Australian Government
Australian Signals Directorate

ACSC
Australian Cyber Security Centre

# A Whirlwind Tour of Emerging Technology & Engineering at the ACSC

Kylie McDevitt

# Outline

- My career pathway
- IoT Security
- Control System Security

# Wanted to be a Lawyer

# Studied Engineering at ANU

- 1996 - 1999

# Senior Engineer at Telstra

ACSC Australian Cyber Security Centre

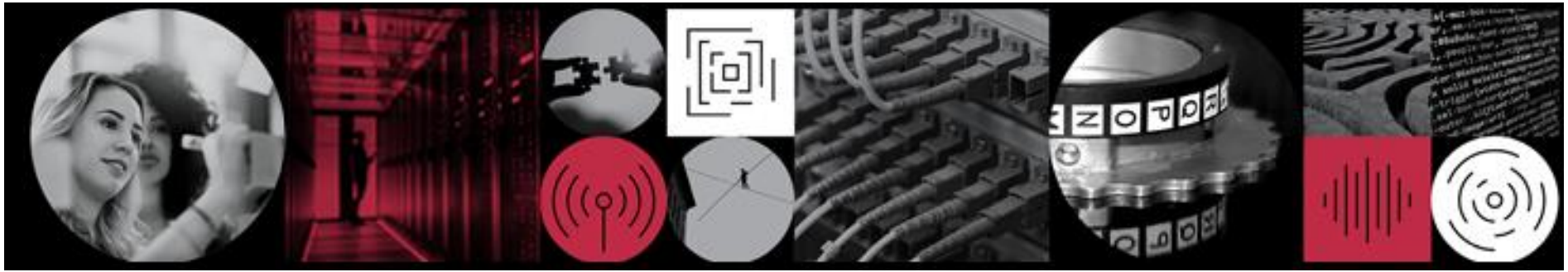
- Interned with Telstra in 1998-99
- Stayed with them until 2003
- Network Development
- Cellular Engineering

# Mum Duties

# ASD/ACSC

ACSC Australian Cyber Security Centre

- Joined in 2009
- Nov 2013 moved into “Cyber Branch”
- 1 year with Cisco in 2015



# Outside Work

- BSides Canberra
- Csides
- www.bsidescbr.com.au/csides.html
- InfoSect Fyshwick
- Cyber Defence lecturer at UNSW Canberra

