightened Probability of Theft

What features of products raise their probability of being stolen? CRAVED supplies answers, but risk factors like 'removable' are too specific at this point. Products are often loosely described as 'attractive' to criminals; we have already encountered 'vulnerable', restricted now to the causal sense; and there is also 'provocative' - for example through triggering an offender's jealousy by sight of someone owning a more expensive phone than their own. But these terms are entangled.

Attraction is quite a 'composite' term when one considers the range of underlying causal mechanisms it touches on. A thief can be attracted to steal a music player, say, because it simultaneously engages attention, excites desire and appears obtainable by virtue for example of its vulnerability to theft. *Provocation* in common usage confuses *prompting* and *provoking* - two 'precipitating factors' in Wortley's (2001) expanded two-stage approach to situational crime prevention. Prompting, with theft, tells an already motivated offender that here is something to steal. Provoking not only signals the presence of the target but awakens the emotion and motivation in the offender which drives him/her to steal. In CCO terms this amounts to 'readiness to offend'. A product could be *vulnerable* in common usage through being visible (prompting/provoking theft) and removable (facilitating theft). Do we want 'vulnerable' to mean both?

Clearly the terminology just described provides a shaky basis for scientifically and practically articulating the causes of elevated probability of theft. Something more consistent is needed.

Our suggested framework stems from the *process* of theft. At its simplest this comprises:

- *Seek and/or see* target product
- *Want* product
- *Take* product
- *Realise value* from product

Essentially the 'seek, see, take and realise' parts comprise a minimalist cognitive 'crime script' for theft (Cornish 1994). The script takes the 'view *from* the offender' (Ekblom 2007) as an active 'foraging' agent seeing the crime situation from the functional perspective of pursuing his/her goals and maximising reward in a 'rational' or 'utility' framework (Zipf 1950; Cornish and Clarke 1986; Johnson and Bowers 2004).

The 'want' part is, by contrast, a 'behind the scenes' causal mechanism for which the offender is the vehicle. Motivation and emotion may both precede the search (via anticipation) or be provoked on sight of the product ('I *must* have that phone!' or '*He* doesn't deserve it, *I* do!'). This is the 'view *of* the offender' (Ekblom 2007), focusing on the internal causes of his/her goals and behaviour. But it simultaneously describes features of the product: the offender is motivated to steal things which he *perceives* at the time will be of realisable value.

So our earlier question on risk now becomes: what features of products raise the probability of their being sought, seen and taken by thieves? How do offenders' cognitive

and motivational mechanisms operate in conjunction with features of the products to make the offender want them and go foraging for them?

We must be aware that at every stage, two parallel processes are in play: the *objective* risk that the offender will be spotted and caught whilst foraging; and the offender's own subjective *perception* or *anticipation* of this risk. Sharing a similar dualism to this *deterrence*, is *discouragement* - from excessive *effort to succeed* in the theft, and/or *risk of failure*. All these mechanisms play a part in realising the criminocclusive side of the product; all are exploited by security adaptations. For example, anchorage may both physically thwart the offence and cause the offender to perceive that the extra time taken/ noise made in removing the product may alert preventers and increase risk of arrest; and reduce the rate of return for effort. Exaggerating the robustness of a product's appearance may discourage offenders from even approaching it.

After identifying each criminogenic feature of the product, we define the criminocclusive equivalent, and any deliberate security adaptations. The latter we describe in functional terms and illustrate where possible with practical examples, because we ultimately want to map functions onto technical language. Giving multiple views of the same underlying concept may seem redundant. However, we think this versatility entirely necessary for helping the designer, or assessor, of the product to flip perspectives during their work. Our provisional efforts so far are summarised in the Table 1.

Seeking the Target of Theft: Ecological Factors

One criminogenic factor that helps thieves find a product is its *presence* or availability (as in CRAVED). The criminocclusive equivalent is, unsurprisingly, absence. This appears not to be a feature of the product at all, more a matter of *exposure* through a) numbers of product sold; and b) who buys it and where they carry or leave it... associations known by resourceful offenders. But of course, products can be designed for use in certain places, perhaps 'risky facilities' (Clarke and Eck 2003; Eck et al. 2007) and to be portable. One security adaptation to presence could be alarms or reminders to warn people not to take their products into particular locations, or to be careful when doing so. Perhaps this could be termed a product's *locational avoidance*, which in technical language may be realised through a GPS facility and access to crime hotspot data (plus a capable guardian to respond to it).

Seeing the Target of Theft: Perceptual Features

The offenders must *see* the target product, or otherwise *detect* it (e.g., seeing a bulging pocket or using a scanner). This could happen during a planned search or an opportunist encounter. We call this feature *visibility*. The criminocclusive and security equivalent, which enables the product to avoid being seen, is *invisibility*.

During/after detection, offenders must *identify* the product:

- To *value* it (Is it worth taking?). This relates to the concept of 'affordance' (Gibson 1979; Garwood 2004; Pease 2005), the offender's capacity to see utility in an object.
- To judge whether they can *deal* with the targeted product tactically and logistically, i.e., *take* it and later *realise value* from it (How heavy is it? Could I carry it without being noticed? Will I get a good price? Could I crack the database code? Could I access a bank account with it?). This must be done relative to self-knowledge of resources (Am I strong enough to lift it? Can I neutralise the movement sensor?) (Ekblom and Tilley 2000; Gill 2005).

