VARIETY METHODS AND VARIETY THEORY:
AN INNOVATION FRAMEWORK FOR CYBER-SECURITY

DR TERENCE LOVE

CEO

DESIGN OUT CRIME AND CPTED CENTRE

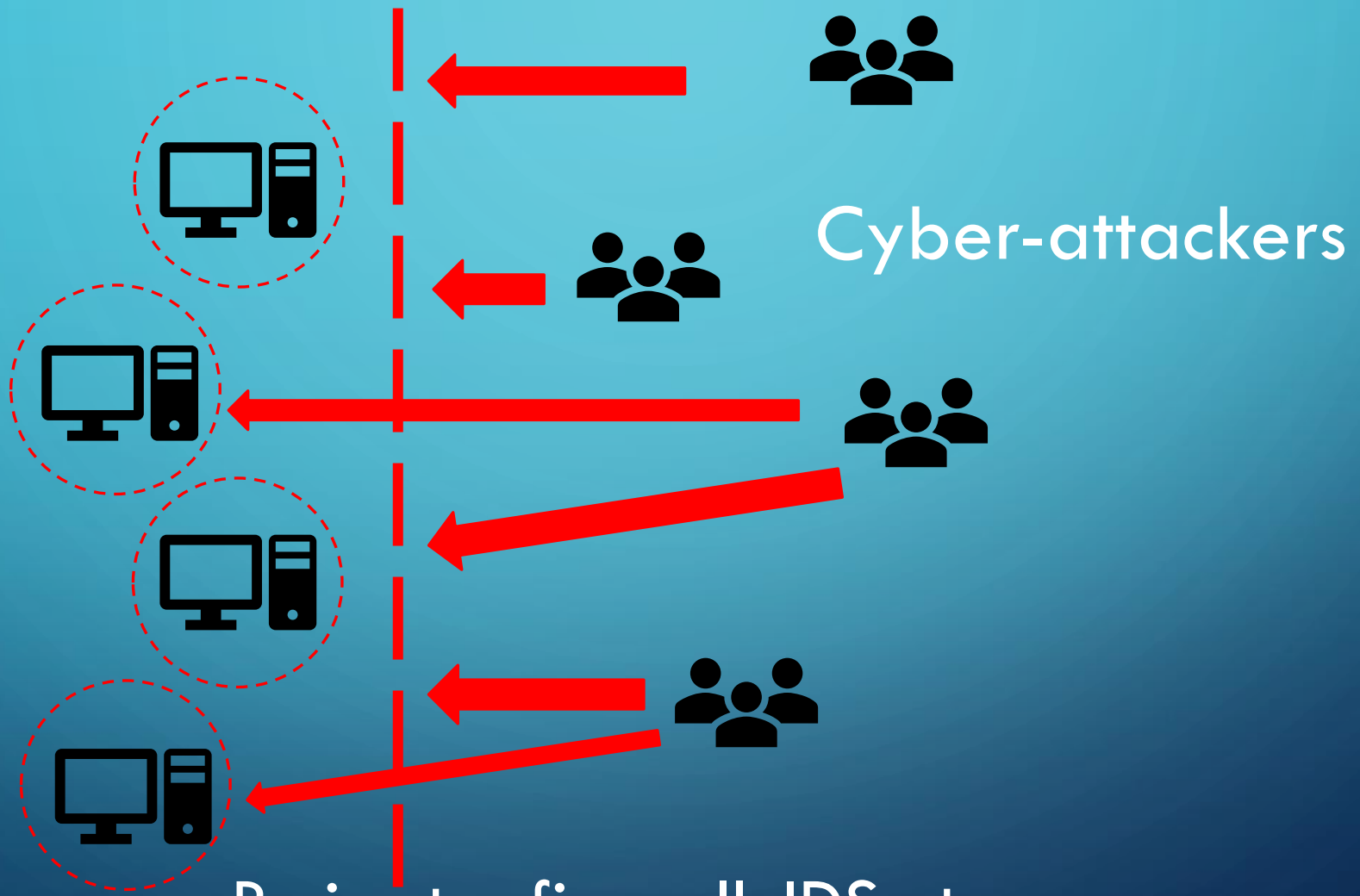
WWW.DESIGNOUTCRIME.ORG

BACKGROUND

- Variety is a mathematical concept
- The Law of Requisite Variety is one of the few 'laws' that applies across all fields.
- Variety is the foundational concept for almost all other theories
- We have developed extensions to the Law of Variety for use in security and redirection of power in complex situations such as cyber-security.