Australian Government

Australian Signals Directorate

ACSC

Australian
**Cyber Security**
Centre

# IoT Security

# Section Outline

ACSC Australian Cyber Security Centre

1. Intro to IoT

2. Classic IoT attacks + demo

3. Consumer advice

4. Vendor advice, a collaborative effort between techs & policy writers within the ACSC

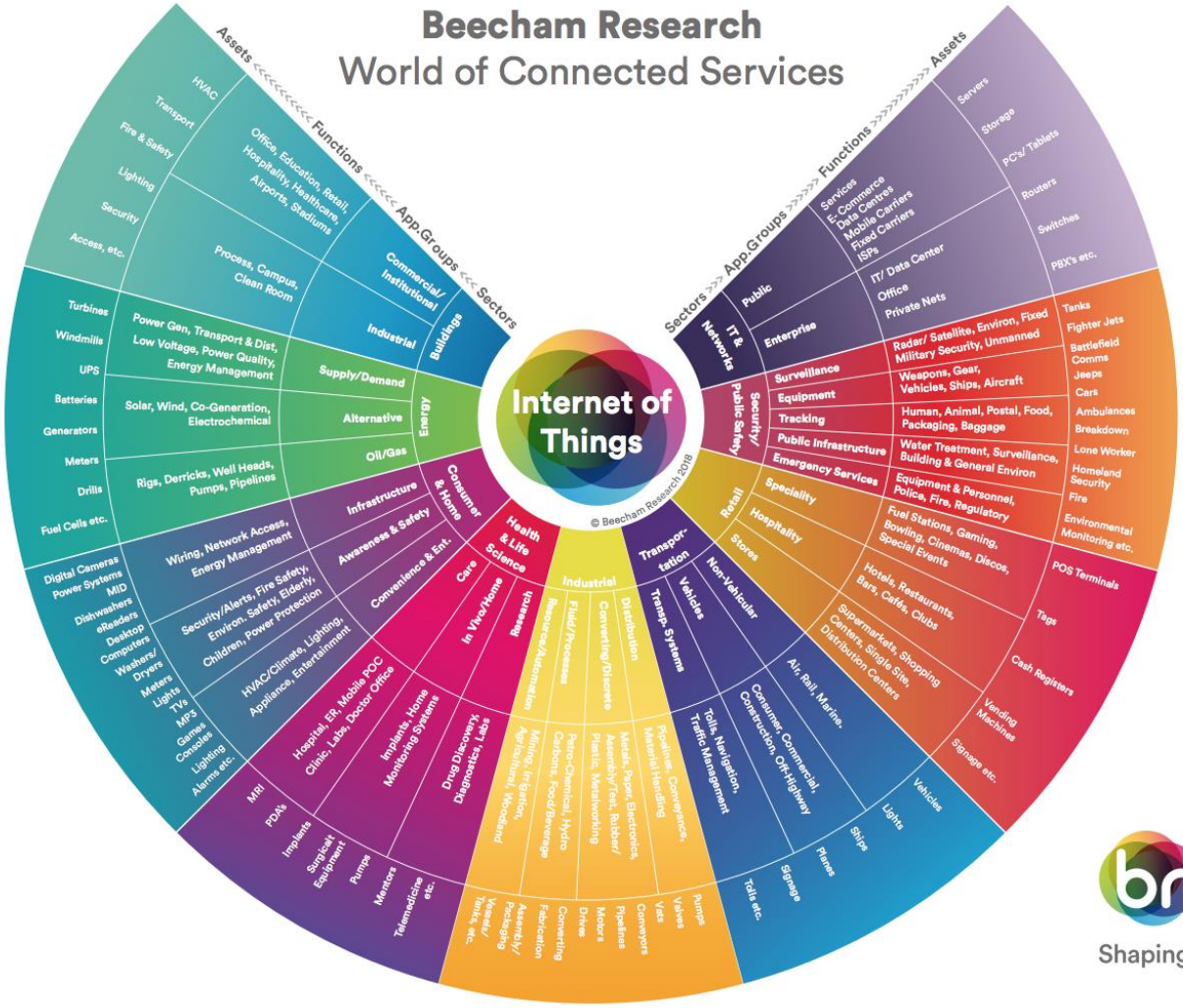
# What is IoT?

IoT is the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

Common examples:

- Home assistants
- Smart devices (TVs, fridges, etc.)
- Home security

# Beecham Research
## World of Connected Services




beecham research

Shaping the IoT future

# IoT Statistics

- In 2008 the number of internet connected things globally exceeded population.
- The Australian home Internet of Things market grew by over 50% in 2017-2018.
- Every second 127 new devices are connected to the internet.
- In 2019 1.9 billion smart home devices are expected to be shipped.
- There is expected to be more than 64 billion IoT devices connected worldwide by 2025.

https://www.newgenapps.com/blog/iot-statistics-internet-of-things-future-research-data
https://www.vxchnge.com/blog/iot-statistics
https://www.businesswire.com/news/home/20181204005588/en/Australia---Internet-Things-IoT-Market-Forecast
https://techjury.net/stats-about/internet-of-things-statistics/

