Regulatory Failure in the Security Space: Some Current Cases

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra

Visiting Professor in Computer Science, ANU, Canberra
Visiting Professor in Cyberspace Law & Policy, UNSW, Sydney

http://www.rogerclarke.com/DV/RFSS {.html, .pdf}

Norwegian Research Center for Computers and Law
University of Oslo – 29 August 2016

The Notion of Security

A condition
in which harm does not arise
despite the occurrence of threatening events

A set of safeguards
whose purpose is
to achieve that condition

The Conventional Security Model
Key Concepts

- A **Threat** is a circumstance that could result in Harm

  A **Threatening Event** is an instance of a generic Threat

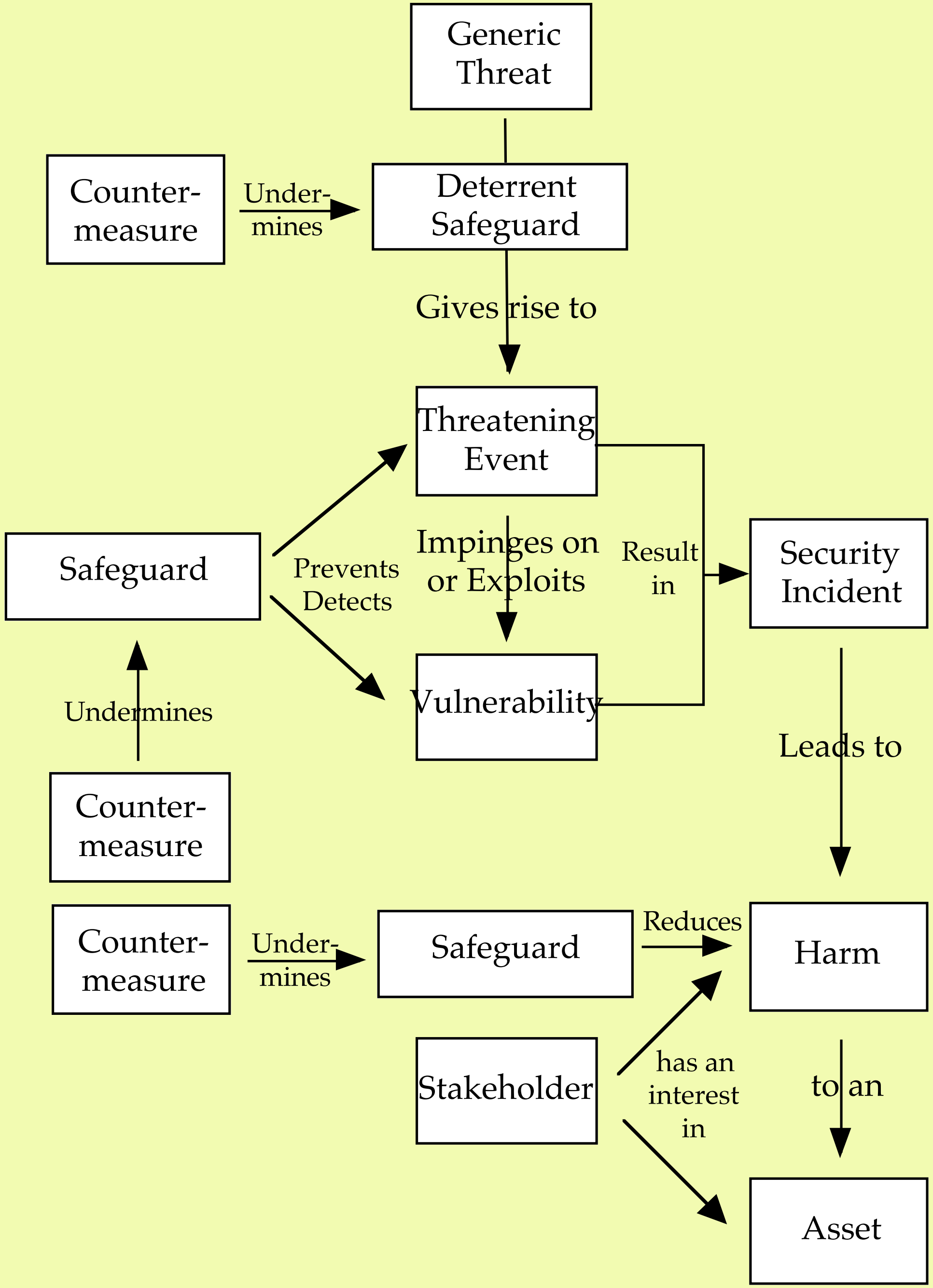
  A Threat may be natural, accidental or intentional

  - An intentional Threatening Event is an **Attack**
  - A party that creates an Intentional Threat is an **Attacker**

- A **Vulnerability** is a susceptibility to a Threat
- **Harm** is any kind of deleterious consequence to an **Asset**

- A **Safeguard** is a measure to counter a Threat
- A **Countermeasure** is an action to circumvent a Safeguard

The Conventional Security Model



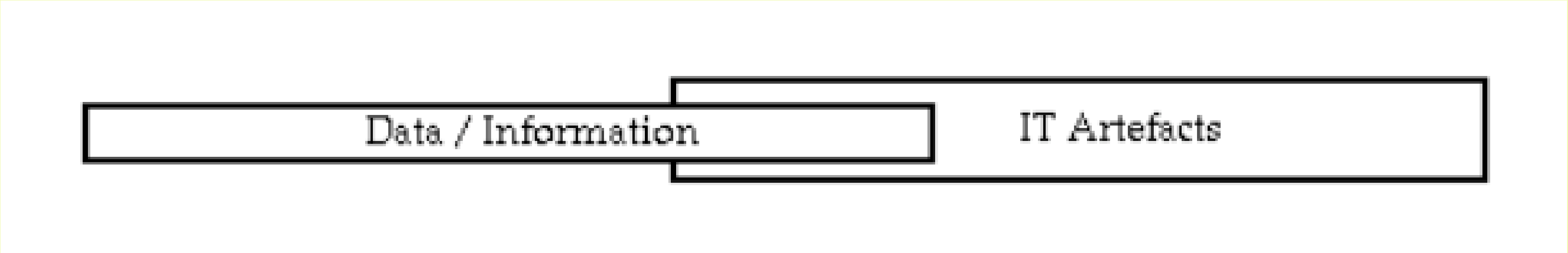
http://www.rogerclarke.com/
EC/PBAR.html#App1

Asset, Harm, Value, Stakeholder

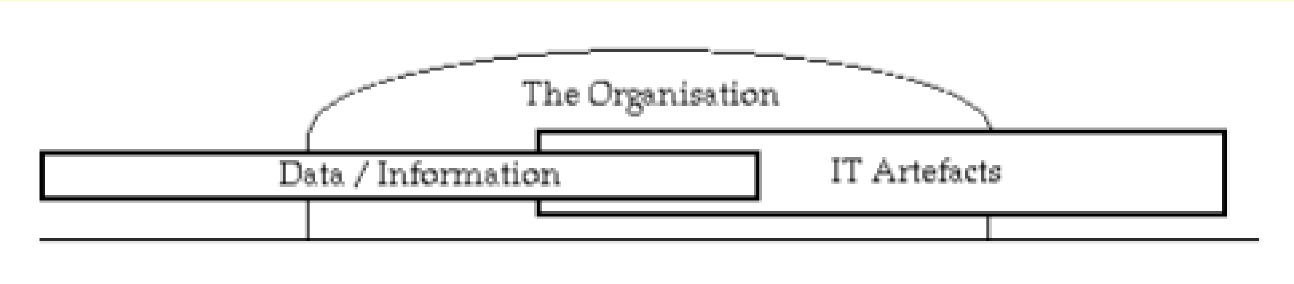
- **Harm** means deleterious impact on an **Asset**
- But which Harm matters, to which Assets?
- That depend on the perspective that's adopted and the **Values** that are perceived in Assets
- So it's necessary to define **Stakeholders**

'Whose Security?'