Table 1 Theft of electronic products: illustration of risk and security features in criminological, functional and technical language

Script stage and criminal motivation - offender	Criminogenic term	Criminocclusive term	Functional security term (if different)	Example of technical security adaptation
Seeking the target of theft: purely ecological factors	Presence in risk environment (availability)	Absence from risk environment	Locational avoidance	Use of GPS to alert owners in certain locations
			Target removal	Detachable satellite navigation console
Seeing the target of theft: perceptual features	Visibility	Invisibility	Invisibility	Concealment from offender, camouflage
	Identifiability (to value, deal with product)	Anonymity	Anonymity	Disguise, standardisation of appearance, removal of distinctive appearance e.g., iPod earphones
	Overt reassurance and encouragement of offender	Overt deterrence and discouragement - offender *anticipates* that product is difficult to deal with, could be *obvious* when being taken, etc.	Deterring/discouraging appearance	Iconography/semantics of design (Whitehead et al. 2007); robust or menacing appearance (e.g., flashing 'security armed' light/sound) communicating capability of taking further action e.g., protest. In effect signalling/ exaggerating/pretending any other security feature.

1. Table is illustrative and provisional, covering only the seeking and seeing stages of the foraging script and analysis of value for theft.

2. Table emphasises offender's perspective; owner/preventer's script/motivation could also be included in different format.

3. Counter-counter-countermoves, e.g., anti-tamper features of existing security adaptations, are not included but could be accommodated using extra columns.

4. Technical security adaptation entries could be further developed to systematically reflect the 'asymmetry' and 'discrimination' principles of security discussed in later section of paper.

The criminocclusive/security equivalent of identifiability could be termed *anonymity* and could technically be realised by disguise or standardisation of appearance.

Some visual features of the product can communicate criminogenic or criminocclusive messages without offenders having to identify make and model. Whitehead et al. refer to the "iconography and semantics of [mobile phone] design, that is, the visual cues conveyed via shape and aspects of style, wording and other imagery." (2007, doi:10.1007/s10610-007-9040-9). A solid, robust appearance, or a flashing 'alarm is armed' light can (as with warning colouration of wasps) give *overt discouragement and deterrence* or, if absent, *overt reassurance and encouragement*.

Wanting - Motivation

We now pause the theft script and look behind the scenes to take the view *of* the offender. The motivational factors in CRAVED are somewhat overlapping, yet incomplete. Offenders seek something whose *value* they can realise through *enjoyment*, *disposal* ...or *misuse*. We consider inherent, or potential, value here; realisation, below.

- The criminogenic product may motivate theft because it inherently gratifies the offender, meets some other need (e.g., esteem from possessing the latest phone), can be sold to realise its value or misused for further benefit.
- Motivational features of products can also be criminocclusive. The product could simply be *worthless* and *useless* to offender and anyone else. On the security side, the classic situational prevention technique of *lowering the value of stolen goods* applies. The product could be made *perishable* over time, such as a phone that can't be recharged without a code. It could also be *fragile*.
- The product could be positively *repellent*, causing offenders to avoid or relinquish it; or indirectly preventing them from disposing of it to others. Such *repulsion* could be inherent, or a deliberate security adaptation. An owner's picture or smell could be embedded in the product, that either repels in itself or awakens feelings of empathy (Ekblom 2007) or guilt (Wortley 1996; Clarke and Homel 1997).

Products can, as said, motivate offenders because they perceive that purchasers in the stolen goods market value them highly. In some cases this value comes from features (such as lightness and compactness) that not only offer convenience to the legitimate owner, but also make the products tactically/logistically easy to steal. Unscrambling this conundrum without spoiling the features that attract legitimate purchasers challenges designers (Ekblom 2005a). Luckily, electronic products (and the systems they are embedded in) have increasing 'brain-power' to support discrimination.

Finally, besides motivating through value, products can *provoke*, for example by awakening an offender's jealousy: an under-researched issue which should concern designers.

Taking: Tactical and Logistical Factors

Let's assume the offender has sought and seen the product, and wants it. To resume the foraging script (the view *from* the offender), perception now slides into decision and attempted action. What criminogenic features of the product help the offender take possession of it and carry it off? From the Rational Offender perspective (Cornish and Clarke 1986), what tactical and logistical features of the product make this task low in effort and risk of harm to the offender, relative to reward?

In the case of theft that is entirely stealthy (taking from places and picking pockets), the offender must gain possession by *removing* the product from its place of storage, carriage or

use without substantially damaging it, injuring himself or attracting attention of preventers including guardians or place managers (Clarke and Eck 2003). Features (some familiar from Cohen and Felson 1979) such as *lightness*, *compactness*, *wholeness*, *graspability*, *free movement and incommunicativeness* all make this easy; *weight or inertia, bulk, fragmentation* (as in audio systems distributed about a car), *smoothness/slipperiness, anchorage/friction* and *protest* make it difficult. Many of these are inherent (as with a product that incidentally shrieks when torn from its anchorage); but all can be developed as security adaptations.

The offender must now *escape* from the theft site carrying the product without being noticed. Most of the features that helped taking possession and removal also facilitate stealthy escape; likewise, conversely, with the corresponding security features. The offender will often need to *conceal* the product, so the *invisibility* which was criminocclusive at the *seeing* stage now becomes criminogenic. This of course includes invisibility to various electronic detector systems. Many of the same features again facilitate *retention* for personal use or *storage* pending resale. *Removability*, however, may help owners prevent theft of the product from a car, say; but (as in CRAVED) their failure to remove the removable product could subsequently aid offenders.

Robbery introduces variations. Additional criminogenic features that act via the owner are *distractiveness* and *masking*, as with game players that occupy the owner's attention, or music players that mask the offender's approach. A security counterpart could *alert* the owner. *Concealability* is less important at the snatch stage, but may become so if a pursued robber seeks crowd-cover. With many of the other features, such as graspability, at the point of snatching there is a marked upheaval where they may, depending on the turn of events, help or hinder the offender and owner in quick succession.

Realising Value - Tactical and Logistical Factors

Various *practical* features of the product help or hinder offenders in realising its value. Incidental value-limiting features inherent in the product, such as perishability, shade into deliberate security adaptations which the offender must tactically overcome (adaptations that are superficial and 'bolt-on' are easier to circumvent than inherent limits to value). Given this, rigid separation of 'wanting' a product for its potential value and realising that value is not supportable; and assigning features to one or other heading is somewhat arbitrary.