# What does this mean to us as Security Researchers?

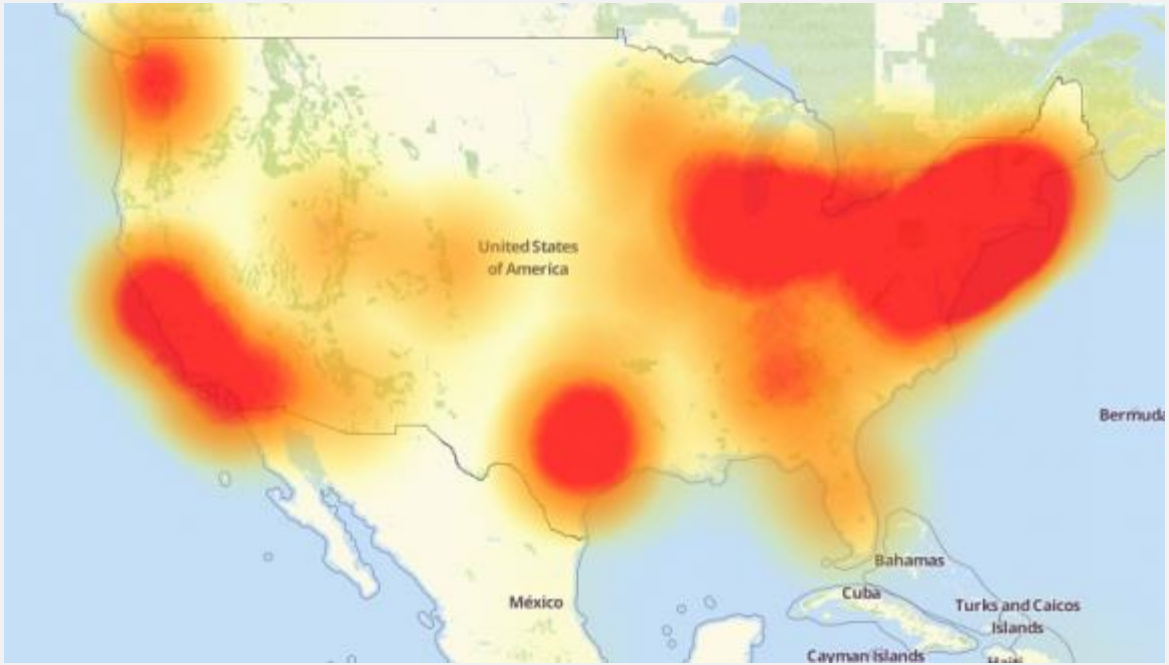
# Security by Obscurity

Firmware is embedded, attackers won't be able to access it

In fact, extracting firmware has been a huge focus of vulnerability researchers for the past decade which has uncovered multiple problems:

- Buggy code
- Embedded default passwords
- Vendor placed backdoors for troubleshooting

# Mirai Botnet - 2016



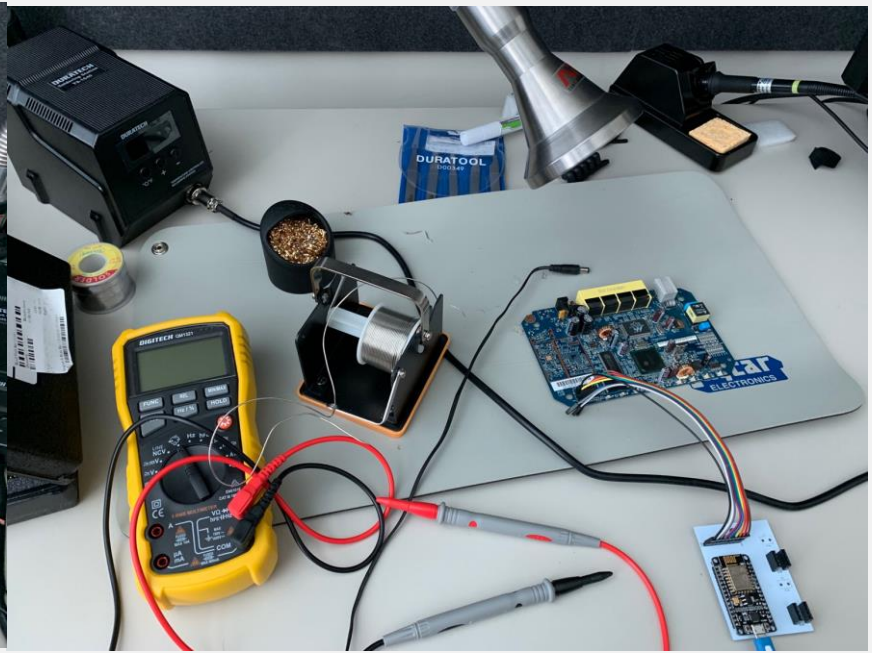

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

# IoT Reaper - 2017

- More sophisticated than Mirai
- Used vulnerabilities in the routers rather than default credentials