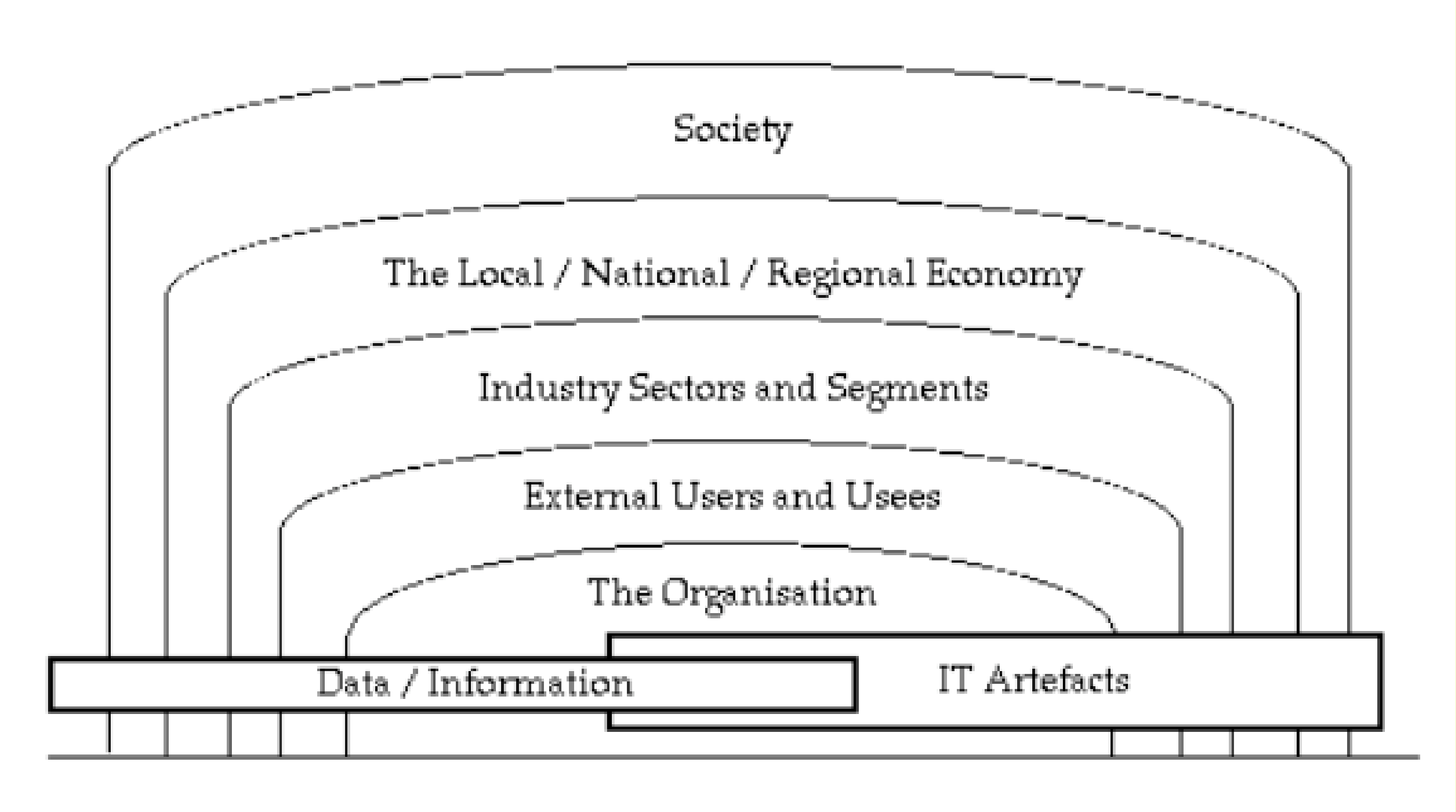
The Scope of Security



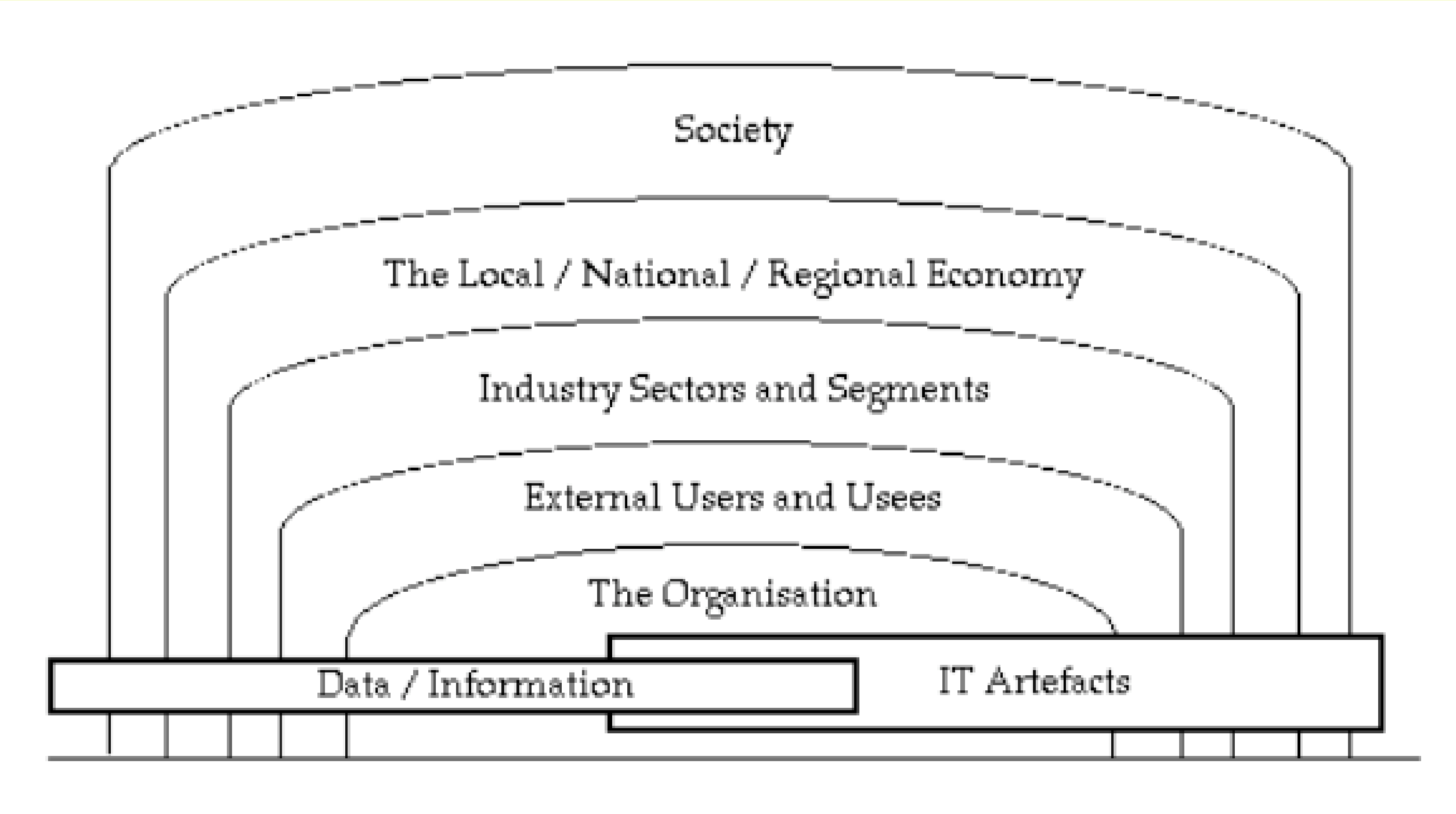
The Organisational Scope of Security



The Many Scopes of Security

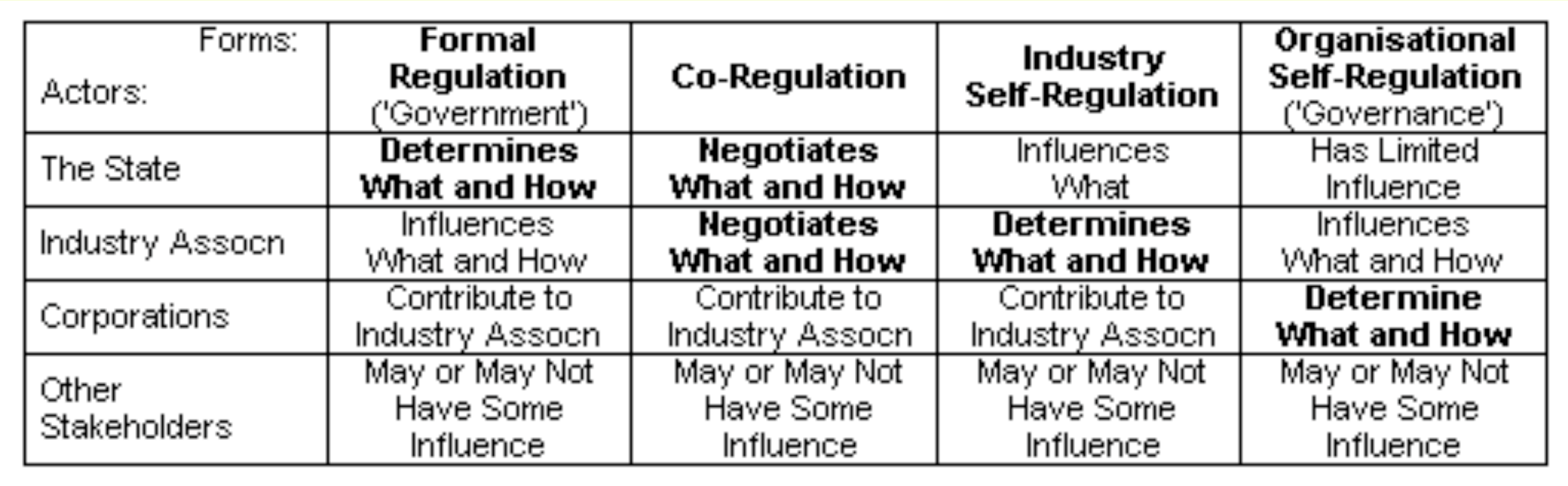


Who are the Champions for Each Perspective?



Which have Power? What Coalitions are feasible?

2. The Regulatory Framework



Forms: Actors:	**Formal Regulation** ('Government')	**Co-Regulation**	**Industry Self-Regulation**	**Organisational Self-Regulation** ('Governance')
The State	**Determines What and How**	**Negotiates What and How**	Influences What	Has Limited Influence
Industry Assocn	Influences What and How	**Negotiates What and How**	**Determines What and How**	Influences What and How
Corporations	Contribute to Industry Assocn	Contribute to Industry Assocn	Contribute to Industry Assocn	**Determine What and How**
Other Stakeholders	May or May Not Have Some Influence	May or May Not Have Some Influence	May or May Not Have Some Influence	May or May Not Have Some Influence

Statutes & Delegated Legislation	Statutory Codes & Standards	Industry Codes & Standards	Customer Charters

XAMAX
Consultancy
Pty Ltd

Clarke & Bennett Moses (2014)
http://www.rogerclarke.com/SOS/Drones-PS.html#R

How to Recognise An Effective Regulatory Scheme

Process

- Clarity of Aims, Requirements
- Transparency
- Participation
- Reflection of Stakeholder Interests

Product

- Comprehensiveness
- Parsimony
- Articulation
- Educative Value
- Appropriate Generality and Specificity

Outcomes

- Oversight
- Enforceability
- Enforcement
- Review

XAMAX Consultancy Pty Ltd

Clarke & Bennett Moses (2014)
http://www.rogerclarke.com/SOS/Drones-PS.html#R

3. Some Test-Cases

1. PIAs for National Security Initiatives
2. Big Data Analytics
3. The 'Internet of Things' ...
4. Remotely-Piloted Drones
5. Autonomous Cars
6. The EC GDPR's DPIA
7. The Precautionary Principle

National Security Measures Since 2001 Have Compromised Many Human Rights

- Freedom from Arbitrary Detention (ICCPR Art. 9)
- Freedom of Movement (Art. 12) ======>>
- Right to a Fair Trial (Art. 14.1), Minimum Guarantees in Criminal Proceedings (Art.14.2-14-7)