CYBER-ATTACKS AND DEFENSE IN DEPTH

Local machine protection

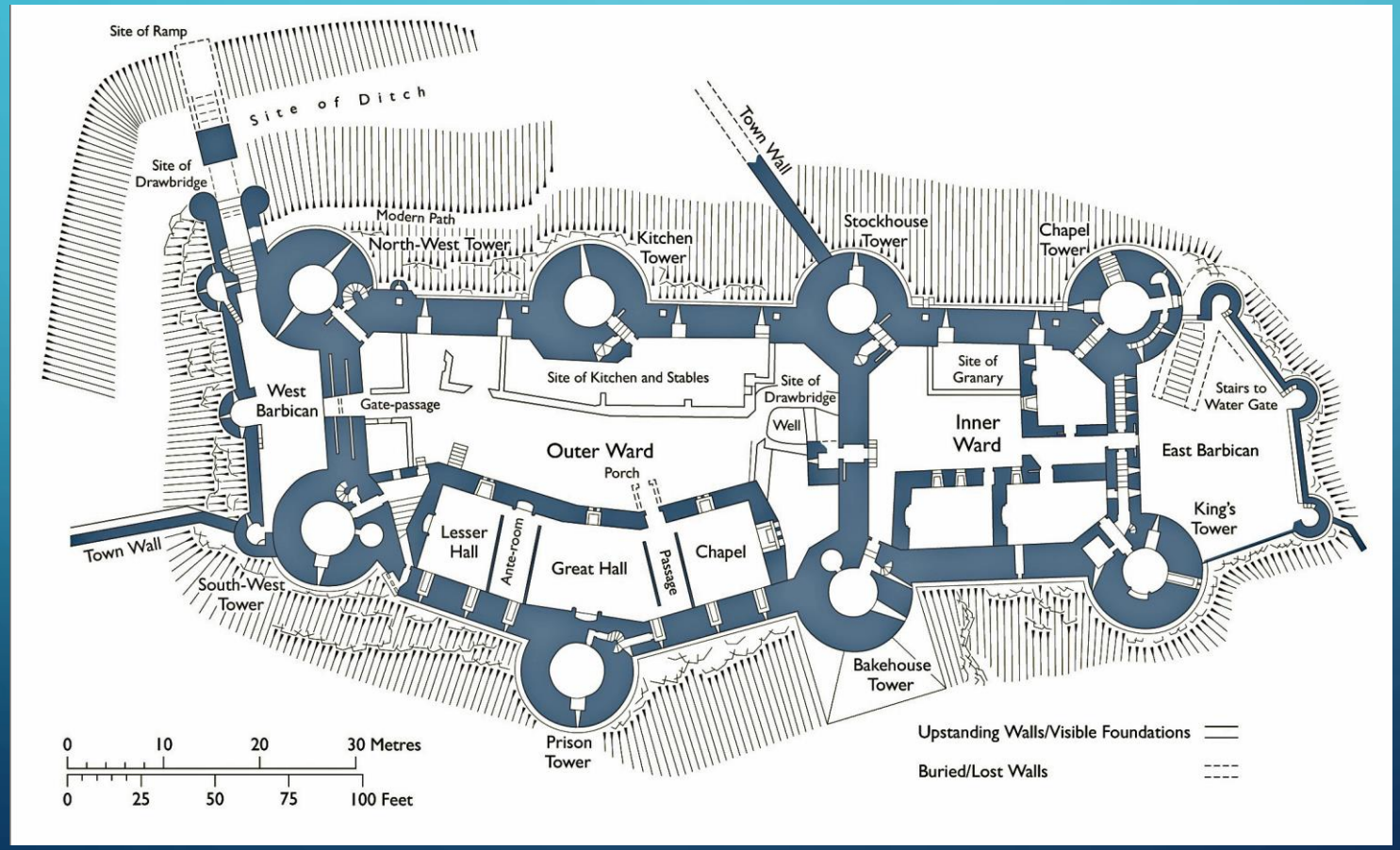


Cyber-attackers

Perimeter firewall, IDS etc

DEFENSE IN DEPTH

Defense in Depth is based on an idea of castle design



BOUNDARY SECURITY: ACCESS CONTROL

Classic design tradition of cyber-security is the combination of:

- Boundary-based security
- Access control
- Identification
- Authentication
- Defense in depth

