The Contested Semantics of 'Security' and the Current Challenges of Big Data and IoT

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/CSS {.html, .pdf}

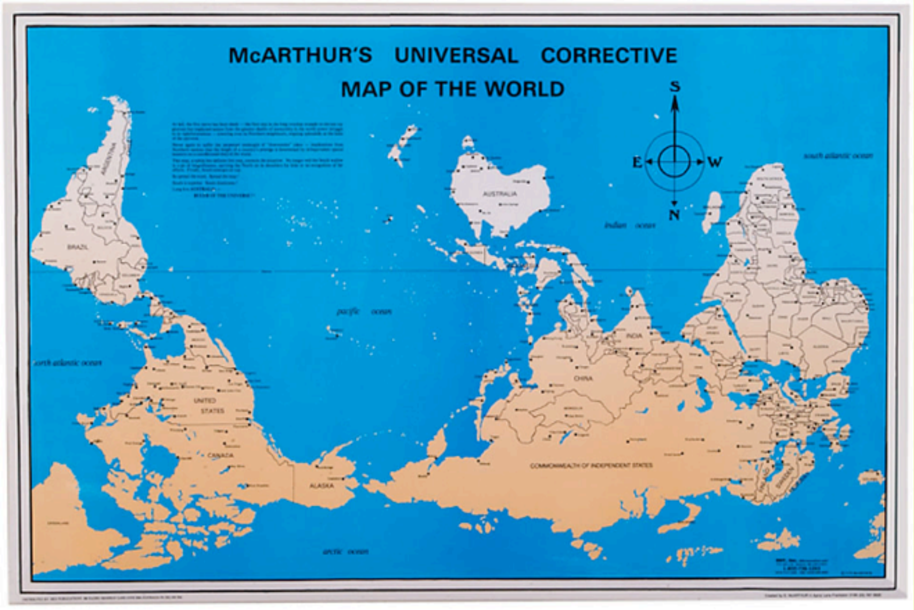
Cybercake, the Institute of Law and Technology, and CSIRT-MU – Masaryk University

24 November 2016

The Contested Semantics of 'Security' and the Current Challenges of Big Data and IoT

Agenda

- The Contested Semantics of 'Security'
- The Concept of 'National Security'
- Current Challenges – Big Data, IoT
- The Critical Roles of Evaluation, Quality Assurance and Risk Mngt



http://www.odt.org/southupmaps.htm

The Notion of Security

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

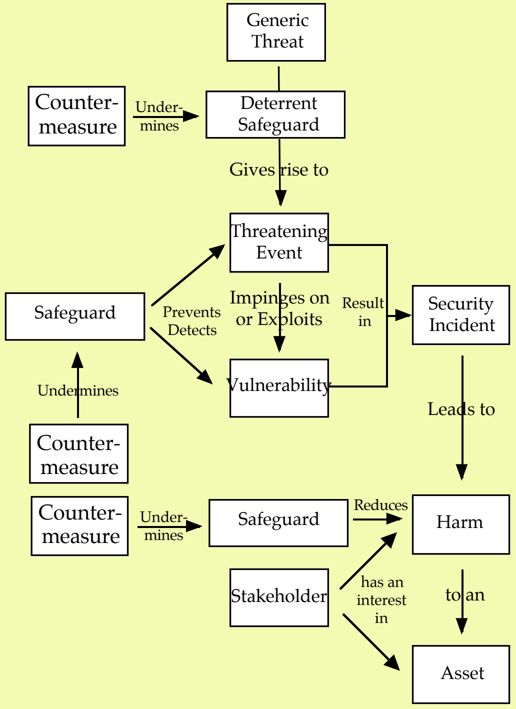
A set of safeguards
whose purpose is
to achieve that condition

