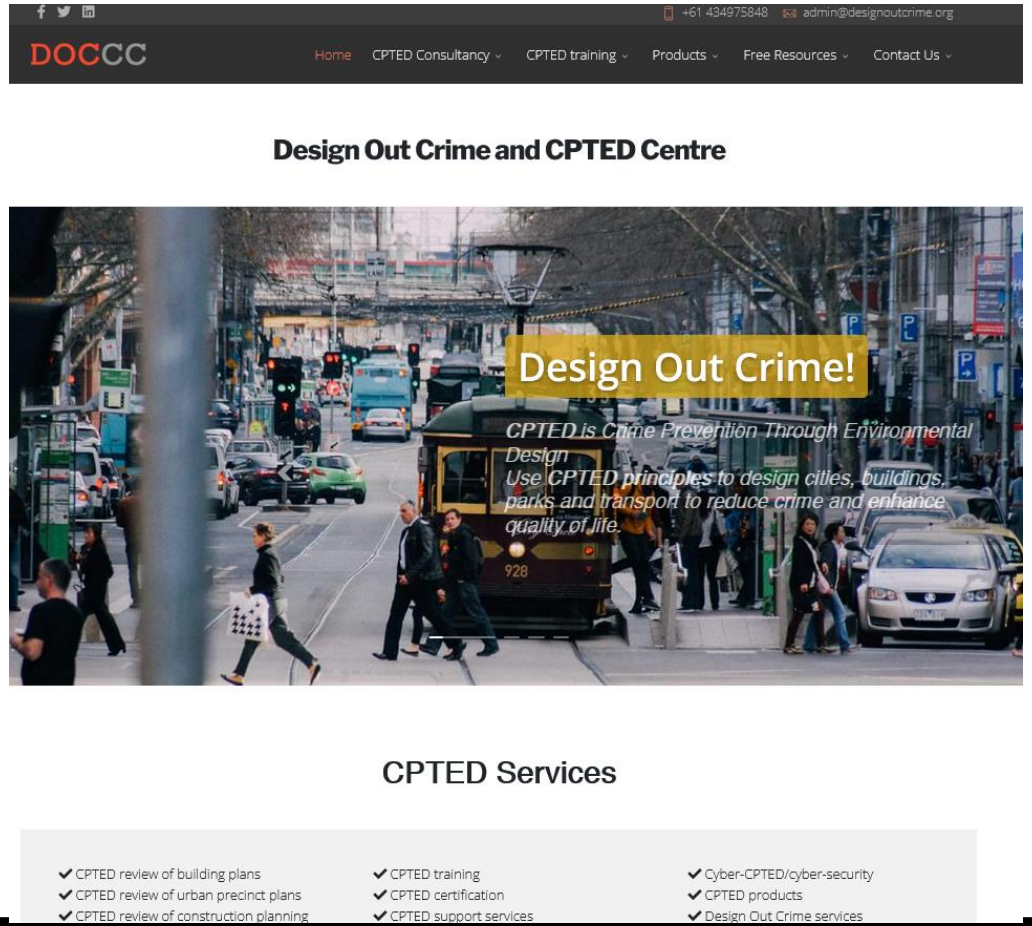
Cyber-CPTED:

Going beyond conventional CPTED, Security and Cyber-Security to address new cyber-physical crimes

Dr Terence Love

CEO, Design Out Crime and CPTED Centre

Who are we?



- Design Out Crime and CPTED Centre
- Previously Design Out Crime Research Centre

What do we do?

- CPTED reviews
- CPTED consultancy
- CPTED training
- Cyber-security analyses and advice

History

- Since 2020, CPTED on around $3billion of development, crime prevention training and novel cyber-security research
- Previous
- From 1971 coding and open source on early internet (JANET UK)
- 1980s Artificial Intelligence programming for industrial projects (e.g. French National Gas industry). Training engineers in robotic systems
- 1990s Sundry computer systems and modelling control systems
- Early 2000s Manager of ECU We-B Research Centre (now Australian Cyber-Security Co-operative Research Centre)
- 2005 Established the Design Out Crime Research Centre across 3 unis
- 2014 Established Design Out Crime and CPTED Centre

What is CPTED?