https://krebsonsecurity.com/2017/10/reaper-calm-before-the-iot-security-storm/

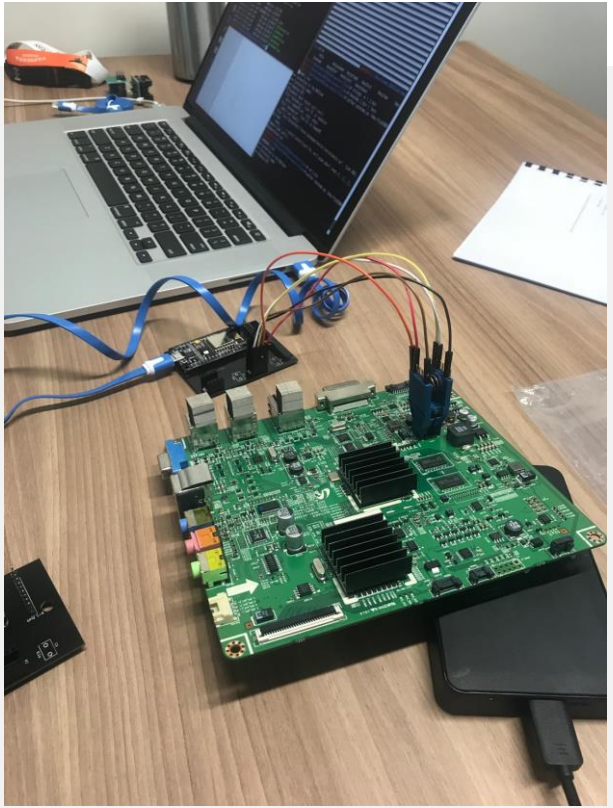
# Building an IoT Lab



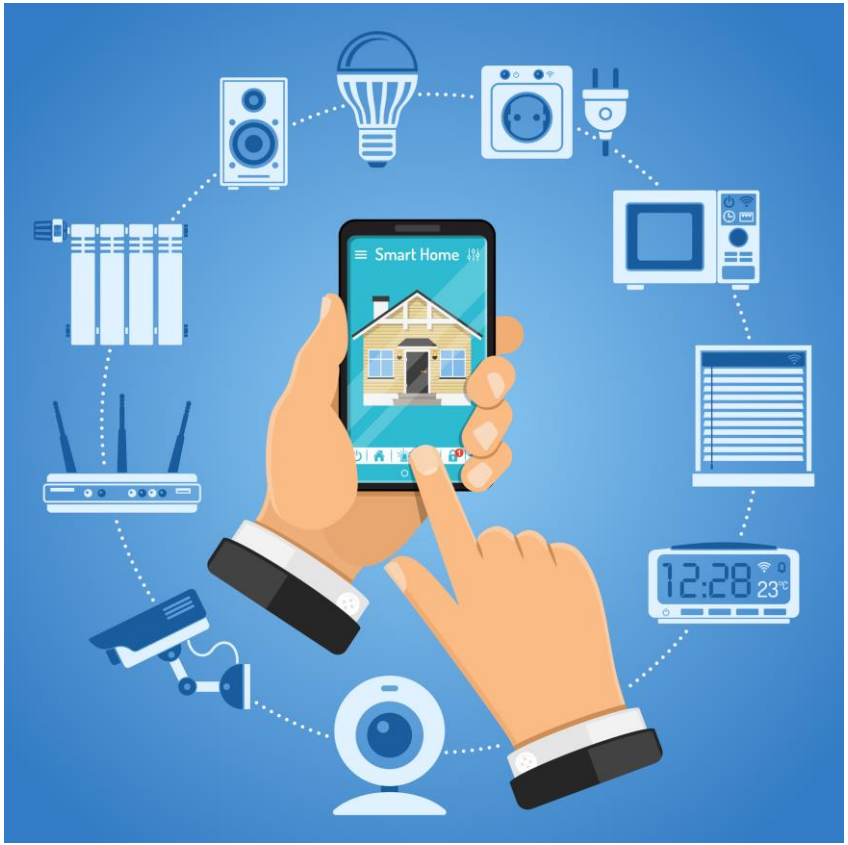
# Extracting Firmware

ACSC Australian Cyber Security Centre

- UART
- JTAG
- SPI



# Case Study

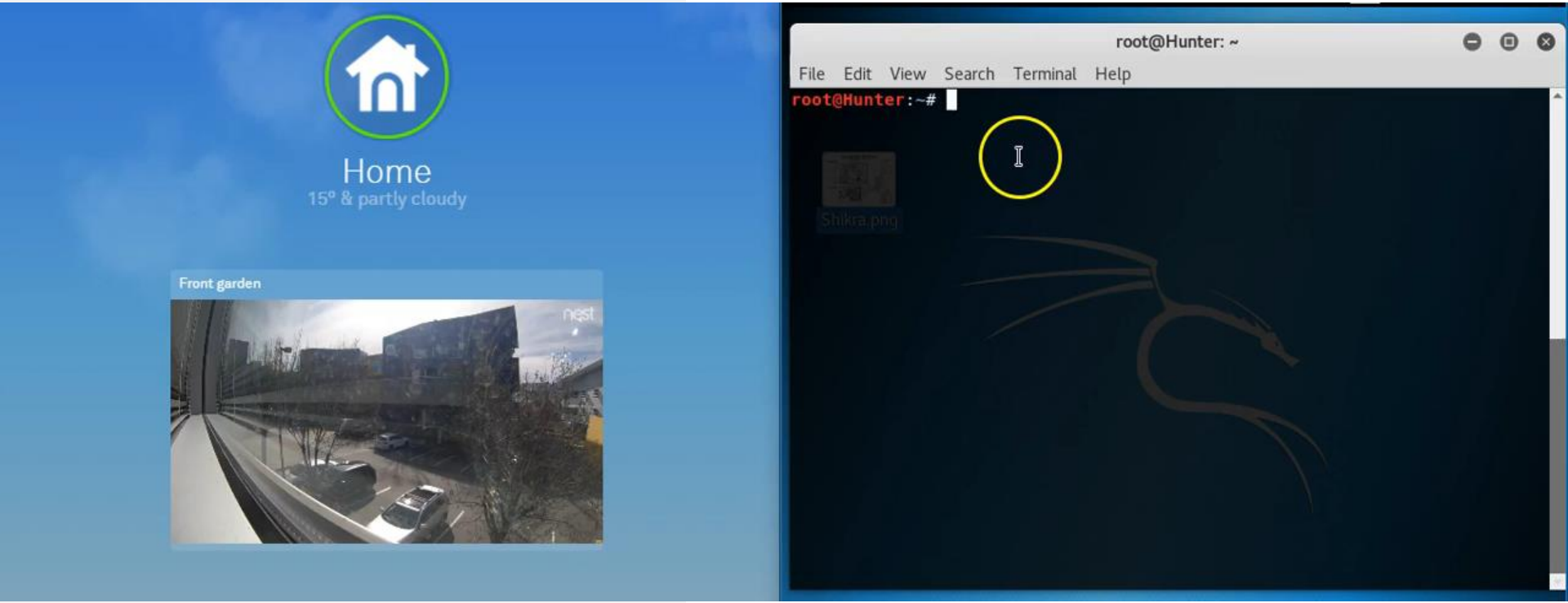


# Google Nest

- Nest Labs is an American manufacturer of smart home products including thermostats, smoke detectors, and security systems including smart doorbells and smart locks
- Acquired by Google in 2014
- After its acquisition of Dropcam in 2014, the company introduced its Nest Cam branding of security cameras beginning in June 2015

```
# Exploit Title: Google Nest Cam - Multiple
Buffer Overflow Conditions Over Bluetooth LE
# Reported to Google: October 26, 2016
# Public Disclosure: March 17, 2017
# Exploit Author: Jason Doyle @_jasondoyle
```

https://www.exploit-db.com/exploits/41643




Credit Dan Hodgson (ACSC AVA)

# How big is this problem?

ACSC Australian Cyber Security Centre

We know we can attack IoT devices

We know this is being spoken about at all the conferences

How bad is the problem in Australia?

# Shodan Scans

ACSC Australian Cyber Security Centre

- Internet Scanner
- Investigating devices on the Internet, but not logging in or testing credentials