Anonymity of the product (e.g., from mass production) is criminogenic by reducing risk in trading stolen goods. Incidental criminocclusive features include distinctiveness (as with stolen paintings, but this could also increase inherent value), fragility and perishability. Equivalent security adaptations include *property marking and registration, spoiling* (as with ink capsules showing the product is stolen, and making it physically unattractive to buyers), and deactivation by various means, termed '*executability*' by Whitehead et al. 2007) to lower its value in enjoyment, resale or misuse (equivalent to 'capture-proofing' military weapons). *Incommunicativeness* can again be turned into *protest*, e.g., via automatic or remotely-activated tracking or emailing.

Defining a Vulnerable Product

Finally, we can define vulnerability. A product *vulnerable to theft* is simply one which can be seen and taken by the offender, i.e., it is manipulable in line with the offender's criminal goal. This embraces all the criminogenic factors associated with theft of the product *except* the motivation it engenders in the offender, and the offender's *anticipation* at the time of theft that its value can subsequently be realised. For the vulnerable product to become an

insecure product, the motivation must also be present: that is, the product must have *anticipated* value to offenders, or capacity to provoke them. For the value to be *realised*, the product must be *susceptible* to enjoyment, resale or misuse.

Further Development

We have hopefully indicated some benefits of importing richer and more rigorous concepts of risk into crime science and systematically applying them to definitions of individual terms, whilst ensuring the entire semantic network is internally consistent. But the task is incomplete. Apart from extending basic knowledge and concepts of criminal hazard and harm, various complications need addressing before a complete schema for appraising risk and security exists. We discuss these briefly.

Preventers and Promoters

Our development of risk and security concepts has mainly followed the *offender's* perspective, but it could equally cover other parties involved in theft. Preventers[13] are people (or intelligent systems) who make crime *less* probable or harmful; promoters do the opposite. Often the same person plays both roles (owner locks phone keypad, or forgets). An *owner's script and motivation* could complement that already described for the thief, facilitating identification of product features which help *preventers* reduce risk, and hinder *promoters* (indeed, reminders to lock, say, should turn promoters into preventers).

Secure Products - a Theoretical Principle?

Our paper has emphasised insecurity over security. More fully incorporating the offender's perspective, however, offers the prospect of being able to state a *positive theoretical principle* for how to prevent theft. (The specific task of reducing harm, given occurrence of the theft, would need its own equivalent statement.) The legal definition of theft is fundamentally about legitimate versus illegitimate possession of (in this case) the product. Based on this, and our understanding of the interplay of the offender's and owner/preventer's scripts, the critical task of reducing the probability of theft is one of *creating or amplifying some asymmetry between the legitimate and illegitimate possessors, during seeking, seeing, taking and realising value for the latter, and retaining, using and enjoying for the former*. The asymmetry exists in terms of differential risk, effort, reward and provocation to one or both parties during foraging and/or retention. The key to realising the principle is either engendering some sort of fundamentally asymmetrical *value* of the product for the two parties that is sufficient to lose attraction to the offender; or creating some kind of *discriminatory* function which allows the owner significantly *easier access to that value* than the thief.

This fits well with the rationale of design against crime which seeks to apply a dual perspective, making products both user-friendly and *ab*user *un*friendly (Gamman and Pascoe 2004; Ekblom 2005a), in contrast to the single perspective of traditional user-centred design. Restating security against theft as an abstract principle could give designers

[13]Owners are not the only people capable of acting as preventers/promoters: the product could be adapted to resist fences, crooked technicians trying to overcome security, and end-purchasers of stolen goods; and designers could shift from promoter to preventer.

and engineers simultaneously the freedom and the clear guidance to exercise their ingenuity whilst also respecting commercial interests, and could likewise give a firmer backbone to the security rating process. In practice, asymmetry and/or discrimination has been attempted by many of the techniques illustrated in the Table 1 (and by those listed in Whitehead et al. 2007). Many centre on more or less sophisticated electronic codes or physical keys. Some treat the product and its environment as a wider system (discussed below) in which the discrimination involves access to an enclosure; or the asymmetry relates, for example, to the simple fact that it is hard for the offender to take a bulky product like a home cinema, but easy for the owner to enjoy it in its rightful place. Applying the principles to the secure design of *portable* products is far more demanding, but *all* aspects of portability are demanding.

Boundary Issues: Eggs and Nests

The *boundary between a product and its environment* is unclear. This is especially true when the environment the product finds itself in, has itself been selected, or designed, to supply security. A bird's egg is a juicy target, protected in various ways. The 'naked'[14] egg may itself be camouflaged, or designed for concealment by its immediate environment, the nest; egg + nest may together be designed as a single unit - 'target in its specially-designed enclosure'; this in turn may be high in a tree, which can either be seen as the immediate *environment* of the egg + nest, or as a wider *designed secure system* developed to cope with the hazards of a still wider environment, in the intermittent absence of parent birds.

With electronic products, we face similar problems of determining boundaries within layered systems and environments (as the MARC paper acknowledges). A music player, say, can be considered when left alone outdoors; in an empty or occupied house; or in a pocket. The product may be designed for hiding (e.g., car radios with drop-down covers), removal from the enclosure when this is left unattended (pull-out satnav (satellite navigation) consoles), or anchoring to the environment. It may be *distributed* in components around the car using electronic communications to maintain functionality. (Coming soon is distribution around the carrier's *person* using wearable technology and 'body area networks'.) The product may be *embedded* in a wireless system that raises the alarm or disables it if removed from a certain location. The embedding may be non-geographical, in that the product may require secure connection to a *service system* with worldwide outlets.

Ecological Dimension: the Risk Environment

Risks of course originate in the product's environment. usually its '*habitat*': the place/s where designers expect it to be. We may thus describe a product as 'at risk' if it is habitually *exposed to a risky environment*. Does the habitat normally contain many offenders? Are these places helpful to offenders, for example with convenient 'lurking spaces' for watching drivers conceal laptops when parking? Does the environment hinder preventers from managing the place or guarding targets?