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**

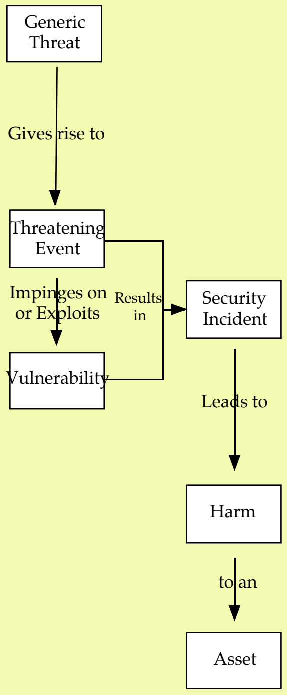
- A **Safeguard** is a measure to counter a Threat
- A **Countermeasure** is an action to circumvent a Safeguard

The Conventional Security Model


Generic Threat
Counter-measure
Under-mines
Deterrent Safeguard
Gives rise to
Threatening Event
Safeguard
Prevents Detects
Impinges on or Exploits
Result in
Security Incident
Vulnerability
Undermines
Counter-measure
Leads to
Counter-measure
Under-mines
Safeguard
Reduces
Harm
Stakeholder
has an interest in
to an
Asset

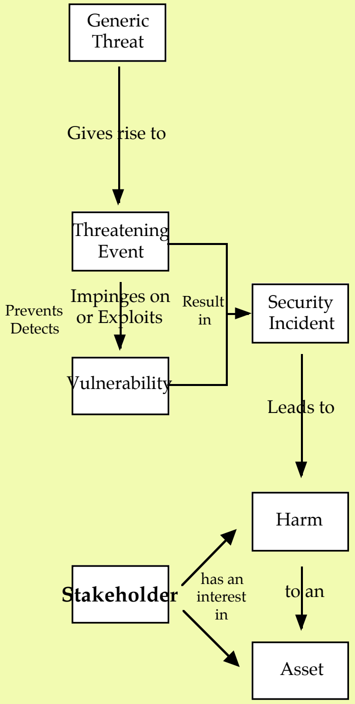
http://www.rogerclarke.com/
EC/PBAR.html#App1

The Conventional Security Model


Generic Threat
Gives rise to
Threatening Event
Impinges on or Exploits
Results in
Security Incident
Vulnerability
Leads to
Harm
to an
Asset

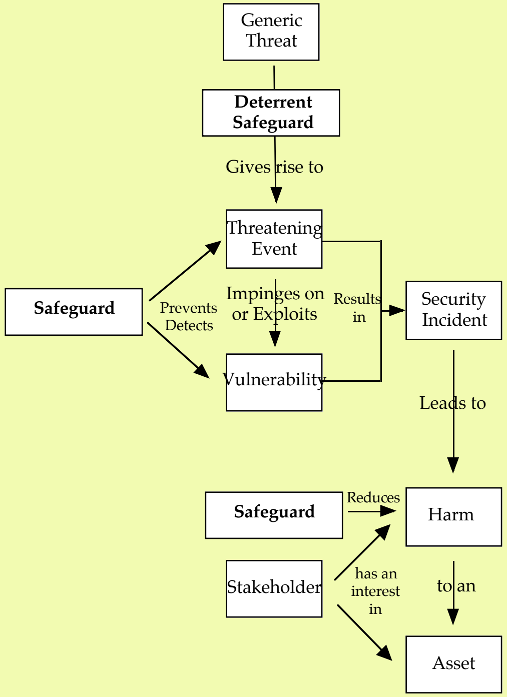
http://www.rogerclarke.com/
EC/PBAR.html#App1

The Conventional Security Model
+
Stakeholder


Generic Threat
Gives rise to
Threatening Event
Prevents Detects
Impinges on or Exploits
Result in
Security Incident
Vulnerability
Leads to
Harm
Stakeholder
has an interest in
to an
Asset