- Privacy (Art.17)
- Freedom of Information, Opinion, Expression (Art. 19)
- Freedom of Association (Art. 22)

- Other Rights Potentially at Risk (Arts. 2.1, 7, 15, 21, 24, 26, 27)

http://www.rogerclarke.com/DV/IANS.html#App4

Extracted from AHRC (2008), Williams (2011),
HRLC (2011, 2012) LCA (2012), Lynch et al. (2014)

3.1 PIAs and National Security Initiatives A Five-Factor Test

1. Is there evidence of a PIA process being performed?
2. Were advocacy organisations aware of that process?
3. Did the project sponsor(s) engage with advocacy organisations?
4. Was the PIA Report published on completion?
5. Were advocacy organisations' views appropriately reflected in the PIA Report?

However, it was known that there was a low incidence of published Reports. Hence:

6. Did the PIA Report come to light later, e.g. as a result of an FoI request by the media?

PIAs don't operate as a Control Mechanism over Australian National Security Initiatives

AGD

- Passed the 5-factor test 2/36
- Engagement with advocacy organisations 3/36 (but their views were ignored)
- Secret (hence flawed) PIA processes 10/36

Other Agencies

- Passed the 5-factor test 1/36
- Engagement with advocacy organisations 5/36

XAMAX Consultancy Pty Ltd

Clarke R. (2016) 'Privacy Impact Assessments as a Control Mechanism for Australian National Security Initiatives' Computer Law & Security Review 32, 3 (May-June 2016) 403-418

Case Studies

1. **Document Verification System (DVS) 2004-15**
   Some PIAs, but advocates were excluded, and the 2014-15 expansion was done entirely in secret
2. **ANPR Mass Surveillance 2007-**
   Reneged on publication of the PIA report
   Committed to PIA processes, but did no more
3. **Telecommunications Act s.313 2013-15**
   Impenetrable text secretly interpreted to mean that a 'request' for assistance from a telco or an ISP imposes a positive obligation – any agency, any purpose, no warrant, no controls. And no PIA or other consultation
4. **(Meta-)Data Retention 2003-15**
   No PIA was ever performed, and submissions by 30 advocacy organisations were ignored