Environment does not just *add* to the criminogenic (or otherwise) features of the product: the two *interact*. Consider a product which is currently criminocclusive through camouflage. The camouflage is jointly a function of the product and its environment; it is therefore an *ecological* concept. In fact, every term in risk and security discourse implicitly possesses an 'ecological dimension'.

[14]Armitage and Pease (2007) also use 'naked' in this sense.

What if a product's security features are adapted to the wrong habitat, e.g., because the environment changes? A biological example is the Peppered Moth (Biston betularia). This was perfectly camouflaged to match lichen on trees. Pollution killed the lichen and blackened the trees, rendering the camouflage useless and the moths, dinner.

One important aspect of the risk environment is the offender's *resources* for committing crime (Ekblom and Tilley 2000; Gill 2005). Bolt croppers defeat anchor cables; scanners detect hidden electronics. As Ekblom (2005a) notes, an opportunity is not simply a characteristic of the environment, but *co-produced* by the offender's resources to exploit that environment. An open window on the 3rd floor is only an opportunity to offenders possessing skills, courage and maybe a ladder.[15] The Loss Prevention Certification Board (e.g., 2006) recognises this in its risk assessment frameworks and makes its security specifications *performance-based* rather than technical (e.g., 'block burglars for 10 minutes' rather than 'use manganese steel'.) The specifications are, therefore, *future-proofed* against changes in offender capabilities - revisited below.

Offenders also respond to ecological cues: perception shades into association. Even an opportunist offender could *infer* the likely presence of a product: a teenager probably *will* carry a mobile phone; a dapperly-dressed business executive, a laptop.

Another ecological issue concerns the company the product keeps. Does it *gain* risk from being designed for travel in a handbag? Does it *spread* risk to other, less-valuable, products normally kept with it? This poses a problem for rating the risk/security of individual items in isolation, as the MARC authors noted. But sometimes it can be exploited for security, through the concept of 'herd immunity'.[16] This occurs when a critical proportion of a herd of animals (or humans) is immunised: the rate of contagion becomes less than the 'replacement level' and the infection dies out. Likewise there may come a point when offenders judge people as not worth robbing, or homes not worth burgling, because the likelihood of finding anything of realisable value in them is low.

As Project MARC discovered, judges assessing risk and security had to make many assumptions about the environment in which the product would be exposed to risk of theft. *All the risk and security features of products that we list depend for their effect on* supportive or interfering features of the *environmental context, including offenders' resources*. Many depend on *transactional relationships* between offender and various preventers/promoters who are part of that environment, including the owner/carrier of the product. What have been treated as 'scalar' variables (which just have quantity) are actually 'vectors' (quantity + direction) in a multidimensional ecological space. Failure to 'think vector' underlies confusion between, say, 'concealable from offender' versus 'concealable from preventer'.

For a risk/security assessment system the only workable way to handle this would be to identify a limited set of 'typical risk environments' for domestic electronic products which the product would be security-adapted to, much as the product might be 'tropicalised' for certain geographical markets. This would include some level of reasonable security behaviour on the part of owners and possibly other preventers. If the product were designed only to be used in a secure environment, the manufacturers could declare this.

[15]Pease (2005) takes a similar ecological view of opportunity in connecting it to the concept of affordance (see also Garwood 2004 for an empirical study). This concept may in fact be more familiar to designers (e.g., Norman 1998) and thus more helpful than that of 'opportunity'.

[16]Armitage and Pease (in press) refer to both herd immunity and bycatch as concepts, but do not name them.

Perhaps we can specify each 'standard risk environment' as, for example, 'product in owner's averagely secure home when attacked by averagely-resourced offender, prepared to accept low risk/effort'. These standards would have to underlie any 'traffic-light'-type security rating scheme adopted for easy communication to consumers.

Evolution: Countermoves and Arms Races

As Armitage and Pease (2007) note, nothing stays still. Changing social and technological circumstances and adaptive, inventive, offenders mean that what works in preventing crime now, may become ineffective in the future. Security adaptations of products may themselves need to evolve (like the Acacia thorn which grew so long it needed a small thorn protecting the base, to avoid being bitten off by grazing animals) or be discarded in favour of new ones. From a longer-term perspective the process resembles an arms race (Ekblom 1997, 1999, 2005a,c; see also Walsh 1994; Killias 2006). Arms races move faster when the medium of the struggle is mainly Information and Communications Technology. Tactically, running arms races requires repeated iterations of move, countermove and counter-countermove, as with evolution of safes and safebreaking (Shover 1996). More strategically, they require incorporation of variety and adaptability pre-and post-production (Ekblom 2005a).

Any assessment of products' risk and security must acknowledge the stage in the arms race the individual product (or its general class) has reached. Looking at security features and their match to risk should therefore involve understanding how far move and countermove have evolved (Ekblom 2005c). For example, does the product at risk of theft (move) have a registration label (countermove)? If the label is tampered with (counter-countermove) does it also have an *anti-tampering* function (counter3move) such as one which leaves an indelible mark on removal?[17]

Both offenders' and preventers' scripts may become progressively elaborated as the number of countermoves accumulates on each side ('switch on security measures'/ 'disable security measures' etc) although automation reduces reliance on preventers (Whitehead et al. (2007).

More broadly, risk/security assessments require sensitivity to the current state of play between offenders, products and preventers, and how this may change over the product's lifetime. *Crime-proofing itself must be future-proofed*. Again, performance/functional specifications are better than technical ones for future-proofing security standards. They also support the strategic requirement for *innovation and creativity* in design. Further such requirements could centre on *robustness across a range of possible 'risk futures'* (every design is a bet on the future), including deliberate pursuit of *variety* and *adaptability*. Industrial participants in the crime-proofing process, particularly those in the furiously-evolving consumer electronics sector, should find this a familiar perspective across *all* dimensions of design, which they must handle well to remain competitive.