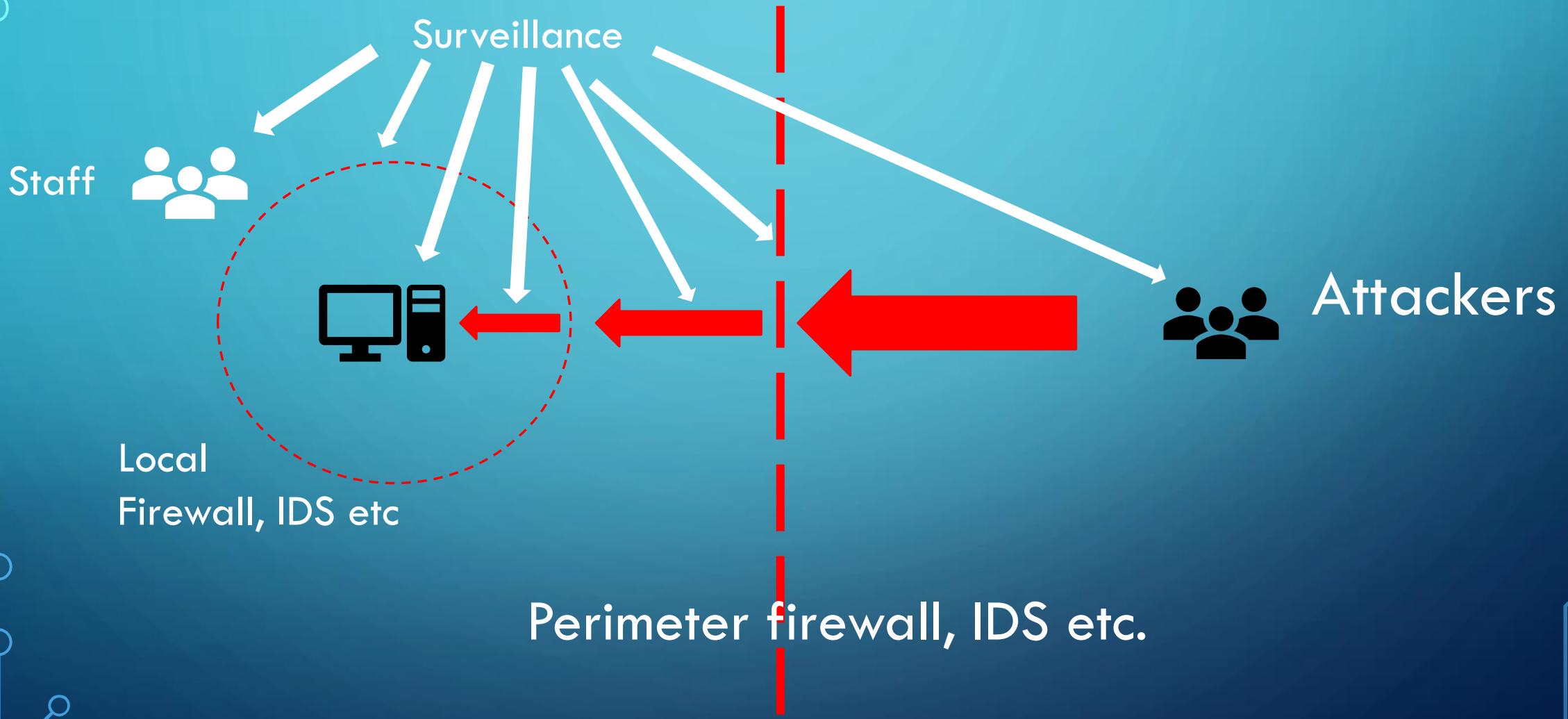
CYBER-SECURITY - SURVEILLANCE

Another tradition of cyber-security is the use of surveillance:

- Surveillance of network boundaries and traffic
- Surveillance of file and folder characteristics (checksums etc)
- Surveillance of unexpected behaviours (e.g. AI/ML detection)
- Surveillance by search for signatures of malware
- Surveillance of user access behaviours
- Surveillance of staff behaviours in and outside work

These all apply to both cyber-attacks and to system failures.

