Resilience to (Cyber)Crime – a View from Design and Crime Science

Paul Ekblom

EPSRC cSALSA project / National CyberSecurity Centre workshop on **Citizen-Centred Cyber Resilience: Building Resilient Communities from the Ground up** 4 March 2020

This work was supported by the research project, ACCEPT: Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks" (http://accept.cyber.kent.ac.uk/), funded by the EPSRC (Engineering and Physical Sciences Research Council) in the UK, under grant number EP/P011896/1 and EP/P011896/2.

Coming up

- Defining resilience – diversity of concept
  - Risk, prevention and resilience – how they relate
  - Different aspects of resilience to focus on
- The challenges facing cyber resilience efforts
  - Adaptive offenders
  - Arms races and co-evolution
- The human side of resilient security (and resilient crime)
  - The roles people and organisations play in crime and civil life
  - Professional know-how in security
  - Involving 3rd parties in security – mobilisation and behaviour change

Resilience – Many definitions, all with relevance to security

- Ecology, Engineering
  - The capacity of a system to absorb disturbance and reorganise while undergoing change so as to retain and/or quickly recover essentially the same function, structure, identity, and feedbacks
- Organisational
  - The ability of an organisation to adapt and survive in the face of threats, including the prevention or mitigation of unsafe, hazardous or compromising conditions that threaten its very existence
- Economic/business
  - The ability of a local economy to retain function, employment and prosperity in the face of the perturbation caused by the shock of the loss of a particular type of local industry or employer
- Network
  - The ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation
- Control system
  - Ability to maintain state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature
  - Addressing complex control system interdependencies, including human-systems interaction
- Security – DHS
  - Ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions
- *Note salience of **adaptation** throughout…. But place to start is **risk***

Risk, Prevention and Resilience – roughly distinguished

Resilience of…

- We can focus on different aspects of resilience in security
  - Main cyber system/network – the **asset** we are protecting/ preserving
    - **Intrinsically** resilient (architecture – redundancy, modularity etc)
    - Resilience conferred by **security features/add-ons** (back-ups, firewalls etc)
  - Protective security – **resilience of security features/elements** themselves, and entire **security system**, against attack/countermeasures
- Note also that **Offenders and OCGs/networks** can be resilient or fragile
  - Their planning, plans, preparations, actions, recruitment, trust can be disrupted
  - by Law Enforcement, Administrative Action or indeed rivals in crime

The Challenges that Cyber Resilience must face

- Which challenges to resilience are most relevant to **(cyber)security**?
  - **Threat** – differs from accidental/natural hazards
    - Malintent – purposive, goal-directed
    - Accessibility and nature of attack surface and wider environment of opportunity
    - Capability/resources/affordances for crime
  - **Scale** of challenges – many **crimes/opportunities/offenders**, diversity of **contexts** for crime
  - **Speed of change** (e.g. exponential growth of IoT) – makes it harder for law, law enforcement, security to adapt in turn
  - **Complexity** of interactions between components of systems, services, users makes it harder to predict, cope with diversity of combinations…
  - **Lack of constraints** – cyber world defined by codes/conventions, not physical limits e.g. inertia, space, time

Offender Actions/ Affordances – Misdeeds & Security Framework

- Neither Protect nor Prepare get to grips with the **adaptation** dimension of crime and security
  - **Adaptive, innovative offenders**
- What adaptive offenders get up to…

Mistreatment (damage/ harm)

Misappropriation (theft)

Mishandling (e.g. fraud)

ICT as Target of crime

Misuse (as tool/weapon)

Misbehaviour (nuisance, conflict)

ICT as Contributor to crime
eg **resource**

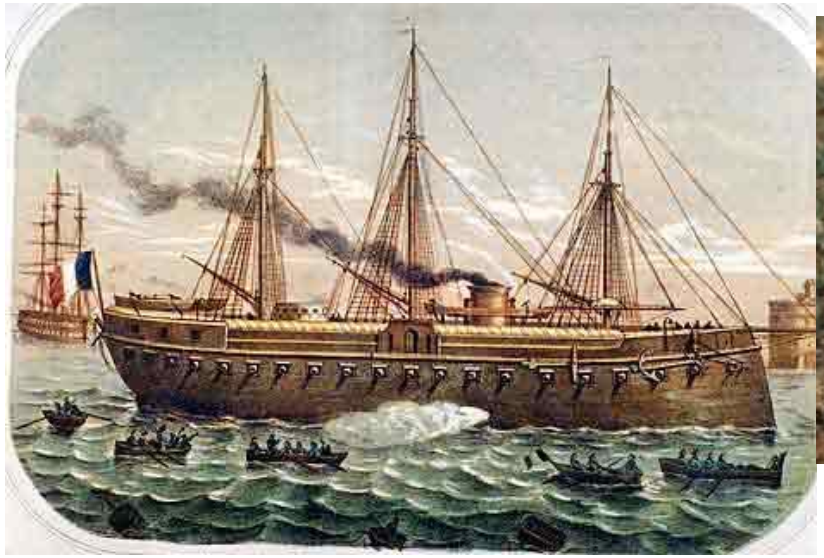
Arms races – cultural co-evolution of crime and security