Conclusions

In concluding, before addressing wider issues we revisit key aspects of Project MARC: CRAVED, the checklist approach, and the specifications for the MARC assessment scheme.

[17]Whitehead et al. (in press) use 'secure' for products whose security features are tamper-resistant.

What of CRAVED?

We drew heavily on the CRAVED risk factors as our starting point for developing the list of criminogenic features of products. However, we found it necessary to develop CRAVED in several ways. We emphasised a second dimension of risk, namely harm and criminal hazard; we increased the detail of the risk features themselves; and we organised these in terms of a combined and dynamic framework of crime foraging script and criminal motivation, which could, in potential, be extended to cover the perspective of the owner/carrier of the product, and which acknowledged bi-directional functions of features such as 'concealable'. CRAVED was a valid approach when the purpose was to rapidly and memorably communicate the concept of 'hot products' to diverse stakeholders, and we hope we retain its spirit here. However, the heuristic application and 'slogan' style may have revealed its limitations for use in the rigorous, practical context of MARC. We suspect the same limitation applies to all such formats, including, perhaps 'IN SAFE HANDS' developed for mobile phones by Whitehead et al. (2007).[18]

What of the Security Checklist?

Armitage and Pease concluded that checklists were not a sound basis for evaluating product security: "the progress of the research, and consultations with respondents and others, demonstrated that this approach would impose an artificial ceiling upon the exercise of ingenuity and skill in crime-reductive engineering and design" (2007, doi:10.1007/s10610-007-9039-2). It also concluded that the checklist approach understated the degree to which security is specific to product type.

> "For example, most of the security measures set out as Table 10 are specific to individual product types or pairs of product types. Since no general or common security features emerge, the justification for standardisation disappears. With hindsight, the classic matrix developed by Ron Clarke ... reflects such a richness of alternative methods that the checklist approach seems formulaic by contrast." (Armitage and Pease 2007, doi:10.1007/s10610-007-9039-2)

We agree with these views on the kind of checklist developed in Project MARC. However... we think these shortcomings derive from using *technical* rather than *functional* language, albeit for the laudable purpose of being user-friendly to the judges using the security assessment scale; and from insufficient rigour in currently-available terminology.

The alternative functional language developed here is, we believe, sufficiently rich, comprehensive, future-proofed and rigorous to support this task. It can moreover offer greater structure and focus than the '25 techniques of situational prevention' (e.g., Clarke and Eck 2003), although there is considerable overlap in content (e.g., 'anonymity'). Functional language can more readily resolve 'troublesome tradeoffs' with commercial interests, like cost and convenience, in designing a product (a major concern in Project MARC). It is attuned to adaptive offenders who can realise more of the potential *reward* from a product by investing more *effort*, or tolerating greater *risk*. (These three organising principles for the 25 techniques are 'functional' in themselves. Together with the remainder, provocation and guilt, they act as key mechanisms underlying the action of criminogenic or

[18]The memorability of any slogan may be gained at the expense of meaningfulness and accuracy of the headings that originators struggle to construct the acronym with.

criminocclusive features and security adaptations. However, their nature as 'interchangeable currency' in the 'foraging agenda' of adaptive offenders means they are not as firm a platform as usually believed.) Functional language can be incorporated at the earliest stages of the design process, when tradeoffs may be easiest to resolve (Ekblom 2005a). Finally the 25 techniques do not aspire to cover harm reduction; our own framework does (albeit embryonically).

The critical requirement is for a way of mapping between a largely 'universal, eternal' *functional framework* for security, and the currently-available and soon-to-be-available *technical realisations* for the class of product presently under scrutiny. The technical realisations must cover both security adaptations and criminal counter-adaptations. The mapping must be done whilst also allowing for changes in classes of products, given 'convergence' of, say, phone/camera/organiser; and changes of boundary between product and system/service. The mapping must explicitly address the *tradeoffs* between different security features themselves (such as anonymity *reducing* the probability of identification by offenders as valuable, versus *increasing* ease of resale). New technology can often relax these tradeoffs (Ekblom 1999, 2005a), though could accentuate them. Finally, the mapping must assume various 'standard risk environments' or 'habitats' to which the product is likely to be exposed, including, of course, presence and resources of offenders. The whole exercise becomes more one of intelligently following a structured and rigorous process, than of ticking boxes on a checklist. Whatever framework is used, though, there will always be subtle interactions requiring experience and judgement to supplement any structure we can give the task. But we believe that an ability to restate security against theft as a theoretical principle, explored above, will give an edge to both secure design and assessment of that design.

MARC Specifications Revisited

Returning to the MARC team's specifications, how do these now look, given our own thinking?

- 'Measure both risk and protection (ensuring that the two are commensurate)'. Preserved, although we now have 'risk and security' with meanings closely-linked in functional language, defined in-depth and embedded in a consistent semantic network, with greater emphasis on harm.
- 'Reflect the language of those who would be tasked with implementing it'. We have developed a language they must learn and apply in a disciplined way. This incorporates elements from crime prevention and security management; and deliberately supports parallel discourses of functional (including performance-based) and technical language. Designers in particular, and the engineers they deal with, should be comfortable moving between these discourses. (Ironically, the MARC paper omitted these disciplines from their list of stakeholders/users.) Other parties, such as manufacturers, retailers and consumers, should obviously receive reports translated into simplified and practical language. This emulates the 'food safety' model the MARC paper commends.
- 'Reflect the language of stakeholders from a variety of European states'. Our proposed language is perhaps initially more challenging to non-native English speakers, but we emphatically argue that the explicit definitions and consistent, interlocking semantic relationship among the terms, will ultimately facilitate international use.