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

The Conventional Security Model + Safeguards



Generic Threat

Deterrent Safeguard

Gives rise to

Threatening Event

Safeguard

Prevents Detects

Impinges on or Exploits

Results in

Security Incident

Vulnerability

Leads to

Safeguard

Reduces

Harm

Stakeholder

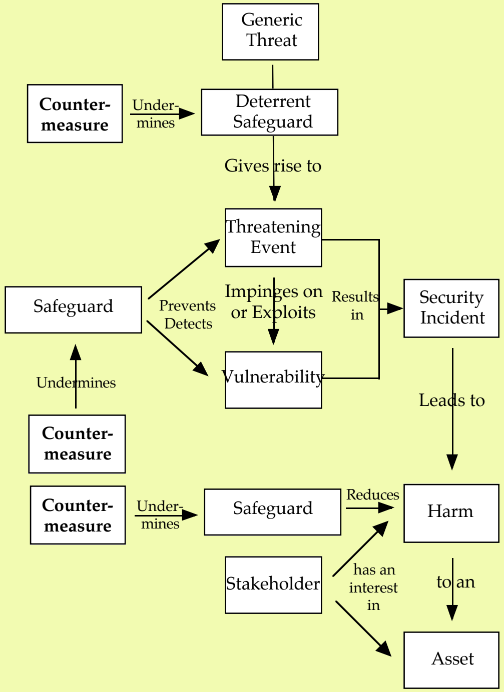
has an interest in

to an

Asset

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

The Conventional Security Model + Countermeasures



Generic Threat

Counter-measure

Under-mines

Deterrent Safeguard

Gives rise to

Threatening Event

Safeguard

Prevents Detects

Impinges on or Exploits

Results in

Security Incident

Undermines

Vulnerability

Counter-measure

Leads to

Counter-measure

Under-mines

Safeguard

Reduces

Harm

Stakeholder

has an interest in

to an

Asset

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

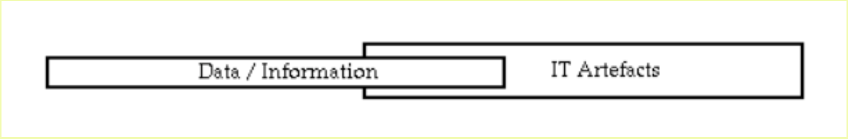
Asset, Harm, Value, Stakeholder

- **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?'