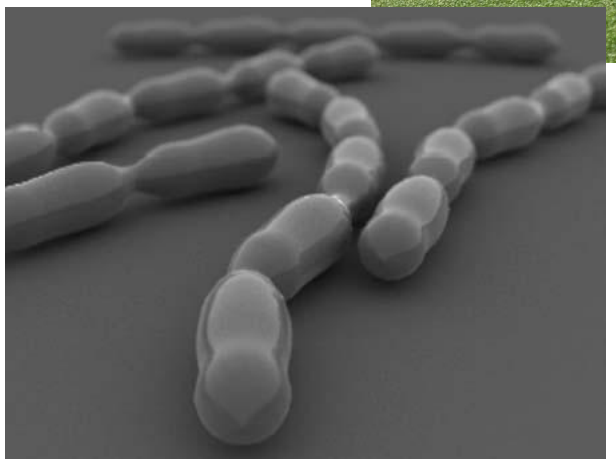
- Adaptability covers **both sides**
- We can see cultural **co-evolution** in **arms races** between offenders & security
  - Safes and safebreakers
  - Coders and codebreakers
  - Arms and armour
  - Detection/concealment of weapons, explosives
  - Well-documented example – Rick Brown on car theft
- The changing social and technological **background** can favour first one side, then the other
  - e.g. radically better cutting tools, resistant materials emerge at various times
- Hence strategic importance for security side of developing, disseminating, maintaining
  - **Capacity to out-anticipate** and
  - **Capacity to out-innovate** adaptive offenders

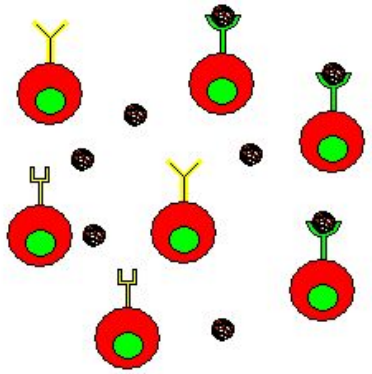
- Encourage variety of security solutions (if not, crack one, crack all)
  - Creativity, innovation, evidence-based and theoretically/practically sound proposals, tested iteratively
  - Design to performance standards/ generic principles, not fixed construction standards
  - Avoid rigidity – crime changes but your security can't
- Study offender resources – current and future technologies, services
  - Block their access to the resources
  - Lock them into particular approaches
  - Limit their R&D, security by obscurity
- Future proofing
  - Anticipation
  - Upgradeability
  - Pipelines of innovations
  - Ready to deploy new security at speed/scale

Learning from other Co-evolutionary Struggles

- Military
- Predator-prey
- Pest-farmer
- Bacteria-antibiotic
- Immune system-virus





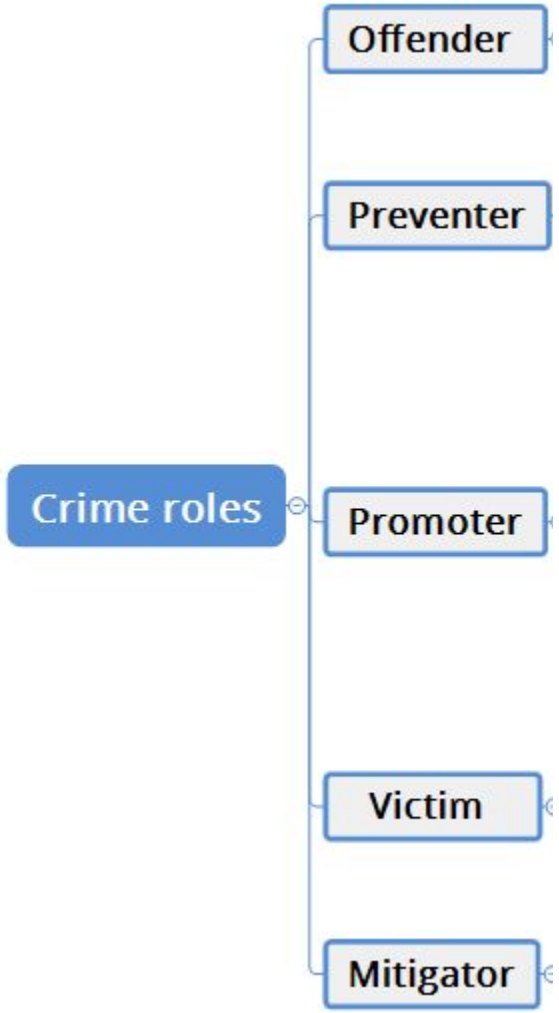


https://www.researchgate.net/publication/238196942_Can_We_Make_Crime_Prevention_Adaptive_by_Learning_from_Other_Evolutionary_Struggles