- [The mechanism should] 'Be developed using a bottom-up approach, rather than imposing a mechanism upon key stakeholders.' We think that deliberate design of the *language* side of the mechanism, our focus here, should take account of the perspectives of the diverse users, and be tested out on them; but that ultimately this is a challenging task for experts. It is not surprising that Project MARC encountered difficulties.

Wider Implications

We think our proposed framework of risk and harm is generalisable to many basic acquisitive crime scripts beyond theft, and could be adaptable to cover violent crime. Likewise, the 'theoretical principle of security' approach could be applied more widely: preventing all property crime, at least, is about asserting asymmetry of ownership or control over some goods.

Ekblom's definition of crime prevention (e.g., Ekblom 2005b) as 'reducing the risk and potential seriousness of criminal events by intervening in their causes', needs modification. We must more clearly articulate the dual nature of risk; and replace the 'juridical' concept of 'seriousness' with that of harm. A possible redefinition could therefore be: 'reducing the risk of criminal events in terms of their probability of occurrence and consequent harm, by intervening in their causes.' Directly addressing the consequent harms, and the people, systems and other things they affect, is covered under the wider definition of *community safety* (e.g., Ekblom 2001 and see http://www.designagainstcrime.com/web/crimeframeworks) which could also now be revised.

There are implications, too, for CCO. The present exercise has taken the target of crime as focus and mapped out, in fine detail, through stages of a crime script, how its features interact with those of every other element of that framework: wider environment, enclosures, preventers, promoters; and aspects of the offender including what they value, their resources, perceptions, decisions and actions. This suggests ways forward for CCO in its application both as a guide for design of products and places and a means of integrating crime prevention more generally.

Crime science, like other sciences, must take its terminology seriously. We have shown how complex and subtle the field of product risk and security really is, and how the language must fit the task. To immodestly suggest a parallel of much greater significance, Antoine Lavoisier constructed a suite of terms and concepts for *chemistry*, dragging it from the confines of alchemy into the modern era, and establishing the conceptual platform on which the massive theoretical, empirical and practical advances of the 19th Century were built (let alone allowing Felson (1998) two centuries later to refer to 'the chemistry for crime'). Sadly that achievement did not halt the guillotine.

There is a broader issue of under-specification in crime science language. As with many disciplines, pressure for economical communication amongst aficionados has led to a 'default' approach to the use of terms. Everybody implicitly knows, that the 'risk' in the rational offender decision agenda of 'risk, effort and reward' (Cornish and Clarke 1986) refers to risk of harm to offenders through confrontation with victim or police, and any violence, arrest and punishment that follows. But there are other, neglected, risk dimensions: risk that effort may outstrip reward, risk of returning empty-handed, risk of wrongly assuming the product is saleable. All are significant from a wider 'foraging' perspective. This, together with the interchangeability of risk, effort and reward to the adaptive offender, noted above, suggests that re-organising the 25 techniques of situational prevention should be explored.

And crime science more generally must engage more systematically with harm. Doing so offers the prospect of integrating the parallel worlds of security, risk management and crime prevention and community safety. Surely this is a worthwhile prospect.

Appendix

Glossary of Key Terms

Note:

While these definitions were developed to cover theft, generalisation and/or adjustment should be possible to all types of crime.

Terms in *italics* are defined elsewhere in this glossary. Every effort has been made to design terms to interlock in a consistent semantic network.

Product refers to consumer electronic products such as mobile phones, personal digital assistants (PDAs), Laptop computers and MP3 music players.

Updates to these terms will be posted at http://www.designagainstcrime.com/web/crimeframeworks. 'Feature' has since been changed to mean 'any distinguisable structural element'. 'Feature' as used in this paper should now be re-labelled 'property'.

Affordance
The offender's capacity to see (criminal) utility in an object.

Attractive
Any *criminogenic feature* of product which causes the offender to form the intention to steal it, whether because of its perceived *value*, *vulnerability* (including visibility and distinctiveness) and capacity for *realisation of value*. Attractiveness is also in the eye of the offenders, in terms of what they themselves value and how well-equipped they are to take the product and realise its value.

Bycatch
Sea-fishing term denoting unwanted fish caught with the wanted ones. In *crime prevention*, property stolen incidentally through being associated with the target product, e.g., by being in same target enclosure (handbag, pocket, car or house).

Crime prevention
Reducing the *risk* of criminal events in terms of their probability of occurrence and consequent *harm*, by intervening in their causes.

Criminally hazardous
A product with the potential to cause *harm* through a criminal event such as theft or robbery.

Criminocclusive
A product's *features* which lessen the probability of its theft.

Criminogenic
A product's *features* which heighten the probability of its theft.

Feature
Any distinguishable physical or informational property of the product, which could be incidental or a deliberate adaptation by design.

Habitat
Ecological term for environment where a particular species population lives, and (through evolution) are adapted to. Crime prevention equivalent could be used to denote the environment/s where a particular product or a set of products typically exist. The *risk environment* is the *risk* dimension of the habitat.

Harm (harmful)
Detrimental effect of an event to a product and/or to people, institutions and systems associated with it. Includes harm to product itself during/after the crime; harm to owner or

other parties through loss or damage of product and its informational contents; harm to owner or other parties through collateral loss of or damage to enclosure/carrier (bag, house, car) and any *bycatch* of other goods taken and perhaps discarded; harm to owner/carrier/householder from theft or robbery event itself; propagation of further harm through misuse of product.

Hazard

Something with the potential to cause *harm*, e.g., through a theft event.

Herd immunity

Public health term denoting a type of immunity that occurs when the vaccination of the majority of the population (or herd) provides protection to un-vaccinated individuals. Crime prevention equivalent is where criminals' belief that secure products will dominate the 'catch' makes the attempt unworthwhile.

Incidental security

Features which unintentionally reduce a product's *risk* of theft.

Insecure product

An *insecure* product is one with strong *criminogenic, susceptible* and *criminally hazardous features*, but without effective *security adaptations/features* to reduce the elevated *risk* of theft to some acceptable level of both probability and *harm*. An insecure product is both *vulnerable* and *valuable* to the offender.