http://www.rogerclarke.com/EC/WS-1301.html

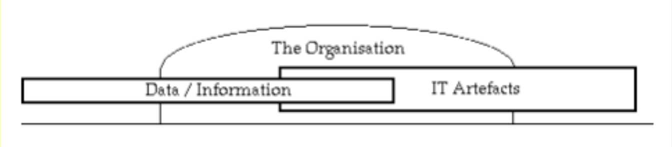
The Scope of Security



Data / Information

IT Artefacts

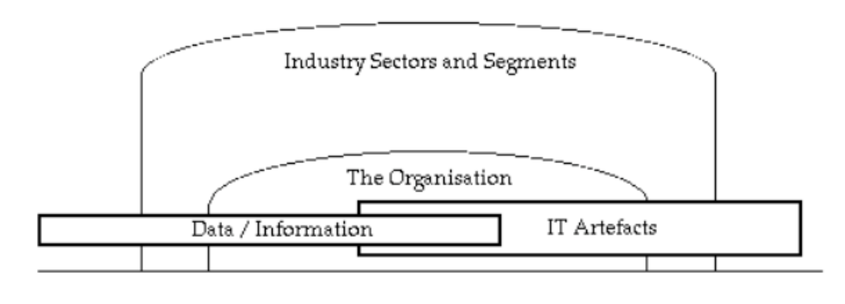
The Organisational Scope of Security



Tensions

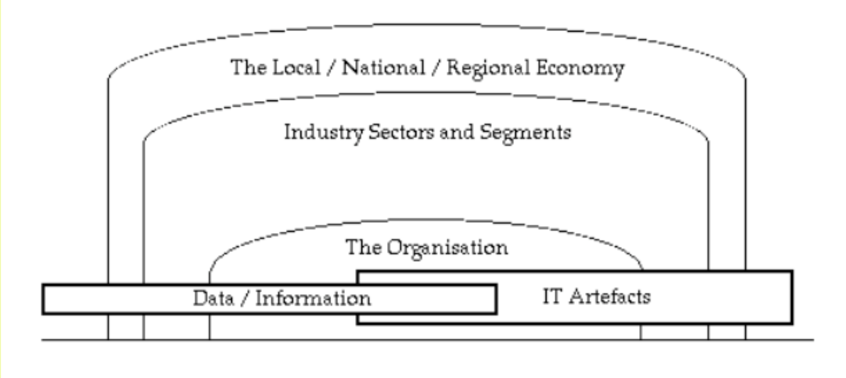
- **Among Organisational Objectives**
  - Certain Costs vs. Contingent Costs
  - Financial Cost vs. Non-Quantifiables
  - Business-As-Usual vs. Invisibles

A Broader Scope for Security



Competition between Corporations
Collaboration, esp. re IT Infrastructure

A Yet Broader Scope for Security

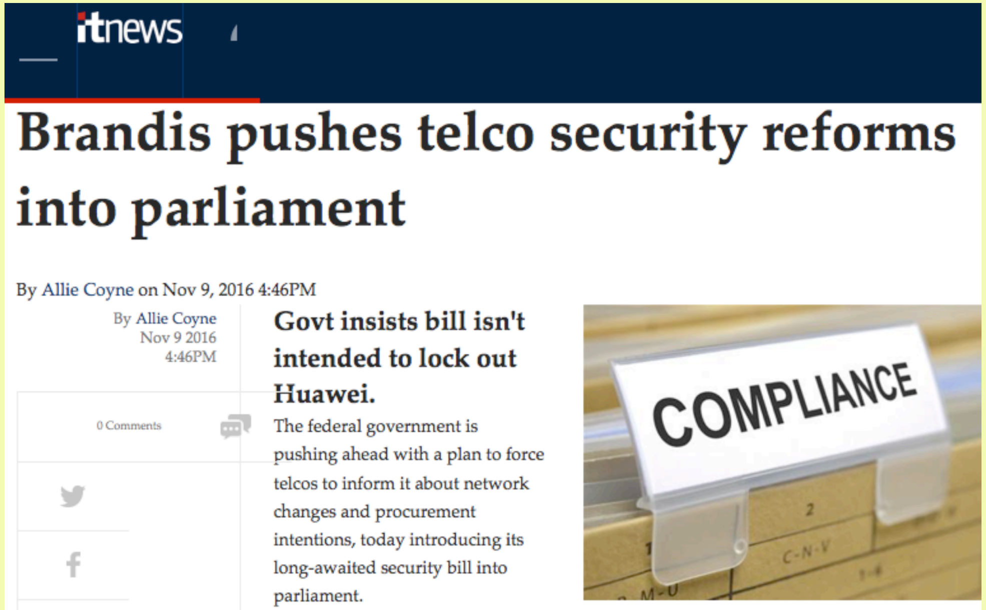

The Local / National / Regional Economy
Industry Sectors and Segments
The Organisation
Data / Information
IT Artefacts

IT Infrastructure for Economic Development
Competition among Nations
'Critical IT Infrastructure'

Industry Sectors Designated by Governments as 'Critical Infrastructure'

- **Military-Industrial incl. Cryptography**
- **Transport**
- **Communications**
- **Energy**
- **Water**

- Public Health
- Emergency Services
- Law Enforcement
- Agriculture
- Financial Services



