The Misdeeds and Security Framework (M&S)

January 2008
Prof. Paul Ekblom

Christopher Booker argues that all stories share only seven basic plots (‘The Quest’ etc). Likewise, the ‘Misdeeds and Security’ framework (M&S) is an attempt to compress and simplify the huge and ever-proliferating array of criminal offences into a manageable, limited and structured set which can be used to guide crime risk assessment and identify the scope for preventive interventions.

M&S is an aid to forecasting which maps out the generic types of crime (and related) risks that may be associated with a particular kind of new technology or design of product, place, procedure or system; and the counterpart opportunities for prevention. It is thus an aid to Crime-Proofing, Crime Risk Assessment and Crime Impact Assessment. In line with the usage in the Definitional System of Risk and Security, risks have the twin dimensions of probability and harm associated with a particular crime or Community Safety hazard.

Disruptive technologies are normally considered to be those that re-write the rules in a market segment by making something much easier or cheaper to do. M&S in effect is a means of thinking about criminally disruptive technologies – those which re-write the balance of advantage and/or motivation between offenders and preventers. (The theme of script clashes between offenders and preventers is pursued in depth in Conjunction of Criminal Opportunity – Dynamic.

M&S complements the Conjunction of Criminal Opportunity Framework [CCO Classic] by specifying the range of types of crime whose causation and prevention we wish to consider. Taking the opposite perspective, if we have a particular kind of crime risk, identified through M&S, whose causes and prevention we wish to look into, we can then be guided by CCO to investigate in depth. Within the scope of M&S, a particular focus on Misappropriation (theft) links it to the Definitional system of risk and security and to Clarke’s CRAVED framework for identifying ‘hot products’.

Origin and Background

The demand for the M&S framework arose from work to systematically and rigorously identify future crime risks and crime prevention opportunities posed by advances in hard science and technology (a need identified by the Police Science and Technology Strategy Group in 2002), in the context of a growing governmental and police interest in ‘crime futures’ more generally. The content of the framework drew on understandings developed through the research conducted in support of the Design Against Crime initiative and the Crime Prevention Foresight Panel of the UK Government’s Crime Reduction Programme (1998-2003), in particular from studies commissioned through the Design Council from Cambridge, Salford and Sheffield Hallam Universities. (Design Council 2000; Learmont 2005).

A multidisciplinary group of scientists, social scientists, engineers, forensic scientists, and police, chaired by the UK Home Office, used and refined M&S to review candidate scientific and technological innovations suspected of having crime implications, identify significant ones for further investigation and report to the Strategy Group with recommendations for action or inaction as appropriate. The wider purpose was to ‘alert, motivate and empower’ scientists, technologists and designers to think thief, to recruit them as ‘scouts’ to spot crime risks/preventive opportunities within their diverse fields and to inform design of new tools and technologies for preventing crime.
M&S was incorporated in the reports of the Government Foresight Project ‘Cyber Trust and Crime Prevention’ (Collins and Mansell 2005) and contributed to ‘crime scenarios’ for the subsequent ‘Intelligent Infrastructure’ project (Ekblom 2006). It also features in an entry on ‘crime and communication technology’ in the International Encyclopedia of Communication (2008).

M&S now imparts ‘futures’ perspectives to the Design Against Crime Research Centre’s work, supporting its objective to empower designers to think thief by identifying the broad kinds of crime risk facing their products.


Abstract

This chapter describes an approach to future scanning recently developed for the group responsible for delivering the UK Police Science and Technology Strategy. The approach enables those concerned with preventing crime to consider a range of scientific and technological innovations (STIs) and to anticipate consequent crime risks and crime reduction opportunities including countermeasures in an arms race. It also seeks to alert, motivate and empower the wider science and engineering community to act as scouts in this task to systematically think crime.

The approach centres on the so-called ‘M and S’ framework and the Conjunction of Criminal Opportunity. It can potentially integrate crime reduction, hard science and technology in a rigorous yet practical way connecting with mainstream crime science and wider crime futures work.

References – M&S


References – Other

Design Council (2000). Design Against Crime. A


The Misdeeds and Security Framework

The Ms test for crime risks

Each selected STI is considered in relation to the possibility that it is at risk of being:

- **Misappropriated** – property stolen, information stolen or made unavailable;
- **Mistreated** – property damaged, people assaulted, self-harm, information integrity compromised;
- **Misused** – as tools/ weapons for crime to support a specific Modus Operandi, or to be consumed as illegal drugs; this heading includes countermeasures against police or forensic tactics, and in particular those which Mislead attempts to identify people or property;
- **Misaligned** – having unintended adverse side effects, eg on privacy and other Human Rights, exacerbating fear, or creating stigma.