# IP Cameras in Australia

ACSC Australian Cyber Security Centre

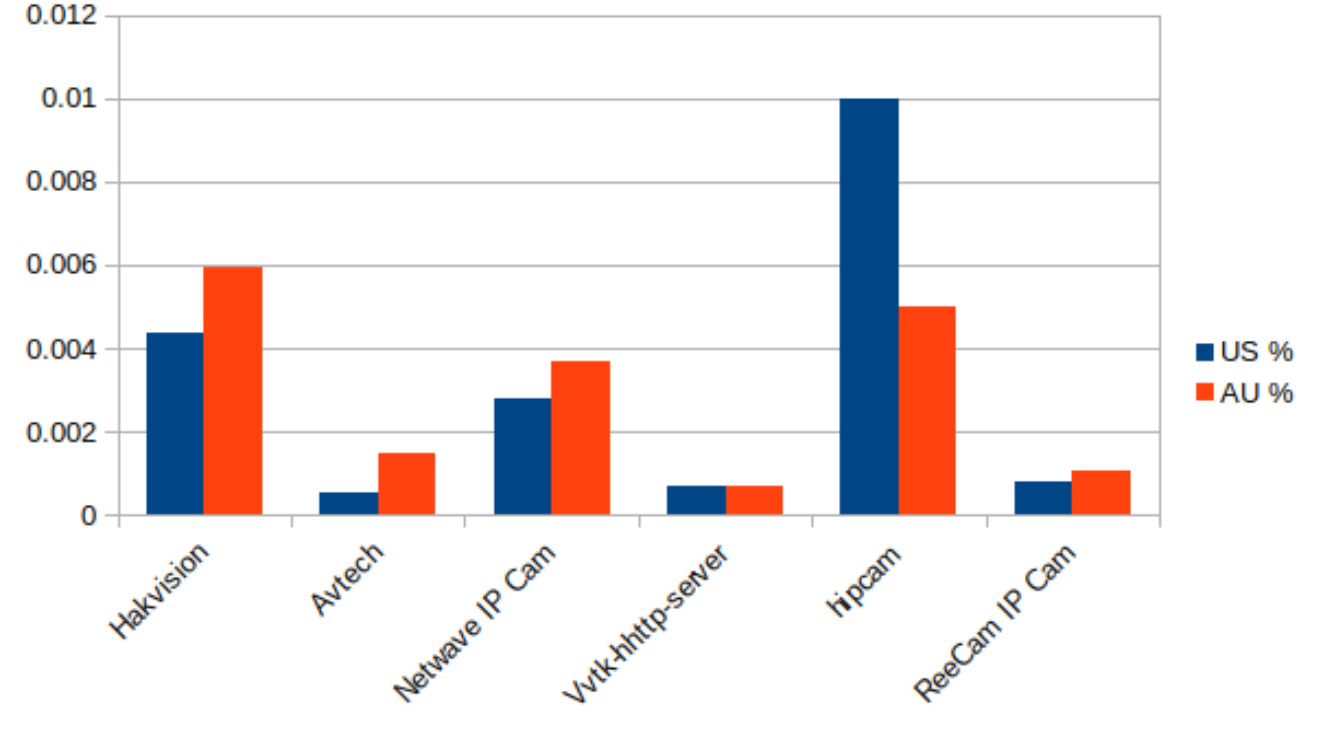
| | | |
|---|---|---|
| IP Cameras | Hikvision | 1453 |
| | Avtech | 361 |
| | Netwave IP Cam | 900 |
| | Vvtk-hhttp-server | 169 |
| | hipcam | 1224 |
| | ReeCam IP Cam | 255 |
| | Total IP Cams | 4362 |