itnews

Brandis pushes telco security reforms into parliament

By Allie Coyne on Nov 9, 2016 4:46PM

By Allie Coyne
Nov 9 2016
4:46PM

0 Comments

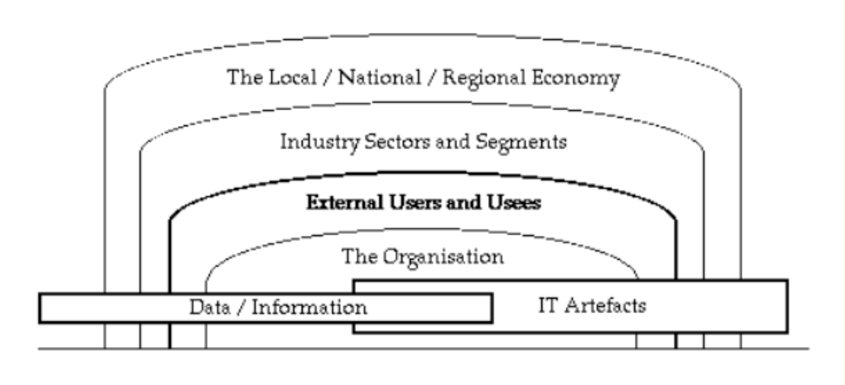
Govt insists bill isn't intended to lock out Huawei.

The federal government is pushing ahead with a plan to force telcos to inform it about network changes and procurement intentions, today introducing its long-awaited security bill into parliament.

http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1051

http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1051_first-senate/toc_pdf/1617120.pdf;fileType=application%2Fpdf

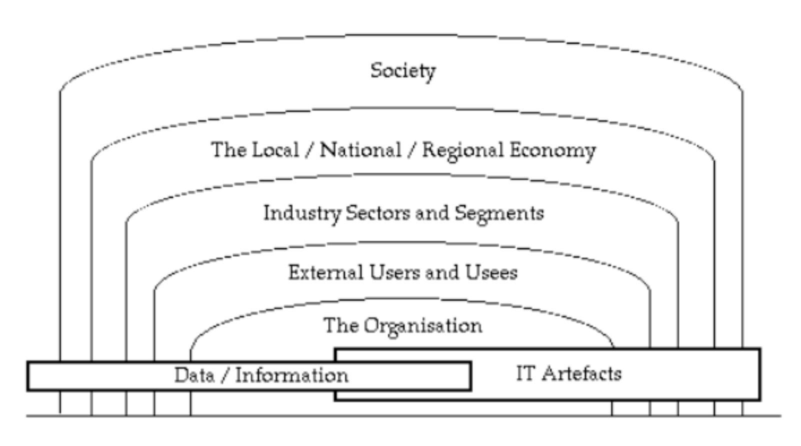
A Mostly-Forgotten Scope for Security



Tensions

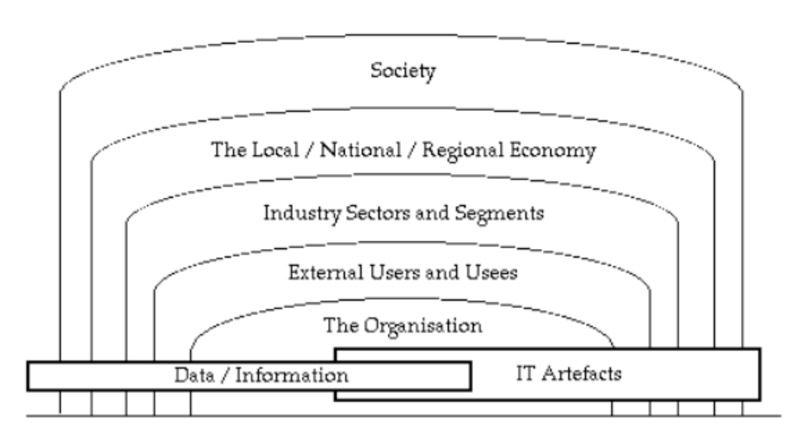
- Among Organisational Objectives
  - Certain Costs vs. Contingent Costs
  - Financial Cost vs. Non-Quantifiables
  - Business-as-usual vs. Invisibles
- **Among Alternative Scope Definitions**
  - A bot doesn’t harm the host, so there’s no incentive to fix it (it's an ‘externality’)
  - Copyright material on P2P networks
  - Personal, Organisational, Sectoral, National, Supra-National Agency Interests