Conclusions about PIAs and NatSec

- 3 of the 72 projects (4%) passed every test
- 57 of the 72 projects **(79%) failed every test**
- **AGD has continually breached expectations, public policy and arguably the law, but has avoided publicity and suffered no sanctions**
- 7 advocacy organisations wrote jointly to the AG in September 2011. No reply was received
- The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is a puppet
- The Privacy Commissioner is a captive
- **PIAs don't operate as a Control Mechanism over Australian National Security Initiatives**

3.2 Big Data Analytics

Big Data

- A single large data-collection
- A consolidation of data-collections:
  - Merger (Physical)
  - Interlinkage (Virtual)
    - Stored
    - Ephemeral
- 'Fast Data', i.e. streaming

Big Data Analytics

Techniques to draw inferences

3.2 Big Data Analytics
Risk Factors – Data Quality
(Assessable at time of collection)

- D1 – Syntactic Validity
- D2 – Appropriate (Id)entity Association
- D3 – Appropriate Attribute Association
- D4 – Appropriate Attribute Signification
- D5 – Accuracy
- D6 – Precision
- D7 – Temporal Applicability

Risk Factors – Information Quality
(Assessable only at time of use)

- I1 – Theoretical Relevance
- I2 – Practical Relevance
- I3 – Currency
- I4 – Completeness
- I5 – Controls
- I6 – Auditability

Risk Factors
Decision Quality

- Appropriateness of the Inferencing Technique
- Data Meaning
- Data Relevance
- Transparency
  - Process
  - Criteria

http://www.rogerclarke.com/EC/BDQF.html#DeQF

Evaluation Techniques for Big Data Projects

	Mainly Quantitative and Financial Data	Mainly Qualitative Data
Mainly the Sponsor's Perspective	Discounted Cash Flow Investment Analysis Financial Sensitivity Analysis Financial Risk Assessment	Internal Cost-Benefit Analysis Risk Assessment
Multiple Stakeholder Perspectives	External or Economic Cost-Benefit Analysis (CBA) Economic Feasibility Assessment	Cost, Benefit and Risk Assessment (COBRA) Economic, Social and Environmental Impact Assessment

http://www.rogerclarke.com/EC/PETsBusCase.html#BC (2008)

3.3 Ubiquitous Computing, Pervasive Computing, Ambient Intelligence, Mobility and the (Inter)net of (Every)Thing(s) and People

3.3 Ubiquitous Computing, Pervasive Computing, Ambient Intelligence, Mobility and the (Inter)net of (Every)Thing(s) and People

eObjects – objects not inherently computerised, but into which has been embedded one or more computer processors with data-collection, data-handling and data communication capabilities

- Active capacity
- Adaptability
- Addressability
- Associability with animals
- Autonomy
- Dependency
- Geo-Locatability
- Human computer interaction
- Identifiability
- Network Locatability
- Mobility
- Impacts
- Portability
- Prevalence
- Use pattern
- Volatility

Manwaring K. & Clarke R. (2015)
'Surfing: ... a framework for research into eObjects'
Computer Law & Security Review 31,5 (October 2015) 586–603
http://www.rogerclarke.com/II/SSRN-id2613198.pdf

Security Challenges within IoT Systems

Cisco, February 2016

http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

- **Minimal-Capacity Devices** – very little physical security, and very little scope for programmed security features
- **Minimal Power**, and minimal data transmission capacity
- **No Backup Connectivity or Power**
- **Inexpensive, High-Volume Manufacture**
  i.e. high failure rate and unpredictable often short life
- **Volatile Swarms**, limited expertise in managing them
- **Complex, Multi-Party Networks**
  of contractual and operational relationships
- **Legal Responsibilities and Liabilities** utterly unclear

'Promoting investment and innovation in the Internet of Things' **UK OfCom, Jan 2015**

http://stakeholders.ofcom.org.uk/binaries/consultations/iot/statement/IoTStatement.pdf

- "Ofcom has identified several priority areas **to help support the growth of the IoT**"
- "a common framework that **allows consumers easily and transparently to authorise** the conditions under which **data** collected by their devices is **used and shared by others** will be critical to future development of the IoT sector" (p.2)
- "... **the need for industry-led approaches that will allow consumers to authorise** easily and transparently the conditions under which data collected by their devices can be shared" (p.5)
- "**industry is aware of these challenges and work is ongoing** to deliver secure and robust IoT networks and services" (p.6)

ACMA (2015) 'The Internet of Things ...' Australian Communications and Media Authority, November 2015, at http://www.acma.gov.au/~/media/Regulatory%2520Frameworks%2520and%2520International%2520Engagement/Issues%2520for%2520comment/pdf/Internet%2520of%2520Things_occasional%2520paper%2520pdf.pdf

- " ... **the regulator for communications and media, the Australian Communications and Media Authority (the ACMA)** is assessing **how existing regulation can be used to facilitate and enable** Australian businesses and citizens to benefit from IoT innovations"
- Forbearance: " ... **a decision to not take regulatory action or forbear can be important** to removing an impediment to action, as well as providing the opportunity for industry participants to develop a solution to an issue" (p.21)
- Use of alternatives to direct regulation: " ... **industry co- and self-regulatory arrangements provide a key mechanism for addressing issues of concern to industry participants** ..." (p.21-22)
- "**Educating and informing citizens** ..." (p.24)
- **'What Risks??'** Risks are referred to only fleetingly and vaguely

'Absolute-Minimum IT Security Safeguards' proposed to the Aust PC'er for use as a Baseline

('If you haven't implemented these, the onus is on you to justify why not')

1. Physical Safeguards
2. Access Control
3. Malware Detection and Eradication
4. Patching Procedures
5. Firewalls
6. Incident Management Processes
7. Logging
8. Backup and Recovery Plans, Procedures
9. Training
10. Responsibility

Beyond the Absolute-Minimum Safeguards

Risk Asssessment, leading to at least some of:

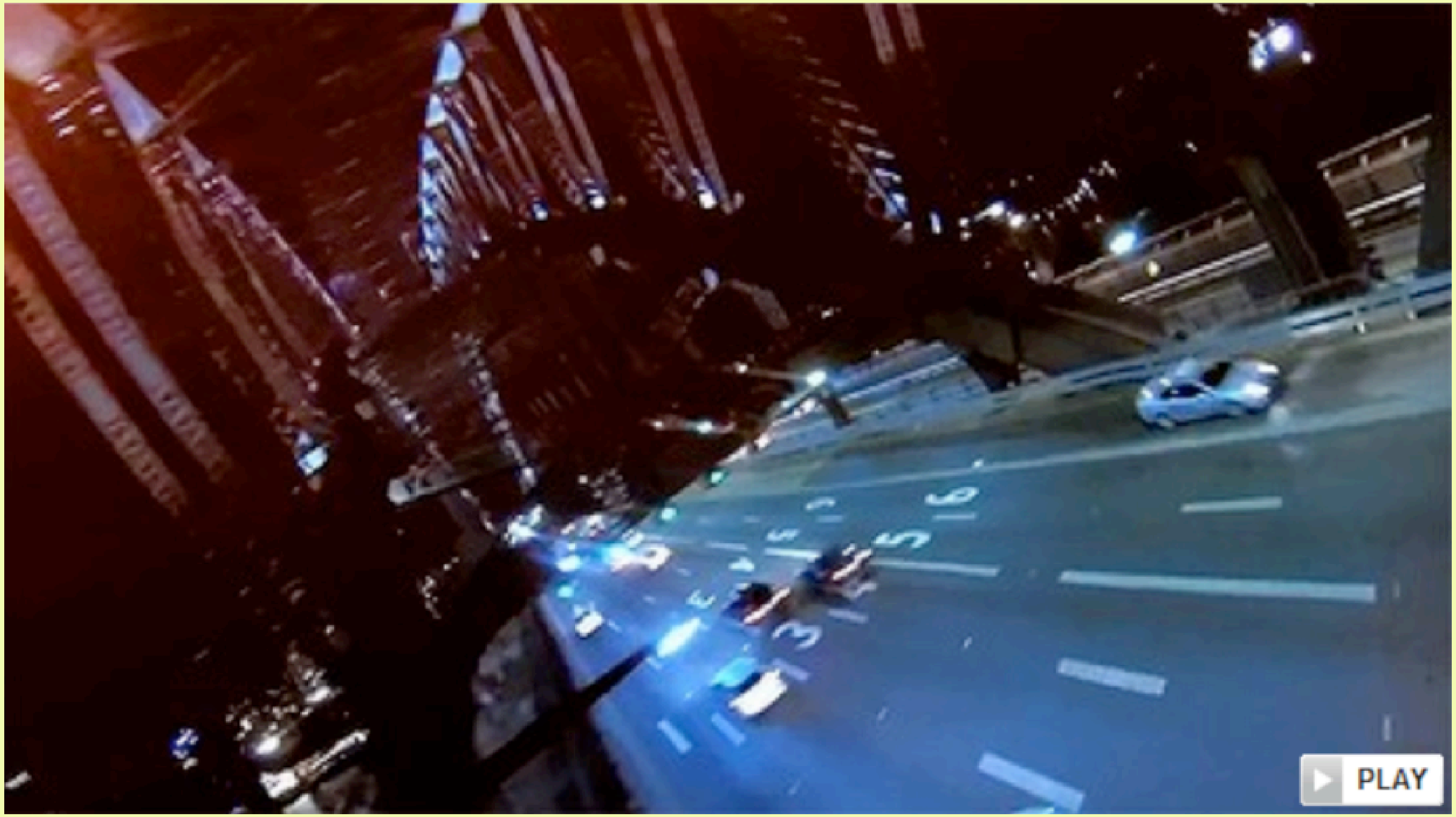
11. Data Communications Encryption
12. Data Storage Encryption
13. Vulnerability Testing
14. Standard Operating Environments
15. Application Whitelisting
16. Device Authentication and Authorisation
17. Use of Virtual Private Networks
18. Intrusion Detection and Prevention
19. User Authentication
20. Firewall Configurations, Outbound

3.4 Remotely-Piloted Drones

These things are dangerous

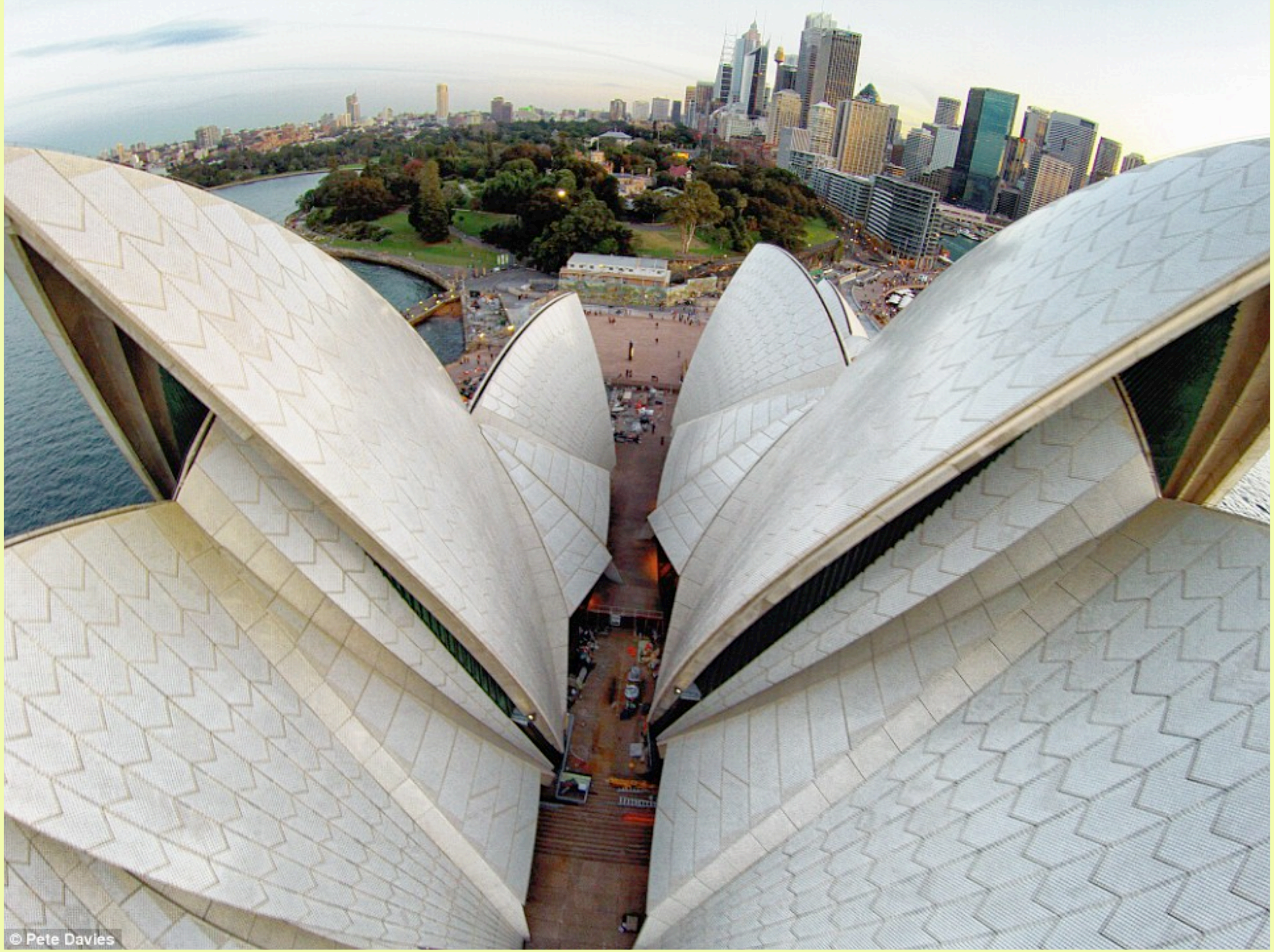
- Risk-Prone Devices
- Risk-Prone Operators
- Risk-Prone Uses

The Prescott Case – Sydney, 2 Oct 2013



http://www.smh.com.au/technology/sci-tech/i-dont-know-whether-its-a-bomb-or-not-train-driver-flummoxed-after-drone-hits-sydney-harbour-bridge-20131126-2y76m.html

http://www.liveleak.com/view?f=dccca42c2905&ajax=1&player_width=512&player_height=384&iframe=true&width=550&height=420