# Routers & Other smart devices in Australia

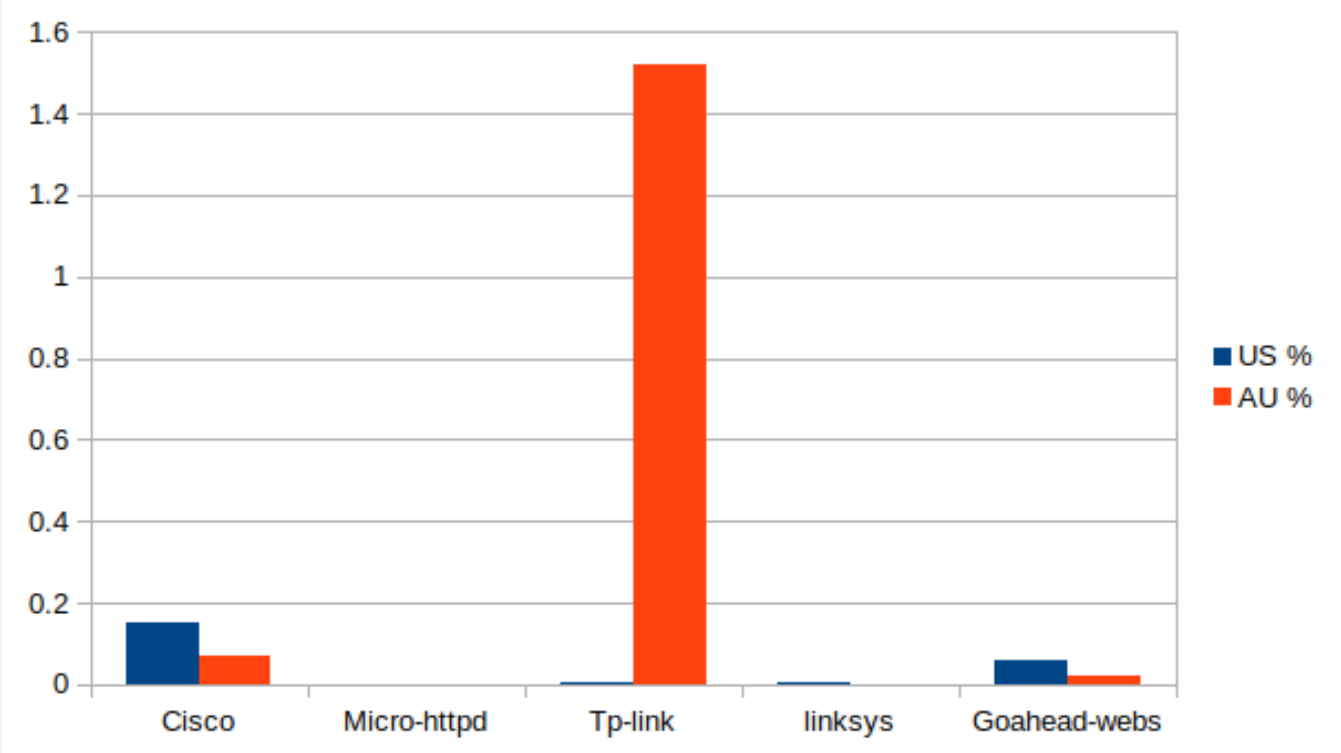
ACSC Australian Cyber Security Centre

| | | |
|---|---|---|
| Routers | Cisco | 17145 |
| | Micro-httpd | 0 |
| | Tp-link | 373117 |
| | linksys | 100 |
| | Goahead-webs | 5753 |
| | Total Routers | 396115 |
| Others | Samsung Smart TV | 0 |
| | Dahua DVR | 6 |
| | Total Others | 6 |