Yet More, Alternative Scope Definitions

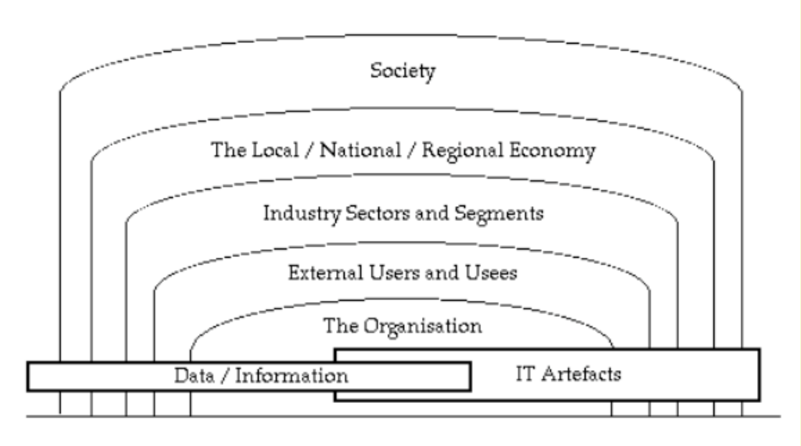


Add in 'Society'. What about 'Humanity'?
What about the Biosphere, the Troposphere?

The Contested Semantics of 'Security'

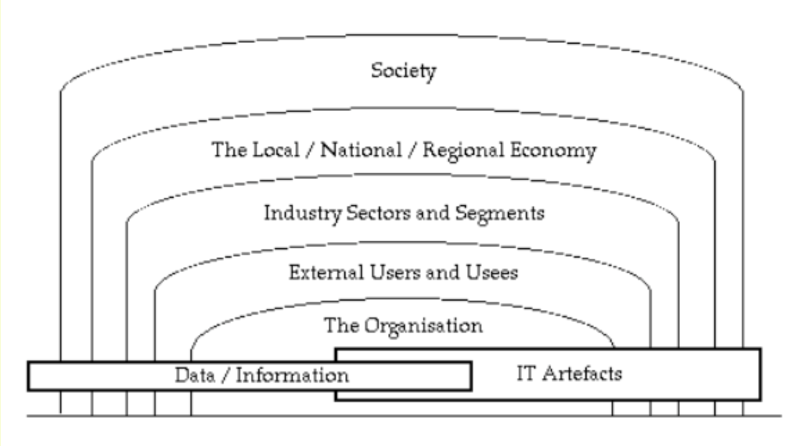


Who are the Champions for Each Perspective?



Which have Power?
What Coalitions are feasible?

And where is ‘National Security’?



Is this 'National Security'?

The protection of a nation from attack or other danger by holding adequate armed forces and guarding state secrets

Encompasses economic security, monetary security, energy security, environmental security, military security, political security and security of energy and natural resources

http://definitions.uslegal.com/n/national-security/

"specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy"

US Freedom of Information Act

Or is this 'National Security'?

- **Critical Infrastructure Security**
  Bombs in ports, ships, railways, energy, ...
  Anthrax in the water supply, ...
- **Public Safety**
  Bombs in aircraft, mayhem in marketplaces
  Major Events, e.g. 'The Euros', The Olympics
- **Prominent Person Safety**
  Bush and Blair; Rushdie and Kurt Westergaard
  Gx, APEC, CHOGM, ...

'Terrorism'

The use of violence or the threat of violence,
especially against civilians,
in order to alarm the public,
in the pursuit of political [or politico-religious] goals

'Terrorism'

The use of violence or the threat of violence,
especially against civilians,
in order to alarm the public,
in the pursuit of political [or politico-religious] goals

'Terrorism' has been conflated with 'National Security'

Some Current Challenges

- Big Data Analytics
- Internet of Things
- (Evaluation Techniques)