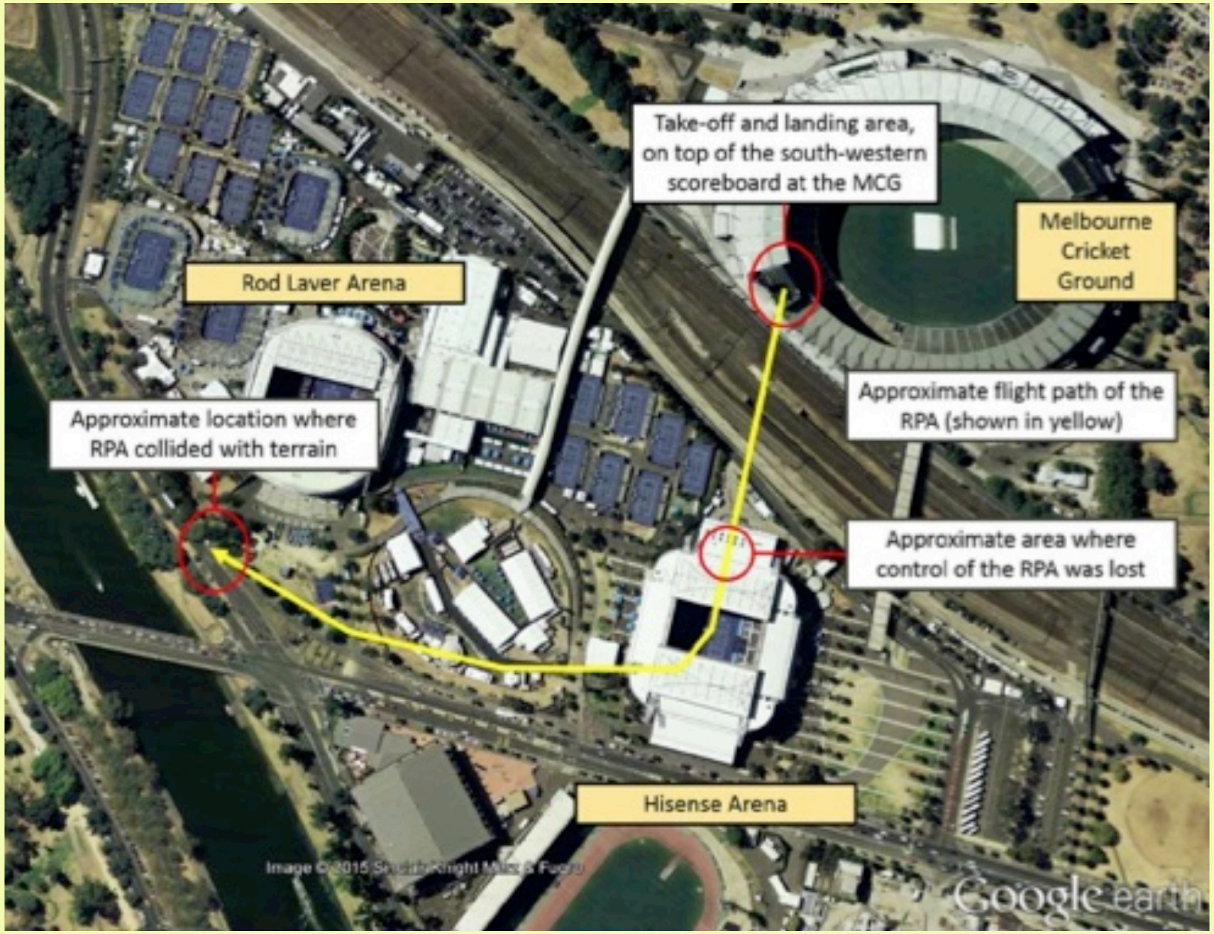
http://www.dailymail.co.uk/news/article-2905158/The-Sydney-Opera-House-Aussie-landmarks-like-NEVER-seen-One-man-drone-offer-completely-different-perspective-world-s-photographed-places.html#ixzz3oWGK6Vlh

WA Triathlon

8 April 2014

Unlicensed pilot, Warren Abrams, New Era Photography and Film
Crashed into a competitor, requiring treatment, stitches
The operator unconvincingly claimed interference or hijack
DPP declined to prosecute; CASA levied an AUD 1700 fine

http://atsb.gov.au/media/5680302/ao-2015-035_final_report.pdf
http://www.abc.net.au/news/2014-11-13/drone-operator-at-geraldton-marathon-fined/5887196


Take-off and landing area, on top of the south-western scoreboard at the MCG
Melbourne Cricket Ground
Rod Laver Arena
Approximate flight path of the RPA (shown in yellow)
Approximate location where RPA collided with terrain
Approximate area where control of the RPA was lost
Hisense Arena
Image © 2015 Sinclair Knight Merz & Fugro
Google earth

MCG

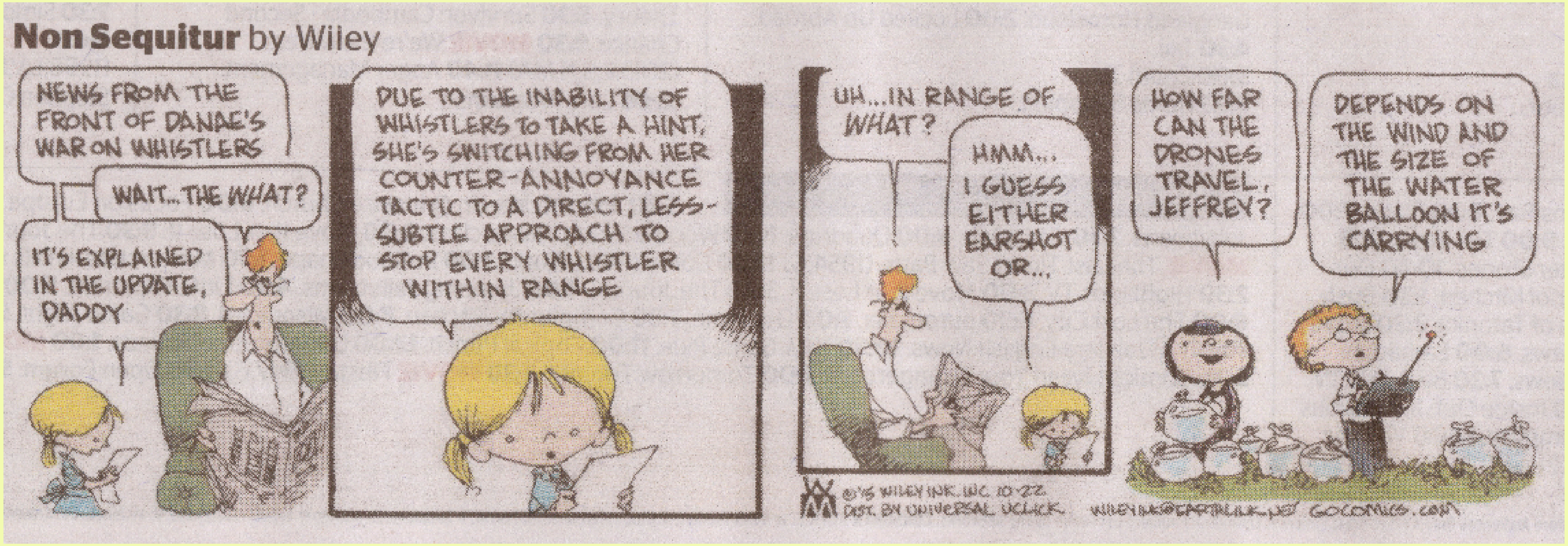
ICC
World Cup Final
29 March 2015

93000 People

Unidentified but licensed company, 3 operators
Multiple control modes, 200m-450m distance
All control was lost – Crashed onto a nearby median strip
Cause unknown – assumed radio frequency interference

http://atsb.gov.au/media/5680302/ao-2015-035_final_report.pdf

Drones and Safety


Non Sequitur by Wiley
NEWS FROM THE FRONT OF DANAE'S WAR ON WHISTLERS
WAIT... THE WHAT?
IT'S EXPLAINED IN THE UPDATE, DADDY
DUE TO THE INABILITY OF WHISTLERS TO TAKE A HINT, SHE'S SWITCHING FROM HER COUNTER-ANNOYANCE TACTIC TO A DIRECT, LESS-SUBTLE APPROACH TO STOP EVERY WHISTLER WITHIN RANGE
UH...IN RANGE OF WHAT?
HMM... I GUESS EITHER EARSHOT OR...
HOW FAR CAN THE DRONES TRAVEL, JEFFREY?
DEPENDS ON THE WIND AND THE SIZE OF THE WATER BALLOON IT'S CARRYING
©'15 WILEY INK, INC. 10-22
DIST. BY UNIVERSAL UCLICK
WILEYINK@EARTHLINK.NET GOCOMICS.COM