Note that, given the complexity of some crimes (Ekblom 2003), it may necessary to use several Ms in conjunction to characterise the crime risk – such as ‘misappropriation of information leading to its misuse’.

The Ss test for crime reduction opportunities

We identify how the STI might be exploited to make persons, physical goods and buildings, means of payment, environments or electronic systems, intellectual property or information:

- **Mistaken** – errors are also made by public or police which whilst not illegal serve to constrain or misdirect crime reduction activity (e.g. false alarms, arresting the wrong person) – this is obviously central to the technology of sensory systems, whether in preventing or reacting to crime; serious mistakes can of course lead to Miscarriages of justice;
- **Mistrusted** – where for example, individual or corporate victims of crime do not report the incidents to the police due to antipathy, or reasoned judgement that there are risks such as disclosure to media or witness intimidation – the negative consequences including not just individual crimes not dealt with, but police lacking a strategic picture of the nature and extent of a given problem;

The Ss test for crime reduction opportunities

We identify how the STI might be exploited to make persons, physical goods and buildings, means of payment, environments or information:

- **Secured** against theft – resistant to theft, indicating that theft has happened, or recoverable/ restorable to owner;
- **Safeguarded** against damage – resistant to, fail-safe in, or indicative of damage;
- **Shielded** against misuse – resistant to misuse, including for attacks on law enforcers, or indicative of misuse, including tamper-evidence;
- **Supporting** – justice/ crime reduction/ community safety, covering
  » Supporting law enforcement – e.g. facilitating arrest/immobilisation;
  » Supporting detection – e.g. forensics, identification;
  » Supporting punishment – e.g. tagging/ curfewing of offenders;
  » Supporting emergency action – covering response to accidents etc;
  » Supporting police-public relations – e.g. IT-based tracking/ maintenance of contacts;
  » Supporting reassurance – e.g. surveillance technology;
- **Scam-proofed** – resistant to or indicative of fraud/ counterfeiting/ smuggling;
- **S**ivilised – environment resistant or repellent to misbehaviour and conducive to good behaviour;
- **Slip-proofed** – resistant to mistakes;
- **S**ertain to report – facilitating reporting of crime incident/safety problem to police;
- **Straightening** adverse side-effects – see ‘Troublesome tradeoffs’ below.

Some terms need defining further. **Resistance** includes something akin to the concepts of ‘primary, secondary and tertiary safety’ from the accident prevention world (stopping the crime happening in the first place, limiting it once under way and limiting adverse consequences). **Indicativeness** contributes to secondary and tertiary resistance, e.g., tamper-evident food containers help people avoid poisoning or fraud and initiate law enforcement or wider preventive action.

Note that some crime reduction opportunities and crime risks emerge, not from a single STI, but from two or more in combination – for example, a new ceramic gun with a new propellant bypassing multiple security detector systems. These pose particular challenges in that knowledge from two technological or scientific fields, plus consideration of crime opportunities and risks, must get into one head, or one interacting group.

### The (counter)n issue

Being an arms race (see Gearing up against Crime), it is sometimes necessary to refer to counter-countermeasures etc. This can be confusing if not carefully related to ‘goodies or baddies’. For example, our draft assessment of Biometrics began by spelling out risks of crime which, we realised, were in fact risks of criminal countermeasures (e.g. guessing password) against existing security measures (the password system) intended to protect against an initial ‘primitive’ crime risk from unrestricted access. A convention became necessary to spell out the degree of recursion at each stage – e.g. 1) risks of crime, 2) opportunities for CR, 3) risks of criminal countermeasures, 4) security counter-countermeasures. However, schemes like this can, if too rigidly followed, hinder comprehensible storytelling.

### Troublesome tradeoffs

Security – protecting against the Ms and delivering the Ss – is just one inherent feature which must be incorporated without jeopardising a product’s main function or wider usability (see Conjunction of Criminal Opportunity – Dynamic and Crime Prevention Through Environmental Design). Troublesome tradeoffs for crime resistance include:
• Safety
• Liability
• Convenience
• Reliability
• Capital/ running costs
• Electromagnetic compatibility
• Privacy and freedom
• Profit
• Social inclusion
• Sustainable environment
• Legal/ ethical norms
• Design freedom