Product resilience

A product's potential to resist, limit or recover from *harm* sustained during/after the theft event.

Realisation of value

The process whereby possession of the stolen *valuable product* is converted into enjoyment, status display, misuse or resale.

Risk

1) The probability of a *criminally hazardous* event (here, theft), happening to the product; and
2) The *harmful* consequences of the event to the product and more significantly to various parties such as the owner/carrier of product or the home it is kept in, or some wider institution or system.

Risk environment

The environment or *habitat* of a particular product (or other entity): the place or system within which it is located, and which contains sources of criminal *risk* for it, including offenders and promoters; and sources of *security*, including various preventers, enclosures etc.

Secure, secure product

Something that is secure is less at *risk* of theft than expected on the basis of its *criminogenic, susceptible* and *criminally hazardous* features, because of specific *adaptations* to its *risk environment*. A secure product, more specifically, is one whose *risk* of theft is less than expected on the basis of its *criminogenic, susceptible* and *criminally hazardous features*, because it is deliberately *adapted* to its expected *risk environment* to be *criminocclusive*, *resilient* in itself to *harm*, designed for incorporation in a *resilient system* and *shielded against misuse*.

Security

Deliberate action by crime preventers (here, on a given product or its environment) which reduces product's risk of theft.

Primary security - reduces probability of *harmful* event

Secondary security - if event does happen, limits *harm* as it unfolds to product, owner and beyond - i.e., increases *resilience* of product and system

Tertiary security - limits propagation of harm that may occur post-event - i.e., increase *shielding against misuse* of product

Security adaptation

A *security feature* deliberately designed to make the product more *secure* against the *risks* typically to be encountered in its expected *habitat* or *risk environment*.

Security level

The *security level* of a product is the degree to which its security *features* outweigh its *criminogenic* and *criminally hazardous features*.

Shielded against misuse

A product incidentally/deliberately difficult for offender to use as resource for crime.

Susceptibility

The degree to which a product, its owner or related systems, people or institutions are capable of being *harmed* by a criminal event or its consequences.

System resilience

The potential of the owner/user, other parties and information systems associated with a certain product, to resist, limit or recover from *harm* sustained during/after theft event.

Threat

A subset of *hazard* originating from malevolent human intent.

Valuable product

A product with the potential to gratify some motivation of the offender - including for enjoyment, status display, misuse or resale. See also *realisation of value*.

Vulnerable product

Any product whose own features enable it to be seen and taken by the offender. Vulnerability incorporates all *criminogenic* factors associated with theft of product *except* the motivation it engenders in the offender.

References

Armitage, R., Clarke, R. V., Pease, K., Savona, E., Montauti, M., & Di Nicola, A. (2006). *Definition of final crime risk assessment mechanism to measure the risk of theft of electronic products and proof them against theft*. Final Report to European Commission.

Armitage, R., & Pease, K. (2007). Predicting and preventing the theft of electronic products. *European Journal on Criminal Policy and Research*, doi:10.1007/s10610-007-9039-2.

Clarke, R.V. (1999). *Hot products: Understanding anticipating and reducing demand for stolen goods*. Police Research Series Paper 112. London: Home Office Policing and Reducing Crime Unit.

Clarke, R. V., & Eck, J. (2003). *Become a problem solving crime analyst in 55 small steps*. London: Jill Dando Institute, University College London.

Clarke, R. V., & Homel, R. (1997). A revised classification of situational crime prevention techniques. In S. P. Lab (Ed.), *Crime prevention at a crossroads* (pp. 17–27). Cincinnati, OH: Anderson.

Clarke, R. V., & Newman, G. (2002). *Secured goods by design - a plan for security coding of electronic products*. London: Department of Trade and Industry.

Clarke, R. V., & Newman, G. (2005a). Modifying criminogenic products - what role for government? In R. V. Clarke, & G. Newman (Eds.), *Designing out crime from products and systems. Crime Prevention Studies, Vol. 18*, 7–84. Monsey, NY: Criminal Justice Press and Cullompton: Willan.

Clarke, R. V., & Newman, G. (2005b). Security coding of electronic products. In R. V. Clarke, & G. Newman (Eds.), *Designing out crime from products and systems. Crime Prevention Studies, Vol. 18*, 231–265. Monsey, NY: Criminal Justice Press and Cullompton: Willan.

Clarke, R.V., & Newman, G. (2006). *Outsmarting the terrorists*. Praeger Security International.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activities approach. *American Sociological Review, 44*, 588–608.