- CPTED is **Crime Prevention Through Environmental Design**
- CPTED is ‘designing the environment to reduce crime’
- Pronounced ‘Sep-TED’ (Big Ted, Little Ted and CPTED)
- New international standard ISO 22341:2021

What is the environment used in CPTED?

- Buildings and their components
- Public spaces
- Public services
- Signage
- Physical systems
- Communication systems
- Social systems
- Social activities
- Work and commerce
- Computer systems
- Recreation infrastructure and activities
- Policies and processes
- Community activities
- Sound and light services
- Traffic management
- Art
- Governance and legitimation
- Technology
- Documentation

Differences between CPTED, Security and Criminal Justice System

Late at night, a young person hops over a garden fence and sprays graffiti on a house wall.

Fortunately, the owners recently had a security firm install top quality CCTV surveillance with face recognition linked to the city's Police CCTV monitoring centre.

Police using state of art predictive policing were waiting for the offender at the end of the street.

They arrested the offender confident in prosecution due to the high quality CCTV and face recognition evidence.

Question: How good is the crime prevention?

Answer: Crime prevention failed. The crime was committed.

- **CPTED** focuses on designing the environment to encourage lawful behaviour
- A **Security** focus is control of access to assets, minimising vulnerabilities
- A **Criminal Justice System** focus is to ensure offenders are identified and prosecuted AFTER committing a crime

Anti-Fragile – going beyond ‘resilience’

After responding to a disaster or problem:

- ‘Resilience’ is merely that you are back to the past state
- **Anti-fragile** is when you are in a better state and the same disaster will no longer be a problem