Vroom, Vroom
The 'Hype' Factor in Big Data

- Volume
- Velocity
- Variety

- Value

- **Veracity**
- **Validity**
- **Visibility**

Laney 2001, Livingston 2013

Use Categories for Big Data Analytics

- **Population Focus**
  - Hypothesis Testing
  - Population Inferencing
  - Profile Construction
- **Individual Focus**
  - Outlier Discovery
  - Inferencing about Individuals
    - Inconsistencies
    - Non/-conformance with a profile

Bug Data 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

Information Quality
(Assessable only at time of use)

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

Big Data, Big Risks
http://www.rogerclarke.com/EC/BDBR.html#BDQ

Big Data Risk Factors Decision Quality

1. Appropriateness of the Inferencing Technique
2. Data Meaning
3. Data Relevance
4. Transparency
   - Process
   - Criteria

'Quality Factors in Big Data and Big Data Analytics'
http://www.rogerclarke.com/EC/BDQF.html#DeQF

Scenario – Insider Detection

The Minister gives terse instructions about whistleblowers (Brutus, Judas Iscariot, Macbeth, Manning, Snowden, ...)

The agency:

- Increases intrusiveness and frequency of employee vetting
- Lowers the threshold for positive vetting
- Exercises its powers to gain access to and consolidate:
  - border movements • credit history • court records
  - LEA persons-of-interest lists • financial tracking alerts
  - all internal communications • social media postings
- Applies big data analytics to the consolidated database

http://www.rogerclarke.com/EC/BDBR.html#BDAQ
http://www.itnews.com.au/News/391656,brandis-boosts-vetting-of-aps-staff-to-prevent-insider-threats.aspx (2 Sep 2014)

Quality Assurance and Risk Management for Big Data Projects

1. Frameworks
2. Data Consolidation
3. Effective Anonymisation
4. Data Scrubbing
5. Decision-Making

http://www.rogerclarke.com/EC/BDRM.html

http://www.rogerclarke.com/EC/BDQAS.html
Euro Intel & Security Informatics Conf., Uppsala, 17-19 August 2016

{ Ubiquitous Computing, Pervasive Computing, Ambient Intelligence, Mobility and } The (Inter)net of (Every)Thing(s) and People

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

Manwaring K. & Clarke R. (2015)
Computer Law & Security Review 31,5 (October 2015) 586–603
http://www.rogerclarke.com/II/SSRN-id2613198.pdf

{ Ubiquitous Computing, Pervasive Computing, Ambient Intelligence, Mobility and }
The (Inter)net of (Every)Thing(s) and People

eObject – An object 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)
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

- **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

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

IoT as DDoS Vector

- What was new ... was ... the particular devices the attackers recruited. Instead of using traditional computers for **their botnet**, they **used CCTV cameras, digital video recorders, home routers, and other embedded computers attached to the Internet as part of the Internet of Things** [Sep 2016]

  'Security Economics of the Internet of Things'
  https://www.schneier.com/crypto-gram/archives/2016/1015.html#1
- **'Source Code for IoT Botnet ‘Mirai’ Released'** [Oct 2016]
  https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

The Contested Semantics of 'Security' and the Current Challenges of Big Data and IoT

Agenda

- The Contested Semantics of 'Security'
- The Concept of 'National Security'
- Current Challenges – Big Data, IoT
- The Critical Roles of Evaluation, Quality Assurance and Risk Mngt

The Contested Semantics of 'Security' and the Current Challenges of Big Data and IoT