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

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. In R. V. Clarke (Ed.), *Crime prevention studies, Vol. 3*, 151–196. Monsey, NY: Willow Tree Press.
Cornish, D., & Clarke, R. V. (Ed.) (1986). *The reasoning criminal*. New York: Springer-Verlag.
Eck, J. E., Clarke, R. V., & Guerette, R. T. (2007). Risky Facilities: Crime concentration in homogenous sets of establishments and facilities. In G. Farrell, K. Bowers, S. Johnson, & M. Townsley (Ed.), *Imagination for crime prevention: essays in honour of Ken Pease. Crime Prevention Studies*. Monsey, NY: Criminal Justice Press.
Ekblom, P. (1994). Proximal circumstances: a mechanism-based classification of crime prevention. In R. V. Clarke (Ed.), *Crime prevention studies, Vol. 3*, 185–232. Monsey, NY: Willow Tree Press.
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, 24*, 249–265.
Ekblom, P. (1999). Can we make crime prevention adaptive by learning from other evolutionary struggles? *Studies on Crime and Crime Prevention, 8*, 27–51.
Ekblom, P. (2000). The conjunction of criminal opportunity - a tool for clear, 'joined-up' thinking about community safety and crime reduction. In S. Ballintyne, K. Pease, V. McLaren (Ed.), *Secure foundations: key issues in crime prevention, crime reduction and community safety*, (pp. 30–66). London: Institute for Public Policy Research.
Ekblom, P. (2001). The conjunction of criminal opportunity: a framework for crime reduction toolkits. Retrieved 31/01/07 from Crime Reduction website: http://www.crimereduction.gov.uk/learningzone/ccofull.doc
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, Vol. 13*, 131–203. Monsey, NY: Criminal Justice Press.
Ekblom, P. (2002b). 'Towards a European knowledge base' and 'The five i's: Experimental framework for a knowledge base for crime prevention projects'. In *European Crime Prevention Conference 2002, 1*, 62–97. Copenhagen: Danish Crime Prevention Council.
Ekblom, P. (2005a). Designing products against crime. In N. Tilley (Ed.), *Handbook of crime prevention and community safety* (pp. 203–244). Cullompton, UK: Willan.
Ekblom, P. (2005b). The 5Is framework: Sharing good practice in crime prevention. In E. Marks, A. Meyer, & R. Linssen (Eds.), *Quality in crime prevention*. Hannover: Landespräventionsrat Niedersachsen.
Ekblom, P. (2005c). 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, & N. Tilley (Eds.), *Crime science: New approaches to preventing and detecting crime* (pp. 27–55). Cullompton, UK: Willan.
Ekblom, P. (2007). Making offenders richer. In G. Farrell, K. Bowers, S. Johnson, & M. Townsley (Eds.), *Imagination for crime prevention: Essays in honour of Ken Pease. Crime prevention studies*. Monsey, NY: Criminal Justice Press.
Ekblom, P., & Tilley, N. (2000). Going equipped: Criminology, situational crime prevention and the resourceful offender. *British Journal of Criminology, 40*, 376–398.
Farrell, G. (2001). Crime prevention. In C. D. Bryant (Ed.), *Encyclopaedia of criminology and deviant behaviour* (pp. 124–133). London: Taylor and Francis.
Felson, M. (1986). Linking criminal choices, routine activities, informal control, and criminal outcomes. In D. B. Cornish, & R. V. Clarke (Eds.), *The reasoning criminal* (pp. 119–128). New York: Springer-Verlag.
Felson, M. (1998). *Crime and everyday life*, 2nd edn. Thousand Oaks, CA: Pine Forge Press.
Felson, M. (2006). *Crime and nature*. Cullompton: Willan.
Gamman, L., & Pascoe, T. (2004) 'Design out crime? Using practice-based models of the design process'. *Crime Prevention and Community Safety Journal, 6*, 37–56.
Garwood, J. (2004). *Perceiving opportunity? Reawakening the criminological imagination?* Paper presented at British Criminological Society conference, Leeds University, England, July 2004.
Gibson, J. J. (1979). *The ecological approach to visual perception*. Boston: Houghton Mifflin.
Gill, M. (2005). Reducing the capacity to offend: Restricting resources for offending. In N. Tilley (Ed.), *Handbook of crime prevention and community safety* (pp. 306–328). Cullompton, UK: Willan.
Gill, M. (2006). Introduction. In M. Gill (Ed.), *The handbook of security* (pp. 1–18). Basingstoke: Palgrave Macmillan.
Haddon, W. (1980). Options for the prevention of motor vehicle crash injury. *Israeli Journal of Medical Science, 16*, 45–68.
Johnson, S. D., & Bowers, K. J. (2004) The stability of space-time clusters of Burglary. *British Journal of Criminology, 44*, 55–65.

Killias, M. (2006). The opening and closing of breaches. A theory on crime waves, law creation and crime prevention. *European Journal of Criminology, 3*, 11–31.
Loss Prevention Certification Board (2006). *Draft Requirements and testing procedures for the LPCB approval and listing of "theft resistant" electronic products*. Watford: BRE Certification.
Norman, D. (1998). *The psychology of everyday things*. Basic Books.
Orwell, G. (1946) Politics and the English Language. In S. Orwell, & I. Angus (Eds.), *The collected essays, journalism and letters of George Orwell*. London: Secker & Warburg.
Pease, K. (2001). *Cracking crime through design*. London: Design Council Publications.
Pease, K. (2005) No through road: Closing pathways into crime. In K. Moss, & M. Stephens (Eds.), *Crime reduction and the law* (pp. 50–66). London: Routledge.
Savona, E., & Di Nicola, A. (2002). Assessing the risk of organised crimes: A user-friendly methodology for law enforcement agencies and policy-makers.
Shover, N. (1996). *Great pretenders: Pursuits and careers of persistent thieves*. London: Westview Press/ Harper Collins.
Tilley, N. (1993). *After Kirkholt: Theory, methods and results of replication evaluations*. Crime Prevention Unit Paper 47. London, UK: Home Office.
Villagrán, J. C. (2006) *Vulnerability: A conceptual and methodological review.* Studies of the University: Research, counsel, education. Publication series of UNU Institute for Environment and Human Security, UNU-EHS, No. 4.
Walsh, D. (1994). The obsolescence of crime forms. In R. V. Clarke (Ed.), *Crime prevention studies, 2*, 149–164. Monsey, NY: Willow Tree Press.
Whitehead, S., Mailley, J., Storer, I., McCardie, J., Torrens, G., & Farrell, G. (2007). Mobile phone anti-theft design: a review. *European Journal on Criminal Policy and Research*, doi:10.1007/s10610-007-9040-9.
World Health Organisation (2004). *Handbook for the documentation of interpersonal violence prevention programs*. Geneva:WHO.
Wortley, R. (1996). Guilt, shame, and situational crime prevention. In R. Homel (Ed.), *The politics and practice of situational crime prevention, crime prevention studies, vol. 5* (pp. 115–132). Monsey, NY: Criminal Justice Press.
Wortley, R. (2001). A classification of techniques for controlling situational precipitators of crime. *Security Journal, 14*, 63–82.
Zipf, G. K. (1950). *The principle of least effort*. Reading, MA: Addison-Wesley.