Cyber-CPTED

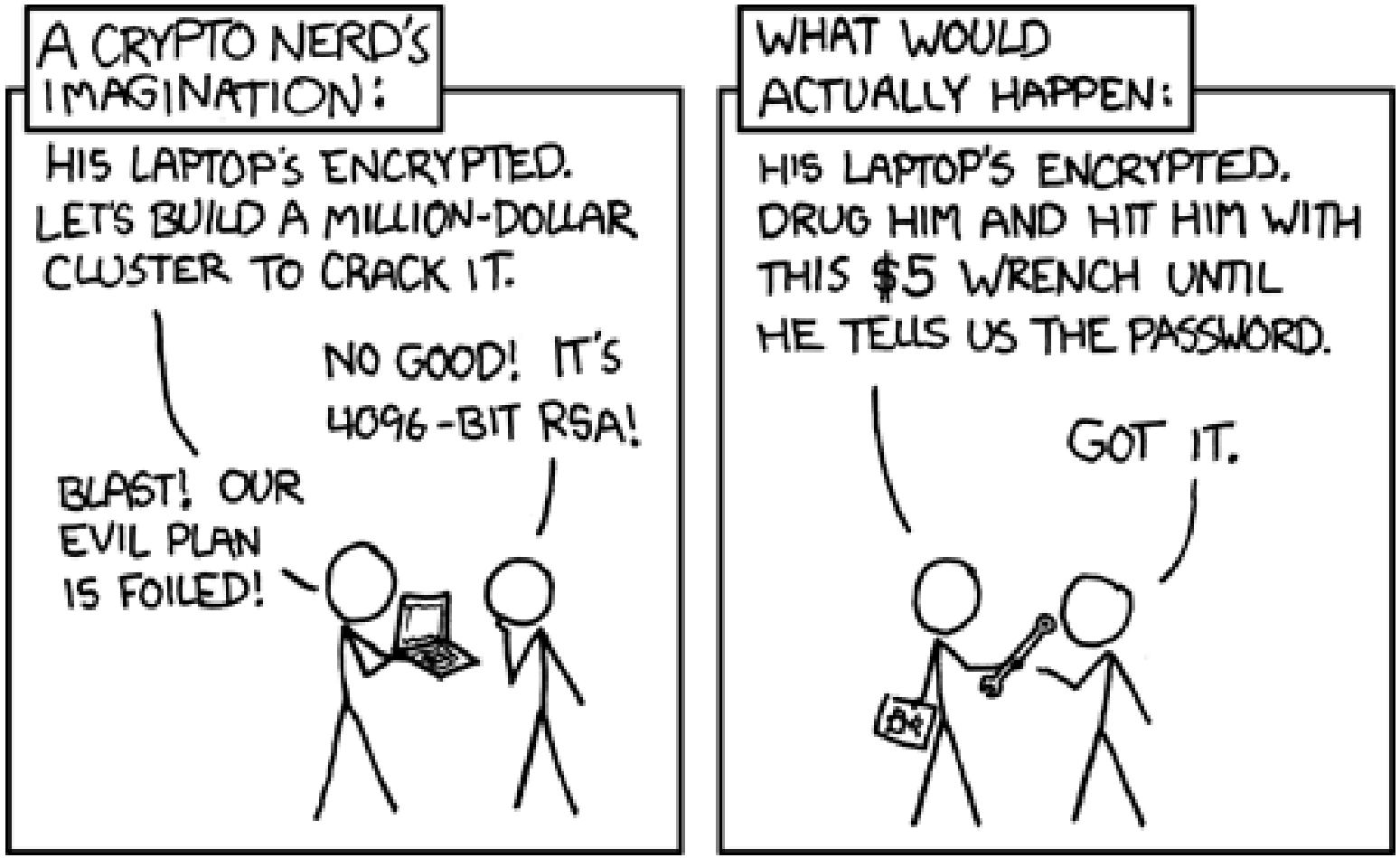
- Cyber-CPTED is CPTED relating to new forms of crime that neither cyber-security nor physical security address well.
- Cyber-CPTED perspective reveals new forms of crime and new ways of addressing them
- Arenas for Cyber-CPTED crimes include:
  - Smart Cities
  - Smart homes
  - Smart vehicles
  - Fin-tech
  - IoT
  - Electronic retail
  - Electronically controlled manufacturing
  - Electronically controlled processes
  - Policing and military control
  - Security
  - Politics
  - Governance
  - Supply chains
  - ---

Examples of cyber-CPTED

- Gym bank hack
- Tesla hack
- Printed weapons
- Electronically supported fraud and theft
- Electronic hacks of physical security
- Physical hacks of electronic security
- Manipulation of prices and costs via computerised systems
- Physical privacy breaches via electronic systems
- Social-physical approaches to attacking electronic systems
- Breaching electronic systems by physical lobbying of politicians
- Bluetooth (BLE) hack of physical locks & IOT devices
- Breaking trade laws by using electronics
- Whistleblower and protected witness failures by mixed physical electronic systems

- Turning off bodycams
- Healthcare physical failure of electronic data records
- Pandemic cyber-policing
- Physical security for bookkeepers
- Illegal police surveillance
- NSA and illegal physical location identification
- Dividend keeper
- False domain names using Unicode alternatives
- Drone deliveries of illegal substances
- Stealing a car with Rolljam
- Industrial remote access systems
- Illegal energy market using smart meters
- Stealing a car with NPR parking
- IOT physical hacks