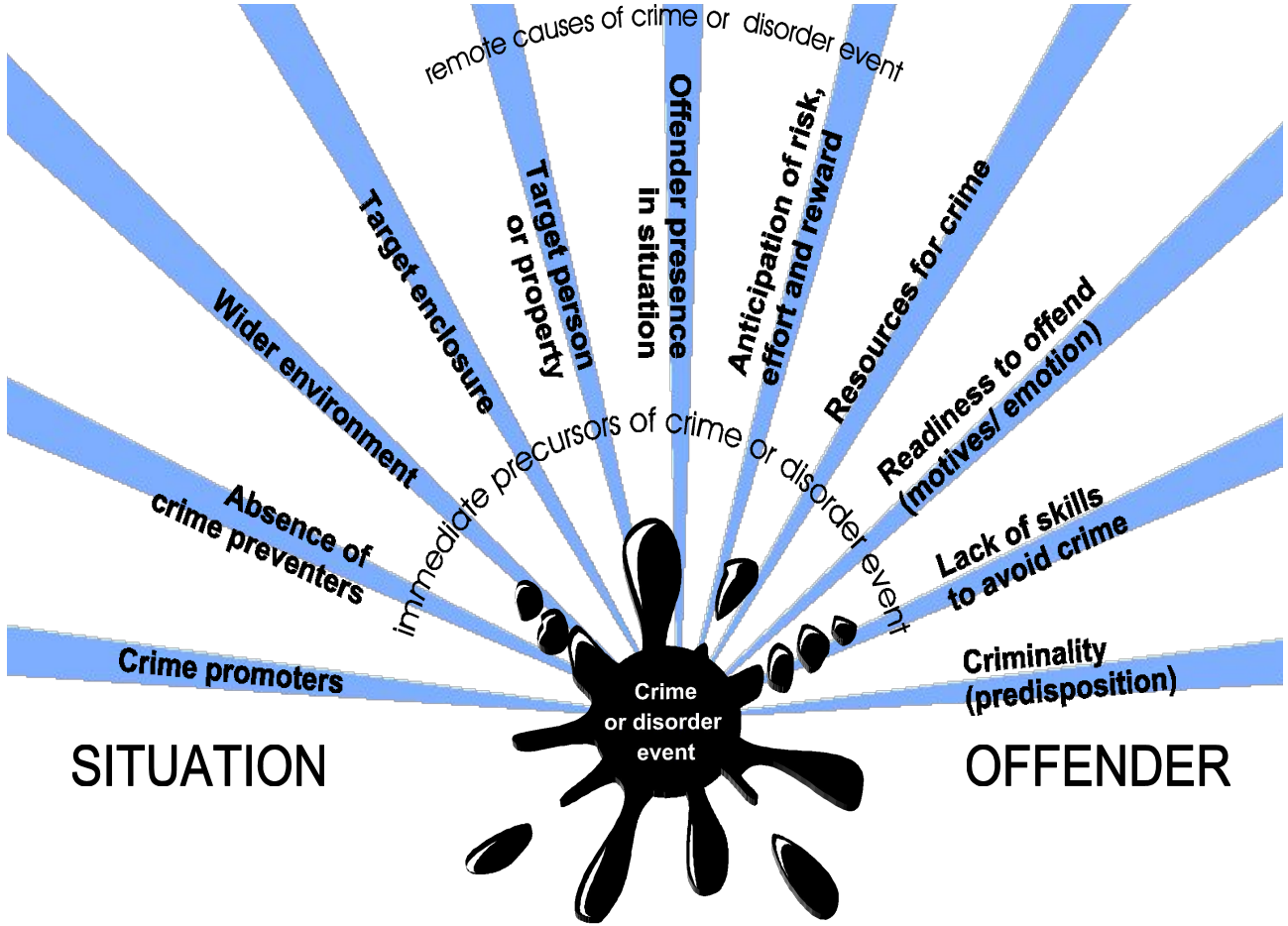
The Human in Resilience

- The human component of an ICT system has an ability to quickly understand novel solutions, and to adapt to unexpected conditions
- Humans can therefore provide additional resilience to, for example, a control system but…
  - Reliably **predicting and influencing human behaviour** is a continuing challenge – Consider current issue of Corona virus hygiene
- Human individuals, groups and communities play a diversity of **roles** in relation to crime and security – important to map these out