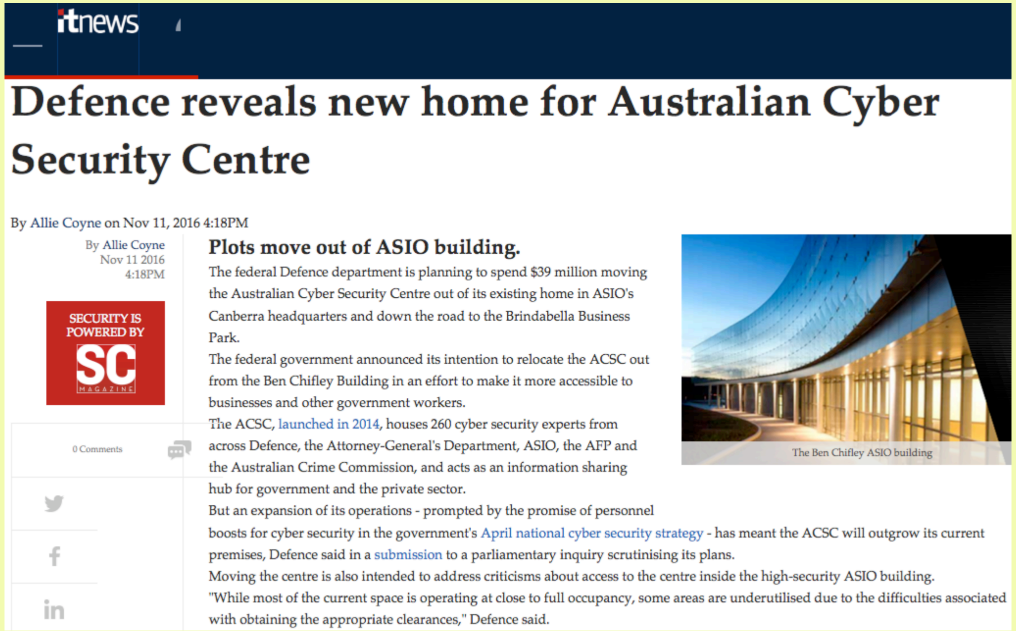
Roger Clarke
Xamax Consultancy Pty Ltd, Canberra
Visiting Professor in Computer Science, ANU, Canberra
Visiting Professor in Cyberspace Law & Policy, UNSW, Sydney
http://www.rogerclarke.com/DV/CSS {.html, .pdf}

Cybercake, the Institute of Law and Technology, and CSIRT-MU – Masaryk University

24 November 2016

Cybersecurity in Australia

- **Australian Cyber Security Centre (ACSC)**
  Since Nov 2014 – http://www.asd.gov.au/infosec/acsc.htm
  "brings together cyber security capabilities from Defence, Attorney-General's Department/GovCERT, Australian Security Intelligence Organisation, Aust Federal Police and Australian Crime Commission in a single location"
- **Cyber Security Strategy (Apr 2016)**
  http://malcolmturnbull.com.au/media/launch-of-australias-cyber-security-strategy, https://cybersecuritystrategy.dpmc.gov.au/
  Assistant Minister for Cyber Security
  Special Adviser to the PM on Cyber Security
  Minister for Foreign Affairs' Cyber Ambassador
  Annual Cyber Security Forums
  Cyber Security Growth [Innovation] Centre



Defence reveals new home for Australian Cyber Security Centre

By Allie Coyne on Nov 11, 2016 4:18PM

By Allie Coyne
Nov 11 2016
4:18PM

Plots move out of ASIO building.

The federal Defence department is planning to spend $39 million moving the Australian Cyber Security Centre out of its existing home in ASIO's Canberra headquarters and down the road to the Brindabella Business Park.

The federal government announced its intention to relocate the ACSC out from the Ben Chifley Building in an effort to make it more accessible to businesses and other government workers.

The ACSC, launched in 2014, houses 260 cyber security experts from across Defence, the Attorney-General's Department, ASIO, the AFP and the Australian Crime Commission, and acts as an information sharing hub for government and the private sector.

But an expansion of its operations - prompted by the promise of personnel boosts for cyber security in the government's April national cyber security strategy - has meant the ACSC will outgrow its current premises, Defence said in a submission to a parliamentary inquiry scrutinising its plans.

Moving the centre is also intended to address criticisms about access to the centre inside the high-security ASIO building.

"While most of the current space is operating at close to full occupancy, some areas are underutilised due to the difficulties associated with obtaining the appropriate clearances," Defence said.

The Ben Chifley ASIO building

http://www.itnews.com.au/news/defence-reveals-new-home-for-australian-cyber-security-centre-441199