Physical response to software encryption



The gym-based bank theft

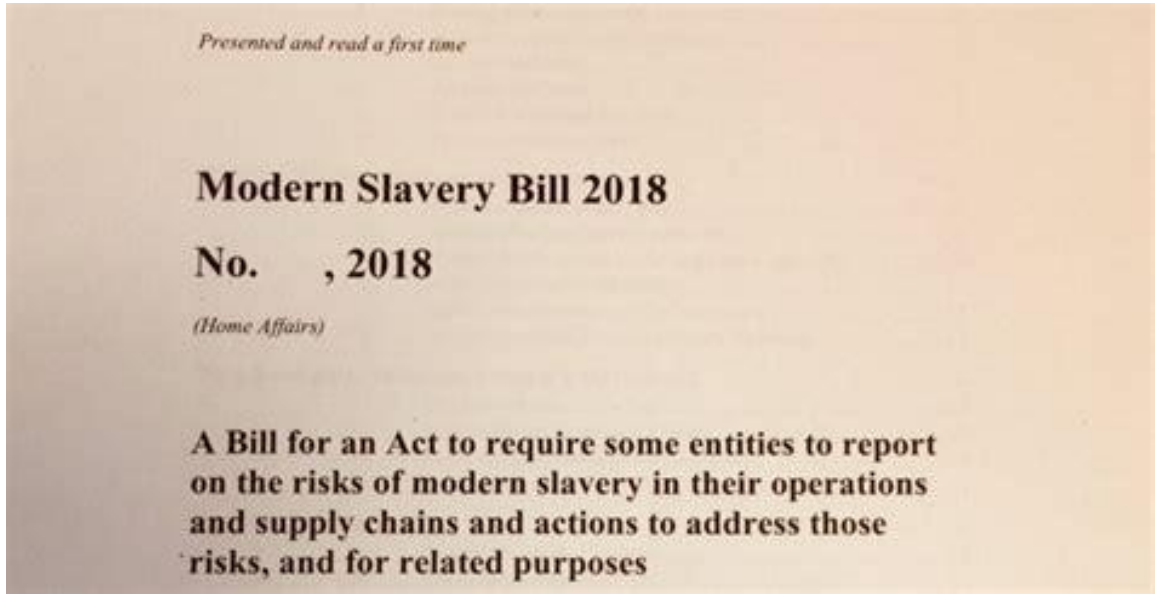
- Steal phone and bank card from gym/pool/sports centre
- Add new device to bank account of card, which requires 2FA via phone
- Bank code notification appears on locked phone
- Have total control of bank account on new device, can
  - Transfer money
  - Lockout previous account owner
  - Use bank card

(Protection is to turn off notifications on phone!)

Physical burglary to steal electronic car access

Breaking electronic vehicle access protection by using physical burglary to steal car keys

Modern slavery in supply chains - electronic systems resulting in crime



Presented and read a first time

Modern Slavery Bill 2018

No. , 2018

(Home Affairs)

A Bill for an Act to require some entities to report on the risks of modern slavery in their operations and supply chains and actions to address those risks, and for related purposes

- Large companies in Australia are legally required to ensure their supply chains are free of modern slavery and report to government Modern Slavery Register
- Companies electronic systems are underreporting supply chain modern slavery and thus resulting in criminal outcomes