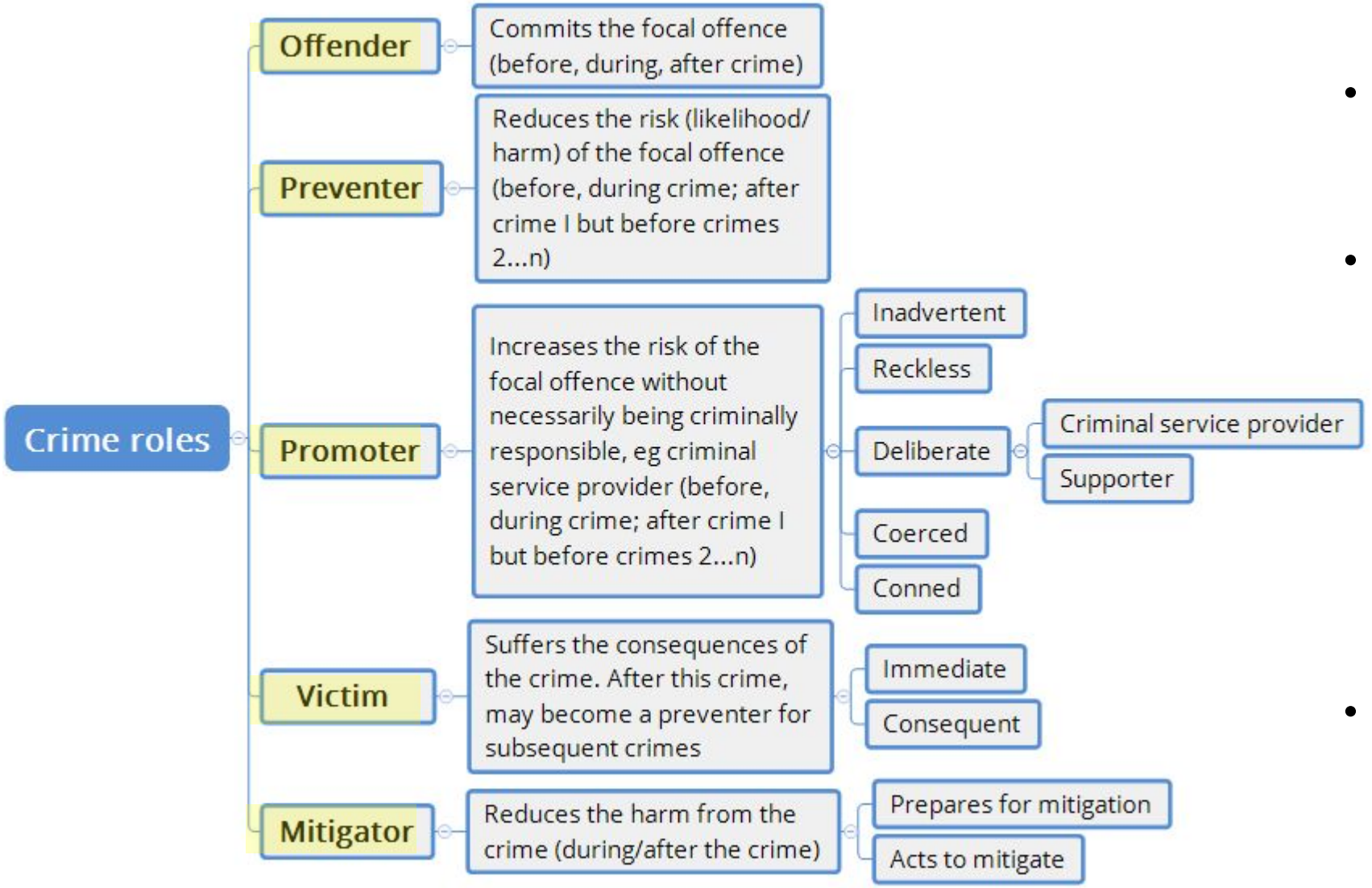
Crime Roles – Who is involved with crime, How?



- The causes of criminal events can be mapped by the **Conjunction of Criminal Opportunity**
- This identifies several **roles** relating to crime – whether material or cyber

