An alternative formulation of SCP principles – the 11Ds (and counting)

Paul Ekblom & Alex Hirschfield

ual: university of the arts london central saint martins

University of HUDDERSFIELD

DaC DESIGN AGAINST CRIME RESEARCH CENTRE

Applied **Criminology** Centre

Organising our knowledge for practice, research and theory

- Most guides in SCP and POP use 3 frameworks for organising knowledge: SARA process, PAT for causes and interventions and 25 Techniques for practical action
- Not the only ways, not necessarily the best, but the first
- Other possibilities exist, however, and new ones can be created
- Consider our knowledge like a rough diamond
  - A major task for us is to cut and polish facets into it, to give us different views and windows into the rich interior
  - One such facet is the 11 Ds…

Project background

- Project – help Security Managers (SM) of large, crowded or important sites to control Hostile Reconnaissance (HR) by terrorists
  - If you control HR, you reduce risk of main attack – by terrorists, armed robbers, industrial spies, etc
- Tasked to draw in ideas and approaches from SCP and POP, to enrich thinking of Security practitioners

Background

- This led ultimately to an interactive toolkit which is now ready for launch on a secure website
- Presented it at a side-show at ECCA last year
- Now aim to describe one element of that toolkit which required us to look again at existing facets of ECCA knowledge

Capturing user requirements

- Spoke to security advisers
- Interviewed SMs (end users) singly/ in groups
- Visited sites

- Found that:
  - Sites highly diverse and often complex
  - SMs had very variable levels of knowledge and available time
  - High-impact/low probability events tricky to plan and budget for

- Toolkit had to handle all these issues, bringing security & SCP together in a way that was
  - Inclusive
  - Focused
  - Generic and generative
  - Offered design freedom for managers of all levels of sophistication working in diverse sites
  - Gave them mental schema to adjust knowledge of what works at theoretical/practical levels to their own working context

Learning from Security – thin pickings

- Interventions
  - Deter
  - Detect
  - [That's it really!]
- Approaches
  - Effects-based approach – focus hard on adversary's goals and try to block them

What did SCP-POP offer?

- PAT took us no further than existing security knowledge (though language different)
- SARA as a process was not particularly adapted to assessing risks of a known category of malicious behaviour in a known site
- What the perpetrator is trying to do and how seemed the only common organising factors behind helping SMs understand and control HR
- So we decided to begin by focusing on what the perpetrator is trying to achieve (effects), how (scripts), and then flip to how the security team can control this
- For this purpose 25 Techniques looked a more promising start

25 Techniques

- We looked at 25T at **principle** (5 columns) level, 25 **category** level, and **exemplar** level
- Not all principles appeared immediately suitable for HR – e.g. *Provocation*
- Not all categories suitable for highly motivated perpetrators – e.g. *Making compliance easier*
- Many cells were already known to security – e.g. *Control Access*
- Few existing exemplars leapt out at us; though we did try to fill a table with HR illustrations, results disappointing
- What to do?

Moving on from 25T

- Wanted to retain the Principles: Methods : Exemplars structure of 25T (and 5Is) – a good way of organising practice knowledge
- Wanted to link Principles more clearly to ‘Think Perpetrator’ and to causal mechanisms
- And wanted to link Methods to ‘Practical actions’
- So we came up with a *wider* range of control Principles and a *narrower* range of generic control Methods

Control Methods

- Methods came from
  - Relevant ones from 25T cells and exemplars
  - Security practice guides

Control Methods

ACCESS CONTROL

Screening and questioning of individuals entering a site at fixed points (at entrance, internally)

- Usually purpose-designed layout (reception desk, gate, physical and visual barriers) and technology (bar code readers, swipe cards, tickets, cameras, biometrics-finger/iris scans for extreme circumstances).

SECURITY ESCORT

- Accompanying the movement of visitors on site.
- Ensuring that no one is left unattended.
- Controlling what they can see or do and where they can go.

INFORMATION / MISINFORMATION

Includes careful use of communication and of imitation security kit, to complement other methods.

- Disguising of equipment/targets.

CONTROL MOVEMENT AND BEHAVIOUR

of perpetrator and other users

- Directing where people go and challenging their movement through a site or location – has potential to make perpetrators stand out from the crowd.
- Spelling out rules and regulations (e.g. "No photography or use of mobile phones").

SURVEILLANCE & RESPONSE

No contact unless suspicion aroused

- Static (security staff or CCTV cameras at fixed location(s)).
- Mobile (via human patrol, or switching sensors – e.g. flipping between CCTV cameras).
- Use of sensors/alarms to detect unauthorised access.
- May or may not be supported by purpose designed layout and technology.
- Response to unlawful / unexplained intrusions / alarm events.