Non Sequitur, October 2015

3.4 Remotely-Piloted Drones Device 'Failure Modes'

Artefact Failure

- Mechanical
- Electrical
- Power
- Programming
- 'Fail-Secure' Misdesign

Pilot Failure

- Education /U'stding
- Training / Skill
- Concentration / Timing
- Contextual Appreciation

Environmental Factors

- Physical Congestion
- Turbulence
- Lightning
- Communications
  - Interruption
  - Data Corruption

'Fail-Secure'?

- Remain in Place
- Land Immediately
- Auto-Return to Origin

XAMAX Consultancy Pty Ltd

Operator-Related Challenges

Modes of Operation:

- VLOS (Visual Line of Sight)
- FPV (First Person View)
  - As an Aid
  - Exclusive (Goggles)
- Instrument-Based Ops (IBO)

Formations:

- Single-Device
- Team / Squadron
- Swarm / Flock

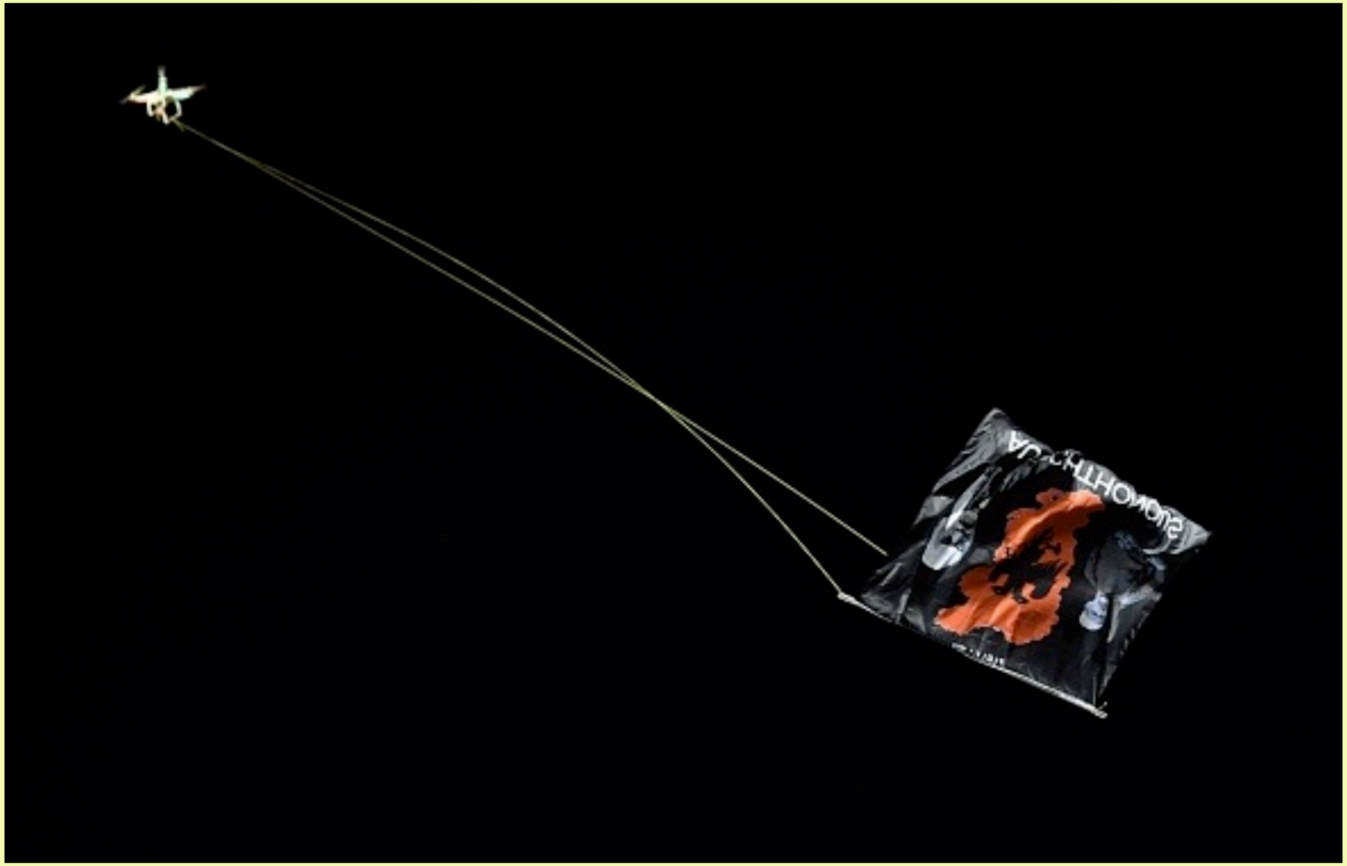
Human Capabilities and Limitations:

- Education ==>> Understanding
- Training ==>> Expertise
- Concentration ==>> Performance
- Task Design ==>> Avoidance of Cognitive Overload
- Risks of Error
  Mis-Judgement
  Dehumanisation

Use-Related Challenges

- **Physical Congestion**
  - Indoors, Forests, Buildings, Pole-Strung Cables, Airport, Emergency Scene (ghoul factor), Celebs/Notorieties (fan/parapazzi factor)
- **Electronic Congestion**
- **Contention**
  - Scheduled Aircraft, Emergency Ops (Search, Fire, Accident, Hostage, Stake-Out)
- **Criminal Uses**
  - Delivery, Diversion, as a Weapon, Jamming
- **Sociopathic Uses**
  - Interference, Weapon-Carriage, Kamikaze

Addendum: Incitement



Euro 2016
Serbia v. Albania
Belgrade
13 Oct 2014

A drone was used to fly a flag over the ground
The flag depicted so-called Greater Albania,
challenging Serbia's sovereignty over Kosovo
Serbian players pulled the flag to the ground

Crowd violence erupted
The players were pelted
The game was abandoned
The result went to court
Both sides were fined EUR 100,000

http://www.theguardian.com/football/2014/oct/14/serbia-albania-euro-2016-flag-halted
https://en.wikipedia.org/wiki/Serbia_v_Albania_(UEFA_Euro_2016_qualifying)

Risks Involving Harm to Public Safety

Impact Factors

- Aircraft Velocity
- Propellor Velocity
- Mass
- The Object that's hit

Consequential Harm

- Explosion / Fire
- Surprise / Diversion
- ***Incited Conflict***

Physical Interference

- Air Ops
- Ground Ops

Comms Interference

- Congestion
- Jamming

Public Safety
Social Controls

- Model Aircraft Clubs
  - Isolated Location
  - Constraints
  - Acculturation
  - Insurance