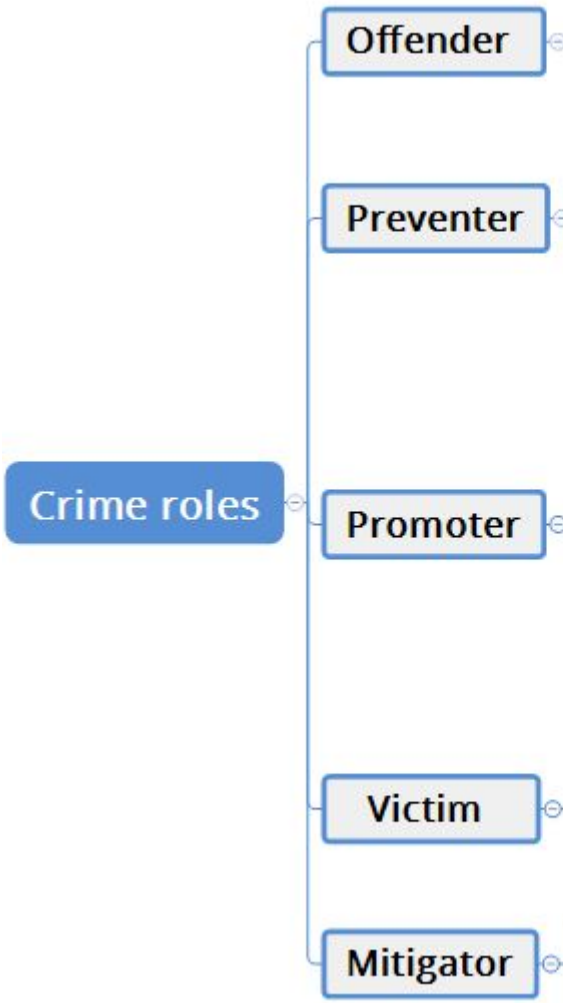


Defining and characterising the crime roles

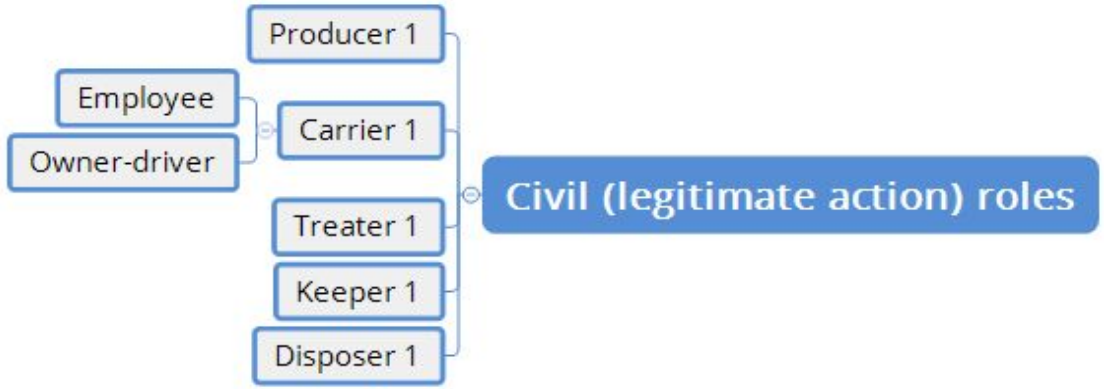


- Roles can be played by **individuals**, **networks, groups** or **institutions**
- Preventers can be
  - **Official, formal and professional**, e.g. police, IT security managers
  - **Informal**, e.g. a user vigilant against phishing or a passer-by intervening to thwart a robbery
- Crime roles can **overlap**, e.g. the same person or organisation can be both victim, and preventer or promoter