Rolljam car theft

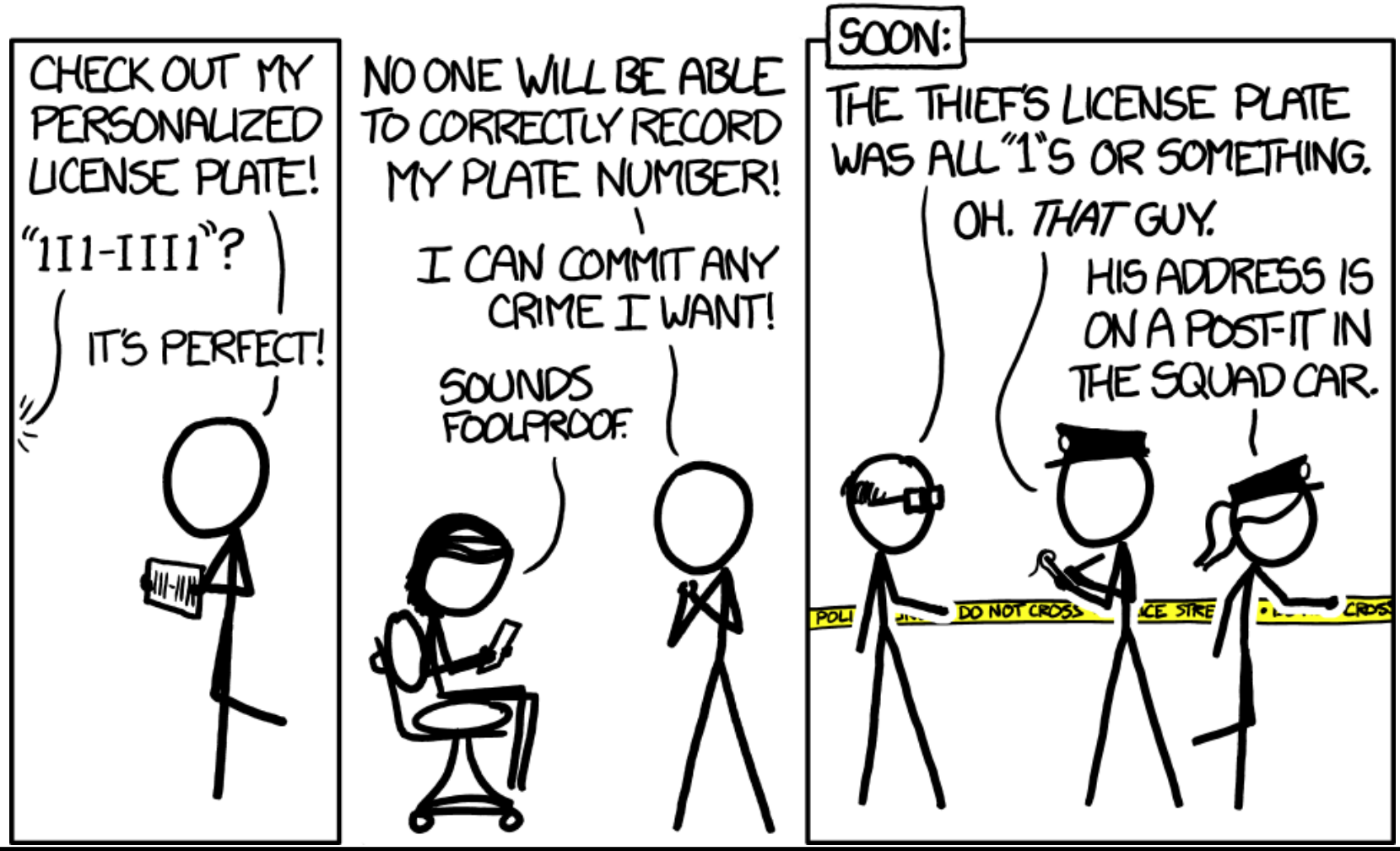
- Rolljam ($450 or build for $35) detects, jams and stores car remote signal from driver to car
- Driver reclicks remote button and rolljam sends old code and records new one
- Rolljam can then be used to open and drive car.

Apple security updates

Apple only fully security patches computers with the most recent macOS

Other Apple devices are not fully secure

License plate



Number plate recognition car parks make vehicle theft easier

Image: https://www.alibaba.com/product-detail/Intelligent-ANPR-License-plate-recognition-camera_62007492372.html

- Hard to steal a car from traditional car parks as ticket required to raise barrier to enable exit.
- With number plate recognition car park, just pay the parking fee and drive out (after using rolljam to access car).

3D printed guns

3D printed guns illegally evade the licensing and recording systems of gun control

https://phys.org/news/2022-11-3d-printed-guns-australia.html

Illegal surveillance

- Physical surveillance by law enforcement is legal (subject to some rules)
- Electronic communication devices such as Stingrays have led to substantial illegal police surveillance
- Ditto for misuse of CCTV
- Illegal COINTELPRO depends on combination of physical and IT

Physically open electronic door lock

Image: https://www.alibaba.com/product-detail/Digital-Key-Pad-Entrance-Door-Lock_1600186697977.html?spm=a2700.galleryofferlist.normal_offer.d_image.339b2086xDbHKb