CHALLENGE

- Contact without prior suspicion aroused.
- High visibility stopping, searching, questioning individuals at random.
- Legitimacy maintained.

EXIT CONTROL

Screening and questioning of individuals at fixed points (via exit, entrance, other fixed points).

- To exterior / interior zones
- Usually purpose-designed layout (reception desk, gate, physical and visual barriers) and technology (bar code readers, swipe cards, tickets, cameras, biometrics – finger / iris scans for extreme circumstances).

OTHER

You may have additional methods – we would be interested to hear about them.

Control Principles – what exactly *are* they?

- The Principles didn't come easily – several iterations and reflections
- Eventually iterations became clearer when we were able to articulate what we thought they were:
  - ***How the interventions are intended to influence the offender in the proximal crime situation***
  - So for example this distinguishes between 'supply information/misinformation' as Method, and 'Deceive perpetrators' as Principle
  - Generally linked through a sentence – 'Deceive perpetrators *by* misinformation'… 'Defeat perpetrators *by* controlling movement and behaviour'
  - Often a many : many relationship between Principle and Method

Control Principles

Principles came from diverse sources including 25T, Security, Conjunction of Criminal Opportunity

- Risk (Deter), Effort and Reward (Discourage)
- Physical blocking (Defeat)
- Deflection (Deflect from/Direct to)
- Enforcement (Detect, Detain)
- Restrict resources for offending (Disable/Deny)
- Offender-oriented/ reverse Precipitation (Demotivate, Disconcert)
- Disconcert was a new one – idea suggested by one of the Security Managers in trial

Control Principles

DETER-KNOWN

perpetrator knows what the risk of exposure is, and judges it unacceptable, so abandons/aborts reconnaissance attempt.

DETER-UNKNOWN

perpetrator is rendered uncertain what control methods they are up against, so again judges risk of exposure unacceptable.

DETECT

facilitate detection of perpetrator by:

- arranging environment and procedures to make them more likely to betray perpetrators' illegal intentions;
- making the actions of legitimate visitors more distinctive;
- briefing staff on what is normal behaviour;
- and training staff to detect suspicious behaviour, and how to respond.

DEFEAT / DELAY

physically block access and movement or block/obscure the information that the perpetrator wants to collect.

DISCOURAGE

perpetrator perceives effort too great, reward too little, relative to risk, so abandons/aborts attempt.

DEMOTIVATE

awakening, within perpetrator, motives/emotions contrary to the mission, e.g. empathy with potential victims.

DISCONCERT

causing perpetrator to make involuntary movement or otherwise to become startled.

DECEIVE

perpetrator acts on wrong information on risk, effort, reward, where to go etc, and is exposed to immediate arrest or protracted intelligence collection, frustrated, or mistakenly decides not to select this site as target.

DISABLE / DENY

equipment helpful to perpetrators such as cameras.