Crime X Civil/ legitimate roles

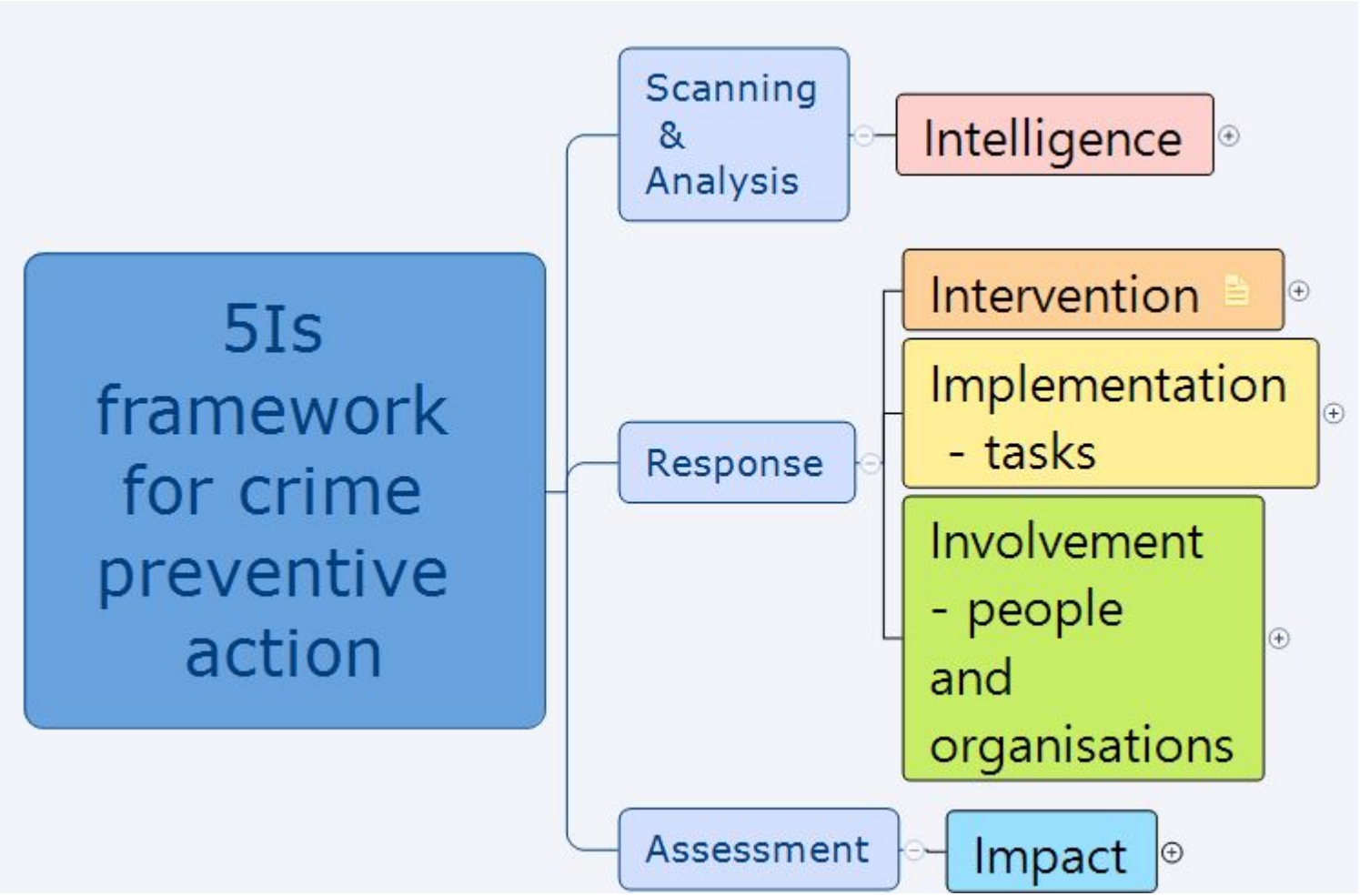


- Crime roles can overlap with **civil** (legitimate) roles
  - E.g. in the normally legitimate activity of **commercial waste disposal**, an Employee of the waste carrier company could be an Offender, a Promoter, a Victim



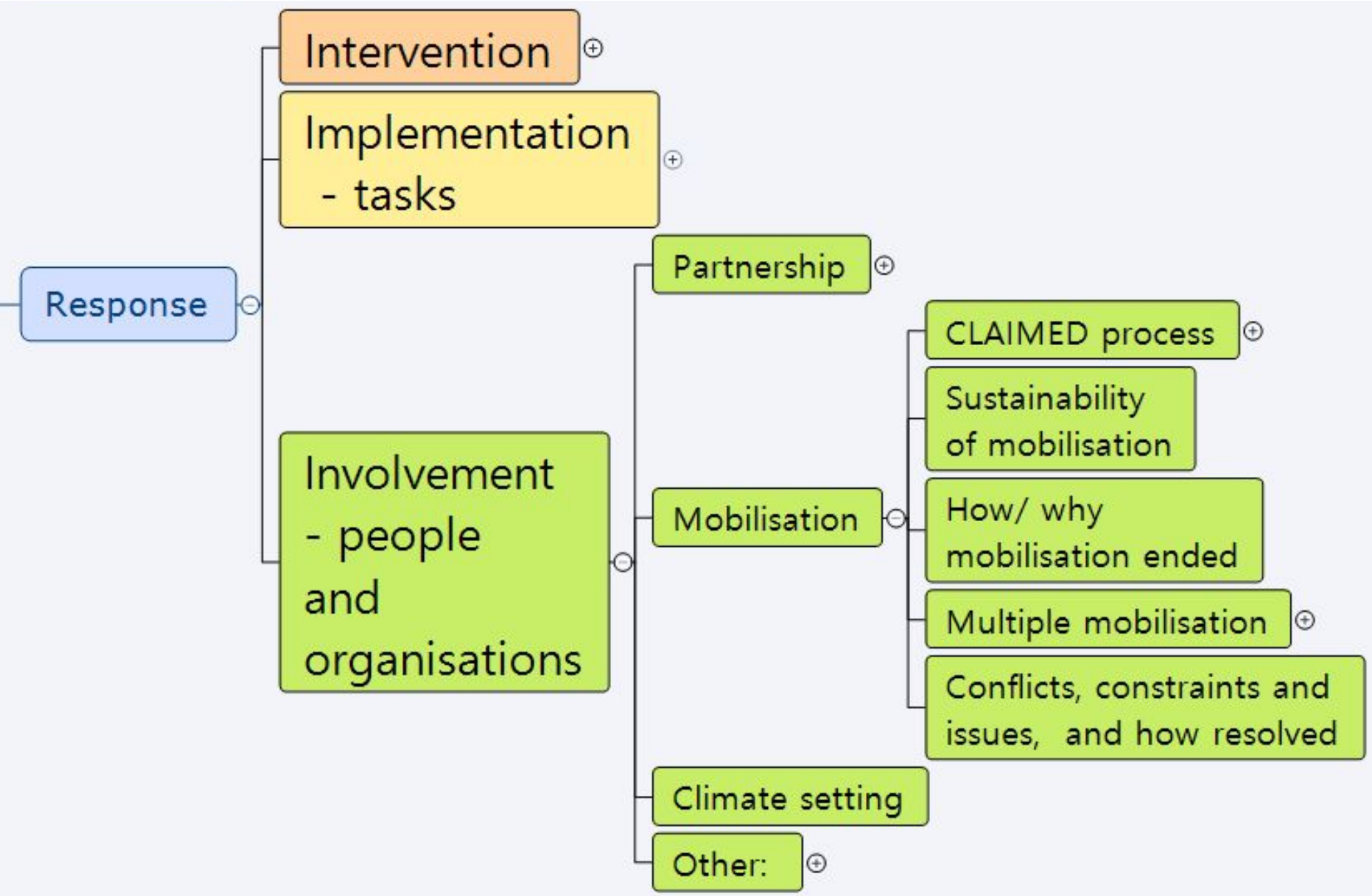
- We can use this understanding of crime and civil roles to consider
  - **Who**, currently or in future, may play **what part** in generating, preventing, responding to or mitigating crime
  - Which are the **civil roles in ICT** that can direct, support or thwart mitigation and resilience?
  - **How** do the players undertake their actions?