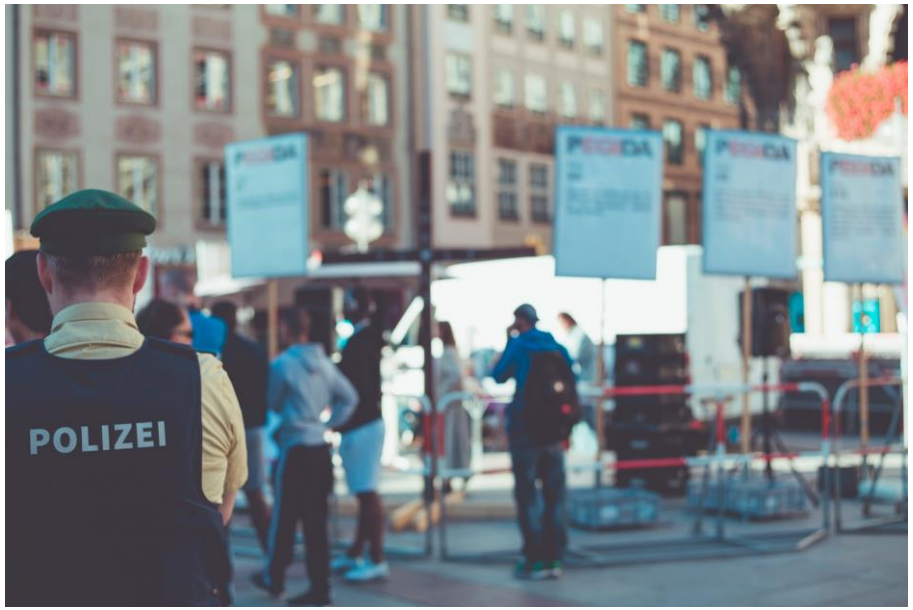
- Electronic door lock has more security in terms of possible permutations than physical key and is unpickable by conventional lockpicks
- However, it will respond to brute force by pipe wrench

This person is committing a serious crime and can be imprisoned

What is a crime?

What is the crime or crimes?

What is a crime?



A **crime** is a behaviour specified as a crime by a Law created by parliament or government.

Pseudo-law making by others

Some pseudo-laws are increasingly and problematically made by government and non-government actors not authorized to make law e.g.:

- Robodebt
- Health system access
- Children access to schools
- Airline refund arrangements
- Broadband and mobile phone contracts
- Access to monopolistic services (e.g. rail)

In many cases, contradicting these result in categories, remedies and exclusions that appear, illegally, to resemble and act as ‘laws’ and ‘crime’ definitions.

Cyber-CPTED crimes

Cyber-CPTED crimes involve hacks that include both physical and electronic systems as means of attack:

- Cyber-enabled physical crimes
- Physical-enabled cyber-crimes
- Crimes enabled by joint physical and cyber means
- Mixed mode crimes whose targets are both cyber and physical

Concept of hacking

***Hack* - a means of subverting a system's rules and intended goals in unintended ways.**

- Voting systems
- Tax accounting systems
- Ownership systems
- Access systems
- Legal systems
- Horticulture and farming
- Management systems
- Manufacturing and process control systems
- Communication systems
- ICT systems
-

Identifying cyber-physical 'crimes'

Criminal acts that subvert a system's rules and intended goals in unintended ways by using combinations of physical and ICT.

Time-based crime prevention

- **Traditional security** focuses on access control – making access to assets more **difficult**
- **Time-based crime prevention** focuses on **increasing the time** necessary to commit a crime so that the crime becomes unviable

Protecting against and reducing risk of cyber-physical 'crimes'

- Go beyond **security** as access control- to reduce encouragement for crime or adverse events
- Increase the **time** needed to undertake crime critical parts of cyber or physical parts of the criminal process – to the point that the crime becomes unviable.
- Identify how cyber environments can be repurposed or compromised using physical means
- Identify how physical environments can be repurposed or compromised using cyber means
- Identify how physical and cyber can be better integrated to encourage lawful behaviour

Questions?

Contact:

Dr Terence Love
CEO, Design Out Crime and CPTED Centre
+61 434975848 admin@designoutcrime.org
www.designoutcrime.org