TRADITIONAL CYBER-SECURITY HAS A LINEAR ASPECT



VARIETY – A CHANGE IN WAY OF CYBER-THINKING

- Traditional cyber-security thinking is based on:
  - Castle-like fortified hardware and software barriers
  - Access control, authentication, resource allocation…
  - Protecting data, processes and systems (protecting the 'King')
- Variety-based cyber-thinking is based on:
  - Information about the size of variety of options that attackers can bring to bear
  - The size of the variety of options that can be used by defenders to control attackers
  - Manipulating the dynamic distribution and behaviour of the changes over time in both varieties of options

VARIETY

Variety is the number of different states that are possible

VARIETY IN CYBER-ATTACKING

Variety of cyber-attack paths

Data corruption

Exploits

Social engineering

Hypervisor compromise

DNS-based

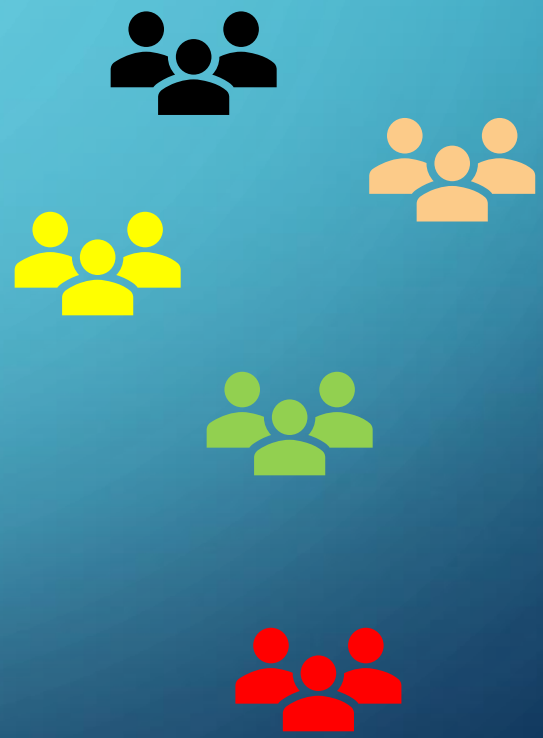
SQL insertions

File-free attacks

Viruses

…

Variety of cyber-attackers

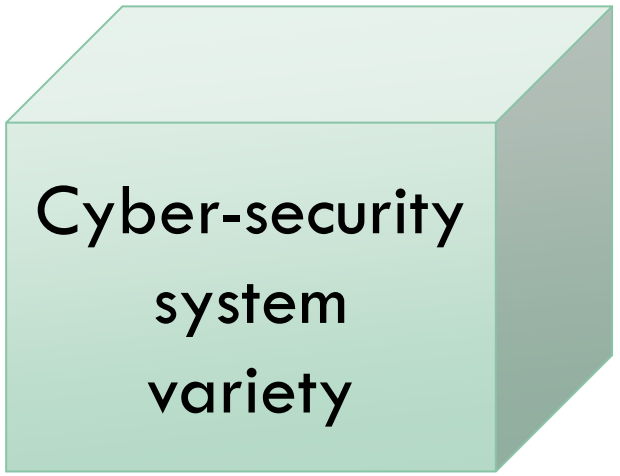


VARIETY DISTRIBUTION DYNAMICS

Variety of multi-dimensional changes in variety over time in a system

LAW OF REQUISITE VARIETY

Variety in control system

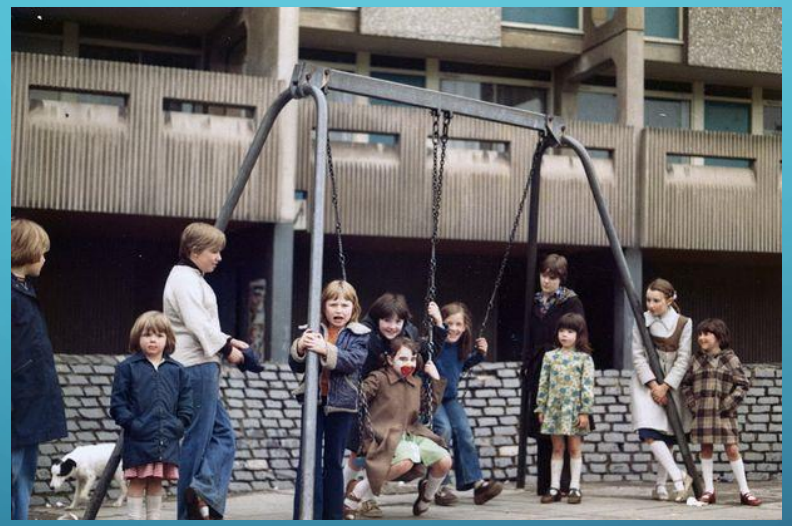


Variety in system being controlled

Cyber-attack ecosystem
variety

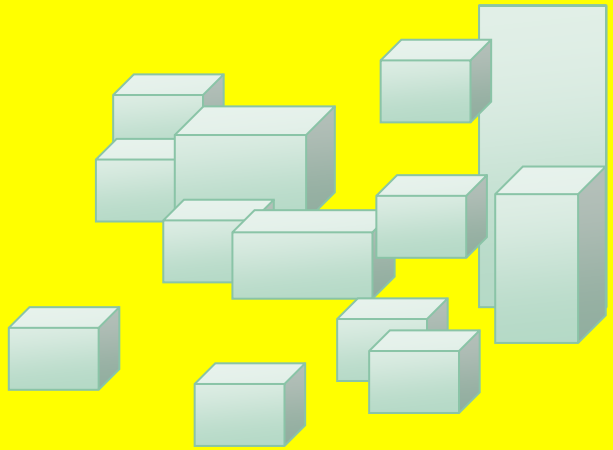
Variety of the Control system must be bigger than Variety of what is being controlled

SCHOOL TEACHER AND CHILDREN



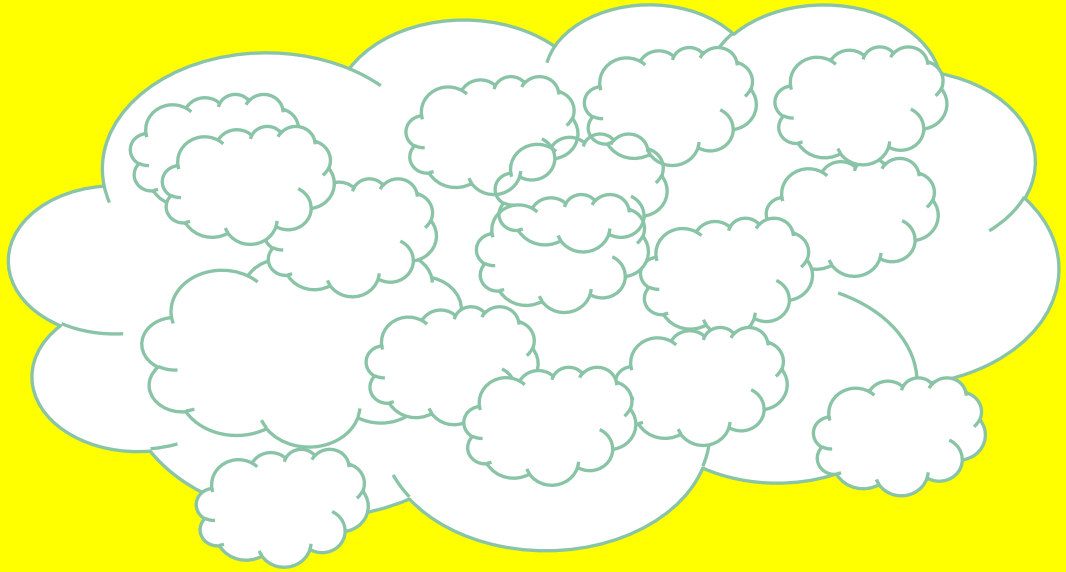
CYBER-SECURITY IS COMPLEX AND DYNAMIC

Dynamically changing control systems



Control

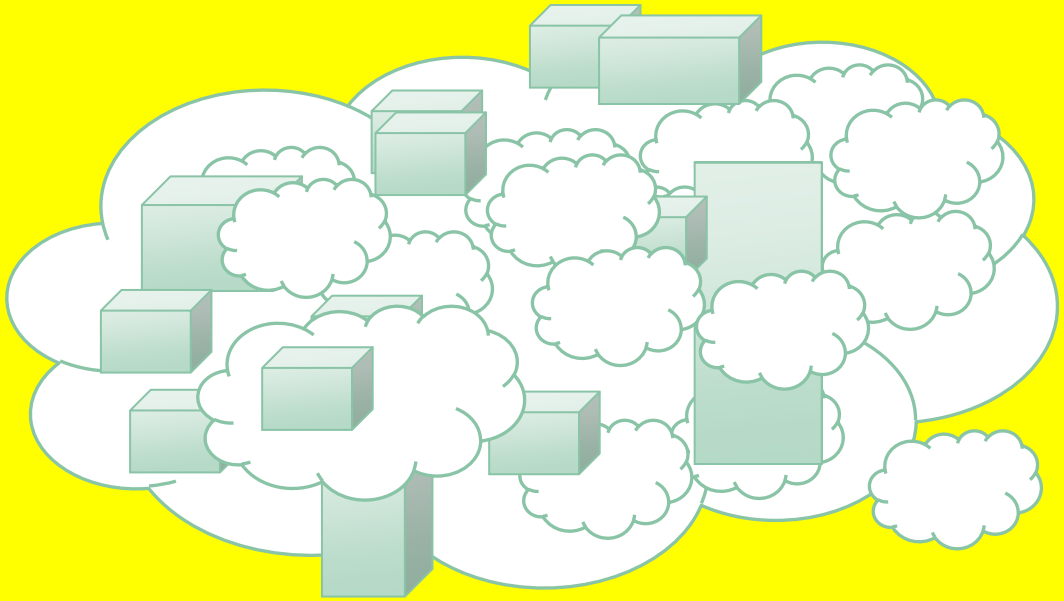
Dynamically changing systems and subsystems