Professional Know-How – Crime Prevention Process



- **Professionals** undertaking the roles of **Preventer** and **Mitigator** usually follow a structured process, typically **SARA**
- The **5Is process model** is a more detailed counterpart to SARA
- In particular, 5Is differentiates the '**Response**' stage of SARA into **3 distinct task streams:**
  - **Intervention** – reducing risk
  - **Implementation** – practicalities
  - **Involvement** – the '**people and organisations**' side of implementing the intervention, going beyond the security professionals
- In turn, these tasks are differentiated further still…

Involvement of 3rd parties – Non-security professionals



Involvement can take various forms, including

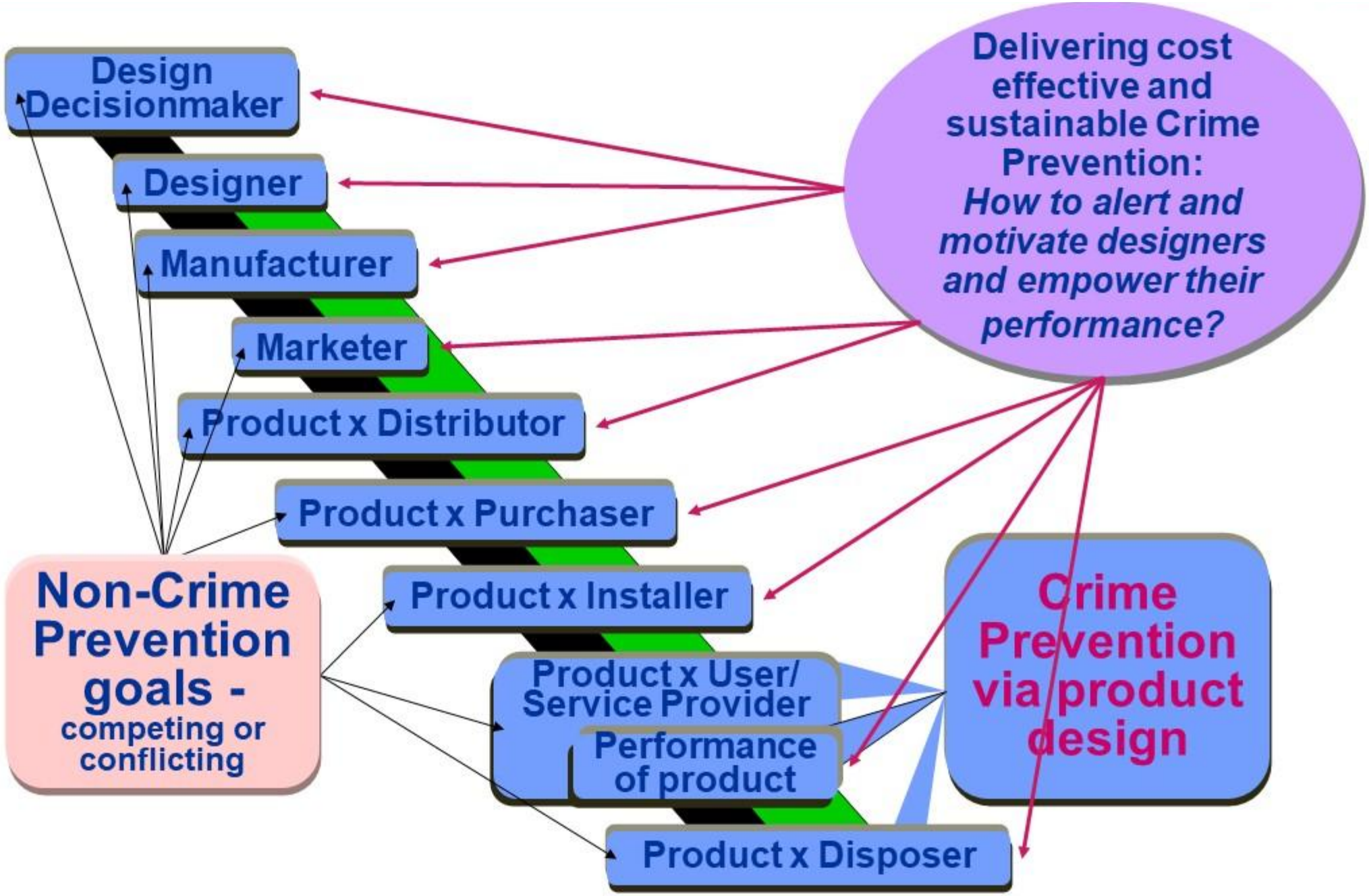
- **Partnership**
- **Mobilisation** of one set of actors by another
- **Climate setting** (e.g. ensuring that employees accept and actively support IT security practices within a company)