DEFLECT / DIRECT

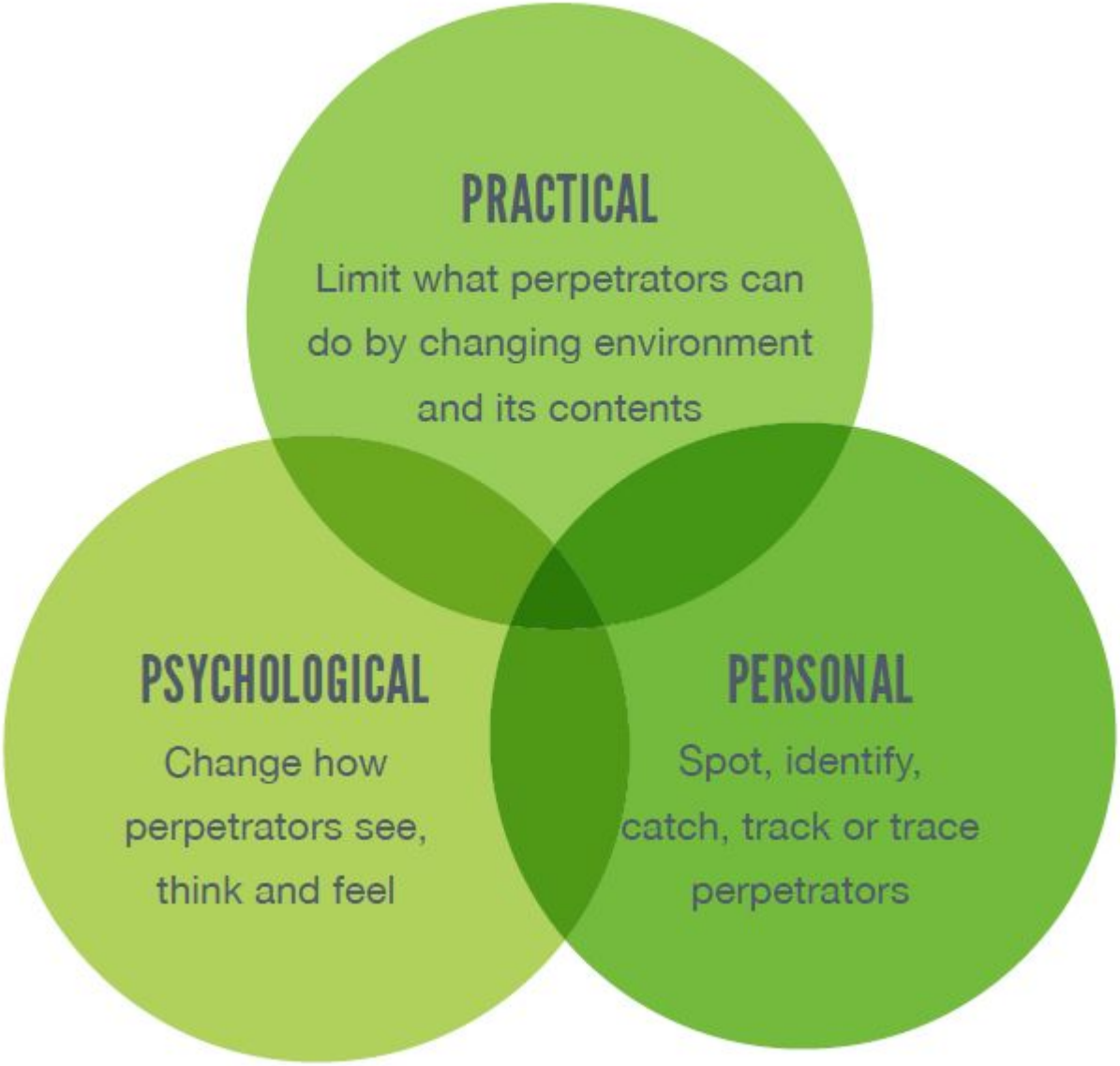
perpetrators towards/away from place or behaviour.

DETAIN

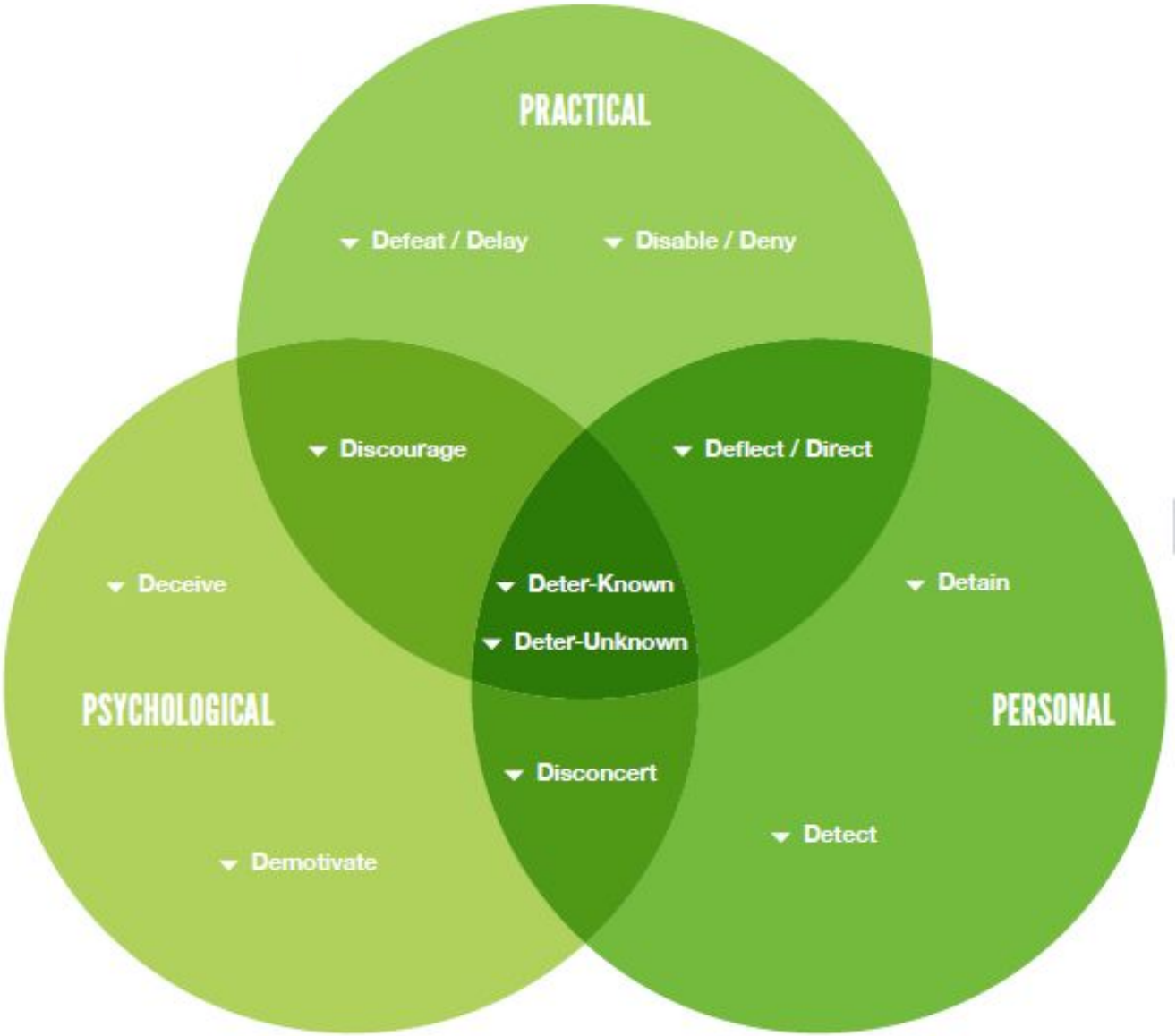
once perpetrators detected, they must be caught and held subject to legal powers (or at least, credible identifying details must be obtained so they can be traced).