Variety of the Control system must be bigger than Variety of cyber-attacking system

VARIETY IS DYNAMICALLY DISTRIBUTED

Variety is dynamically distributed through the control system and the system being controlled

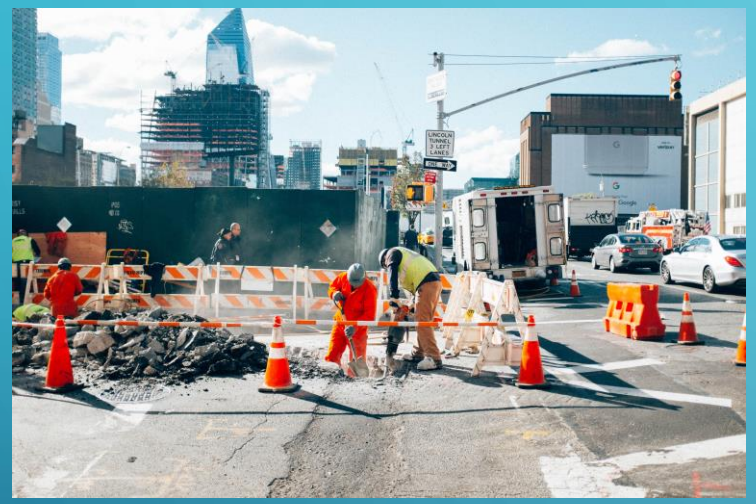


Dynamically changing systems, control systems, subsystem ownerships and variety

INFLUENCING VARIETY LEVELS AND LOCATION INFLUENCES THE CONTROL OF POWER

- It is possible for any actor in a system to change variety
- Balance of power at any point depends on the relative levels of variety of different actors
- Influencing the flows of variety = change to the distribution and ownership of variety
- Changes in the distribution and ownership of variety redirects the power and control at any and every point in the system

UNION CONTROL OF MANAGEMENT



1. Increase variety caused by members
2. Offer to act between management and union membership
3. Result – transfer of management power to union and union membership

VEHICLE EMISSION CONTROL

1. US Vehicle industry resisted emissions laws
2. Environmental groups pressured different states to have different emissions laws (increase) variety
3. Vehicle industry needed reduced variety to keep control of car production
4. Vehicle industry agreed on US-wide emissions law

CYBER-SECURITY: VARIETY AND TIME-BASED CONTROL

- We have developed 14 variety axioms to guide the use of variety to manipulate power and control in cyber-security and information security.
- Recently, we have identified a Law of Requisite Time and an associated set of 14 time axioms for the same purpose.

PRACTICAL USES OF VARIETY METHODOLOGY IN CYBER-SECURITY STRATEGIES

- Four paths to using variety as a basis for cyber-security strategies:
  - Use our variety axioms to change power flows
  - Identify key variety limitations on the opponent's side and increase variety on your side in ways that ensure requisite variety is fulfilled on all system dimensions.
  - Identify key variety limitations on the opponent's side and increase variety on your side to cause them overload and organizational disfunction.
  - Identify the core power pathway and increase effective variety at more than 2 Feedback loops away in ways that achieve power transfer (2 Feedback Loop Law is described elsewhere)

QUESTIONS?

If you would like to know more, please contact:

Dr. Terence Love

CEO

Design Out Crime and CPTED Centre

t.love@designoutcrime.org

+61 (0)434 975 848

www.designoutcrime.org