Involvement – Mobilisation

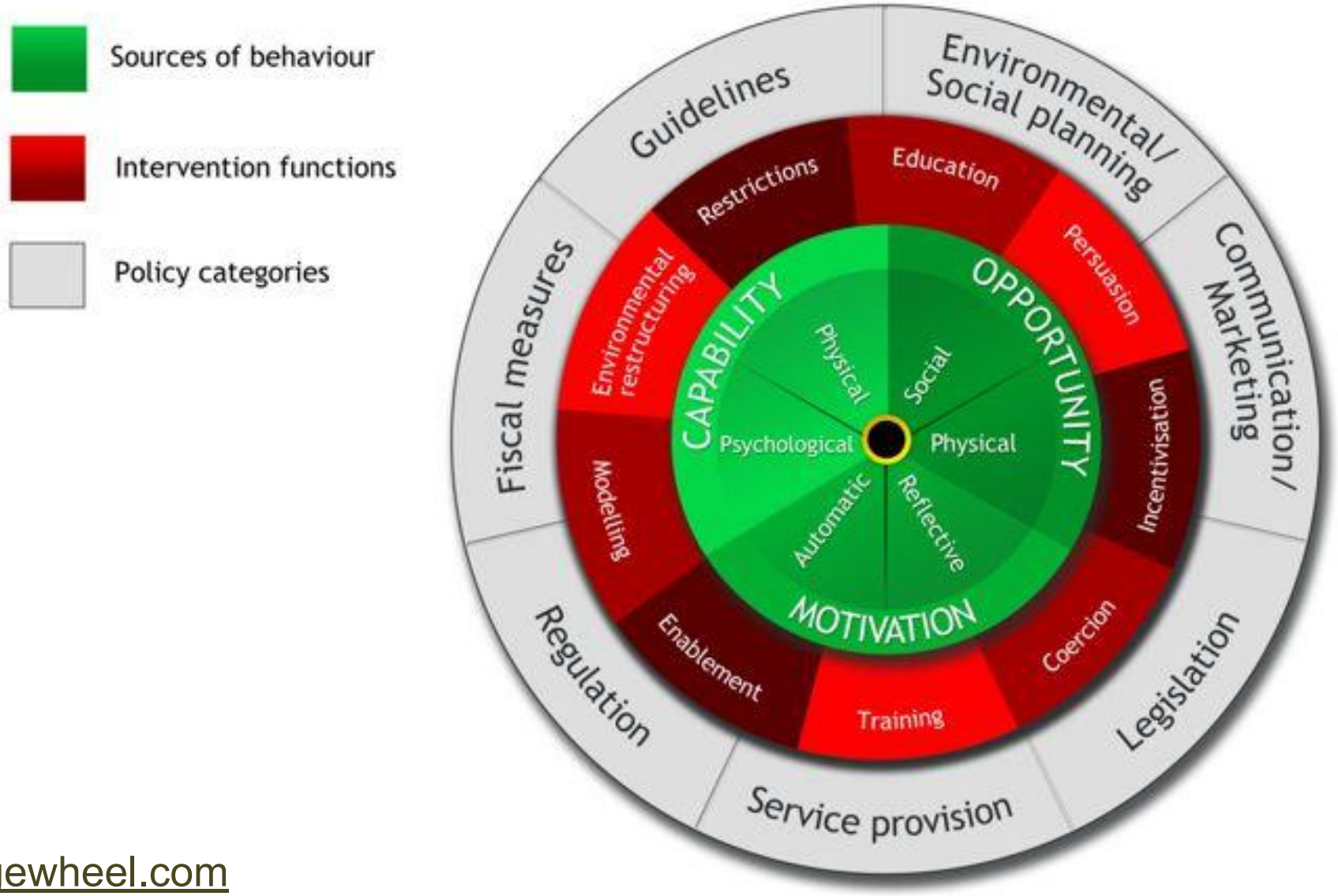
- Mobilisation is about getting people or organisations to
  - Undertake crime prevention **tasks, responsibilities or roles**, or to desist from acting as **crime promoters**
- Mobilisation can be
  - **Direct** (e.g. motivate people to implement intervention)
  - **Indirect or multiple** – e.g. **chains** of implementation, where one set of people/organisations mobilises another...
- The mobilisation process can itself be characterised by **CLAIMED** and perhaps **co-design**

Involvement Chain: Who to influence in promoting a secure future?

- Many civil roles may have to be influenced **in concert** to act as preventers or mitigators and foster crime reductive outcomes
- Consider this example from the commissioning, design, marketing, retail, use and disposal of some future product (material or cyber) which has the potential to be Misappropriated as a target of theft or Misused as a tool for crime



Alternative approach to mobilisation – Behaviour Change Wheel



- http://www.behaviourchangewheel.com
- https://theoryandtechniquetool.humanbehaviourchange.org/tool

Thank you!

p.ekblom@ucl.ac.uk

http://5isframework.wordpress.com

www.designagainstcrime.com/methodology-resources/crime-frameworks