- No Powers, No Enforcement
- No Incentives to Drone Users to Join

Public Safety

Social Controls

- Model Aircraft Clubs
    - Isolated Location
    - Constraints
    - Acculturation
    - Insurance
- No Powers, No Enforcement
- No Incentives to Drone Users to Join

Regulatory Action

- Accidental and Incidental Protections
- Slow Adaptation
- US FAA Pseudo-Controls
- UK / EU (Still Bumbling?)
- AU Permissiveness and Facilitation, without any Public Consultation

3.5 Autonomous Vehicles

These things are dangerous too

- Risk-Prone Devices
- Risk-Prone 'Drivers'
- Risk-Prone Uses

Differently dangerous from human drivers

3.5 Autonomous Vehicles

- **Diverse Contexts of Use**
(motorways, dual highways, variable signage, single-lane tracks, pedestrian traffic, bike traffic, wet roads, poor visibility, roadworks, traffic jams, ...)
- **Diverse Failure Modes**
(hardware, software, wetware, ...)
- **Absence of ...** Humanlike Flexibility, Adaptability, Appreciation of Human Behaviour
- **Presence of ...** Unauditable AI, 'Learning' Algorithms

https://www.theguardian.com/technology/2016/jan/12/google-self-driving-cars-mistakes-data-reports

Driverless Vehicle Trials in South Australia

- South Australia facilitated open-road trials in 2016
- The amendment gives the Minister *carte blanche*, with no requirements other than insurance, and it voids all State liability, permits suppression of data
- Australian Driverless Vehicle Initiative (ADVI): "ADVI's responsibility includes advocating for national consistency in policy, legislation, regulation" [but not effectiveness for the public]
- ADVI 'Partners' include the S.A. Government

http://www.austlii.edu.au/au/legis/sa/num_act/mvoataa201610o2016641/
http://www.premier.sa.gov.au/index.php/stephen-mullighan-news-releases/337-sa-becomes-first-australian-jurisdiction-to-allow-on-road-driverless-car-trials
http://advi.org.au/2016/05/05/summary-statement/

Framework for Automotive Cybersecurity Best Practices

http://www.autoalliance.org/index.cfm?objectid=E24E1D80-12F0-11E6-85D0000C296BA163

Auto Alliance: http://www.autoalliance.org/auto-issues/cybersecurity

Undated, but apparently of February 2016

"The Framework centers on the following **overarching and guiding principles**:

1) Vehicle security by design
2) Risk assessment and management
3) Threat detection and protection
4) Incident response
5) Collaboration and engagement with appropriate third parties" (p.2)

"The **use** of the Framework and the forthcoming Best Practices **will be a voluntary member decision made independently by each automaker**" (p.3)

"**The forthcoming Best Practices will** ..." (p.4)

" ... **<u>the details of the framework will only be released to ... members</u>**, to protect the effectiveness of the security strategies" (Jul 2016)

http://www.itnews.com.au/news/car-makers-issue-cybersecurity-best-practice-guide-431407

3.6 The EC's GDPR
Data Protection Impact Assessment ('DPIA')

3.6 The EC's GDPR
Data Protection Impact Assessment ('DPIA')

- The Trigger (Art. 35.1-35.6):
  Only '**high risks** to the rights and freedoms of data subjects' ...
- 'An assessment of the **impact of** the envisaged processing **operations [only] on the protection of personal data**' (35.1). So:
  - **not driven by social values**, and will be interpreted as a mere Data Protection Law Compliance Assessment
  - **not all five dimensions, and not even data privacy**, but merely the sub-set that is subject to data protection
- **Seeking civil society's views is optional, and there is no requirement that they be reflected in the design** (35.9)
- **Exemption** for authorised programs (35.10)
- **Feature implementation is optional**, ditto review (35.7(d), 35.11)

http://www.privacy-regulation.eu/en/35.htm

A DPIA isn't a PIA

(1) It's merely a Privacy Law Compliance Audit
(2) There's no need to do anything afterwards

- a methodical ...
- and independent ...
- assurance process ...
- to elicit evidence ...
- **to establish whether practices conform with [insert the legal authority/ies] ...**
- **to identify deficiencies** and ...
- to indicate how deficiencies will be eliminated

3.7 The Precautionary Principle

Strong / Legal Form:

"When human activities may lead to morally unacceptable harm that is scientifically plausible but uncertain, **actions shall be taken to avoid or diminish that [potential] harm**"

http://unesdoc.unesco.org/images/0013/001395/139578e.pdf

Moderate / Moral Form:

'If an action or policy is suspected of causing harm,
and scientific consensus that it is not harmful is lacking,
the burden of proof ... falls on those taking [the] action'

After https://en.wikipedia.org/wiki/Precautionary_principle

The Precautionary Principle in Australian Environmental Law

If:

(1) a threat of serious or irreversible environmental damage exists; &

(2) there is scientific uncertainty as to the extent of possible damage

Then:

A. precautionary measures may be imposed by the court to avert the anticipated threat, but such measures must be appropriate and proportionate

Telstra Corporation Limited v Hornsby Shire Council [2006] NSWLEC 133 (24 March 2006), esp. paras. 113-183
http://www.austlii.edu.au/au/cases/nsw/NSWLEC/2006/133.html

The Precautionary Principle
A Forlorn Hope

Strong / Legal Form (in some environment laws only):

"When human activities may lead to morally unacceptable harm that is scientifically plausible but uncertain, **actions shall be taken to avoid or diminish that [potential] harm**"

http://unesdoc.unesco.org/images/0013/001395/139578e.pdf

Moderate / Moral Form (much-discussed, seldom imposed):

'If an action or policy is suspected of causing harm, and scientific consensus that it is not harmful is lacking, **the burden of proof ... falls on those taking [the] action'**

After https://en.wikipedia.org/wiki/Precautionary_principle

These Are All Regulatory Failures

Reasonable / Naïve Public Expectations Are Not Being Fulfilled

- Organisations don't undertake evaluation processes that reflect multiple Stakeholders' interests
- So the requirement has to be imposed from without
- But Executives and Legislatures are interested only in stimulatory measures, not in ensuring appropriate controls and mitigation measures are in place

XAMAX Consultancy Pty Ltd

Regulatory Failure in the Security Space

Agenda

1. 'Whose Security?'
2. The Regulatory Framework
3. Some Test-Cases
   - 3.1 PIAs and National Security
   - 3.2 Big Data Analytics
   - 3.3 (Inter)net of (Every)Thing(s) (and People)
   - 3.4 Remotely-Piloted Drones
   - 3.5 Driverless Cars
   - 3.6 EC GDPR DPIAs
   - 3.7 The Precautionary Principle
4. Conclusions

4. Conclusions

Policy Perspective

- Executives and Legislatures need to be forced to perform their functions, and ensure effective regulation of potentially harmful behaviours

Research Perspective

- More and deeper case studies
- Process studies in insecurity
- Studies of effectiveness of particular safeguards

Regulatory Failure in the Security Space: Some Current Cases

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra

Visiting Professor in Computer Science, ANU, Canberra
Visiting Professor in Cyberspace Law & Policy, UNSW, Sydney

http://www.rogerclarke.com/DV/RFSS {.html, .pdf}

Norwegian Research Center for Computers and Law
University of Oslo – 29 August 2016