Principles – Taming the variety

- Realised we had to organise 11 into subsidiary groups
- Bit of a struggle
- But eventually…



Principles – Taming the variety



After Principles and Methods – what?

In the toolkit, after taking users through Principles & Methods, they were

- Invited to select appropriate Methods for particular script scenarios (e.g. to tackle perpetrator entering site control room, pursuing goal of avoiding detection)
- Presented with Method-specific options
- Invited to list concrete operational or preparatory Tasks to make the Method happen; and specific People to undertake them
- Hence a guided descent from generic Principles and Methods to detailed practicalities of action

Toolkit Logic

How did it go?

- We were conscious of clients breathing down our necks saying ‘simplify!’
- But felt we had to help users cope with the complexity of their sites
- Trial iterations in workshops and on sites revealed
  - Right from start practitioners of all levels (both security advisors and SMs) grasped the principles : methods distinction
  - SMs appreciated the mix of recipe and flexibility, and being made and helped to *think* rather than following checklist
  - Many SMs wanted to rush off and apply the toolkit, and to use it in ways we hadn’t anticipated e.g. training staff

Benefits of using control Principles + Methods

- If SMs know how control methods **work** upon perpetrators, they can **better design practical solutions**, **monitor performance** and **consider improvements**
- Principles are **generative**
  - Can help SMs produce fresh ideas for **new contexts** or where **no known methods** yet exist
  - Fuel adaptation/innovation to keep up with **adaptive offenders**
  - Avoid SMs simply '**designing down**' to fixed list
- Principles are **transferrable**
- Principles **organise practice knowledge**
- Best approach is to use principles and methods in parallel
- Yin and Yang can perhaps spark new research, new theory too?

Control *methods*

Distilled from interviews, security and SCP literature

- **Access control**
- **Exit control**
- **Constraining specific movement and behaviour** – of perpetrator and other users
- **Surveillance**
- **Escort**
- **Random confrontations/challenges**
- **Information/misinformation**

Control principles and Conjunction of Criminal Opportunity

The Ds	CCO
Defeat	Target, Enclosure, Environment
Disable/deny	Resources for crime
Direct/deflect	Presence of offender
Deter-known	Perception/anticipation
Deter-unknown	Perception/anticipation
Discourage	Perception/anticipation
Demotivate	Readiness to offend
Deceive	Perception/anticipation
Disconcert	Readiness to offend, presence, perception/anticipation
Detect	Presence of offender
Detain	Presence of offender

Focusing control Methods & Principles on individual HR perpetrator scenarios – *Control* Scenarios

	...whilst...	HR goal			
		A. Obtain strategic information to facilitate selection/ execution of terror attack	B. Obtain immediate tactical information to facilitate ongoing PHR	C. Bring in/ use/ take out equipment to serve other goals	D. Avoid exposure, arrest, tracing
Movement/ posi	0. Remotely researching site				
	1. Approaching site				
	2. Accessing site				
	3. Moving in site				
	4. Exiting site –				

Select/design a Control Method:

- **Access control**
- **Exit control**
- **Constraining movement and behaviour**
- **Surveillance**
- **Escort**
- **Random confrontations**
- **Info/misinformation**

To...

Defeat
Disable/deny
Direct/deflect

Deter-known / unknown