# Comparative Analysis

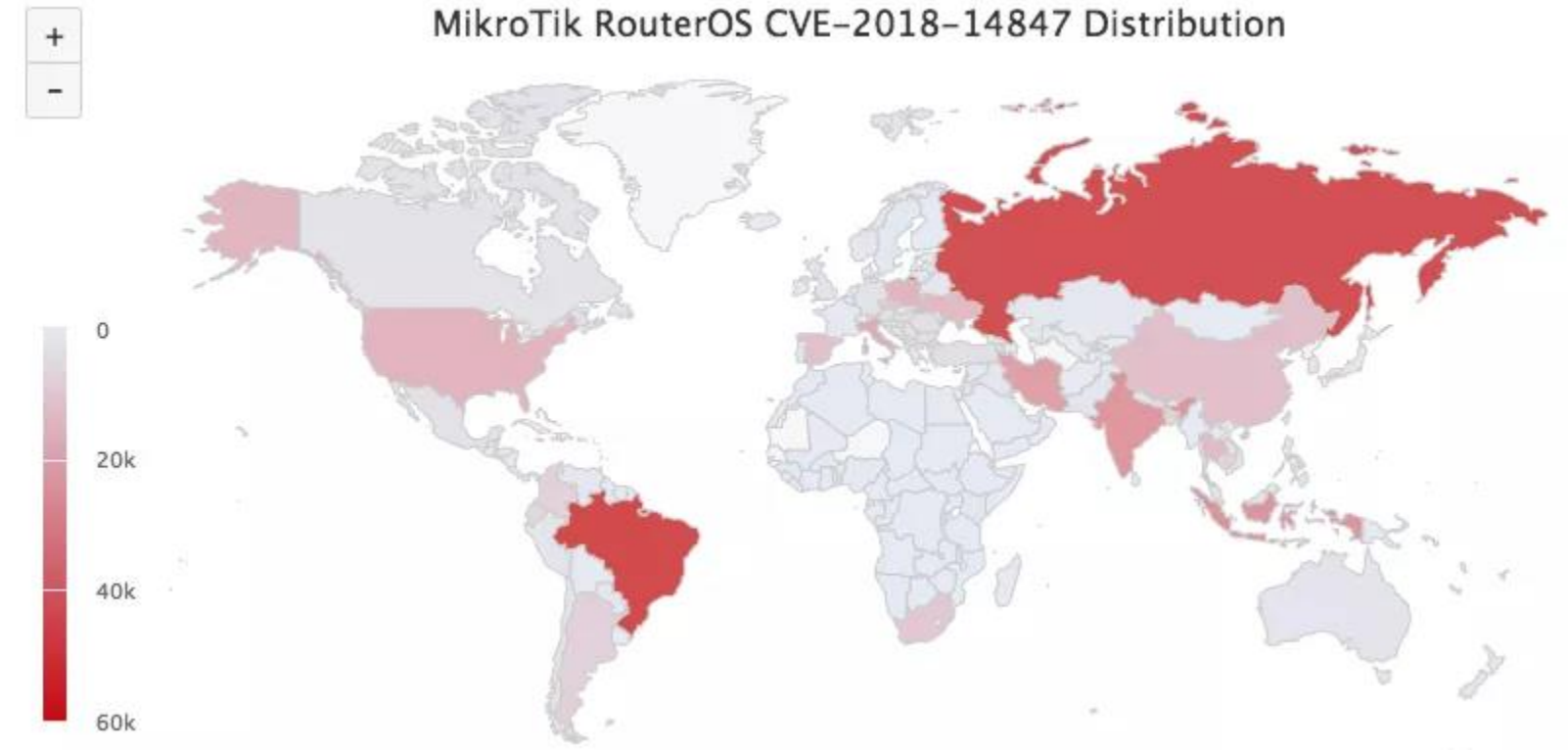


# Comparative Analysis - continued



# What can we do?

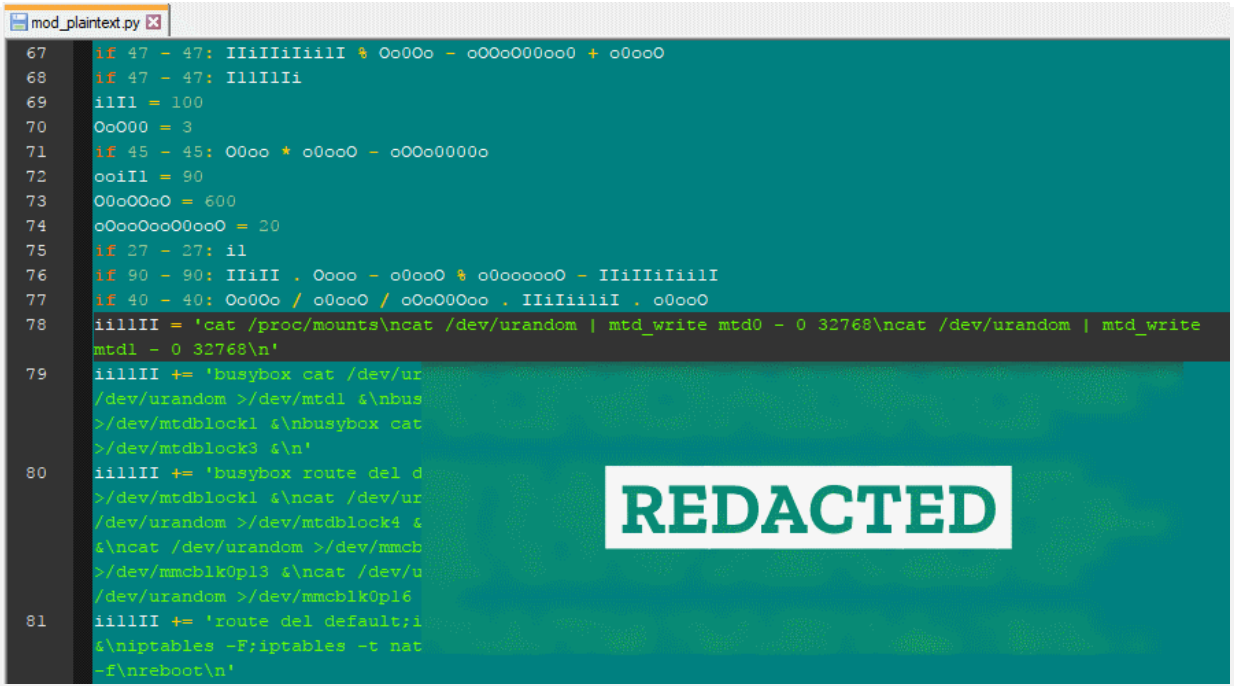
# MikroTik Vigilante - October 2018




https://securityaffairs.co/wordpress/77125/hacking/mikrotik-routers-vigilante.html

# BrickerBot1, 2 & 3 - April 2017

ACSC Australian Cyber Security Centre

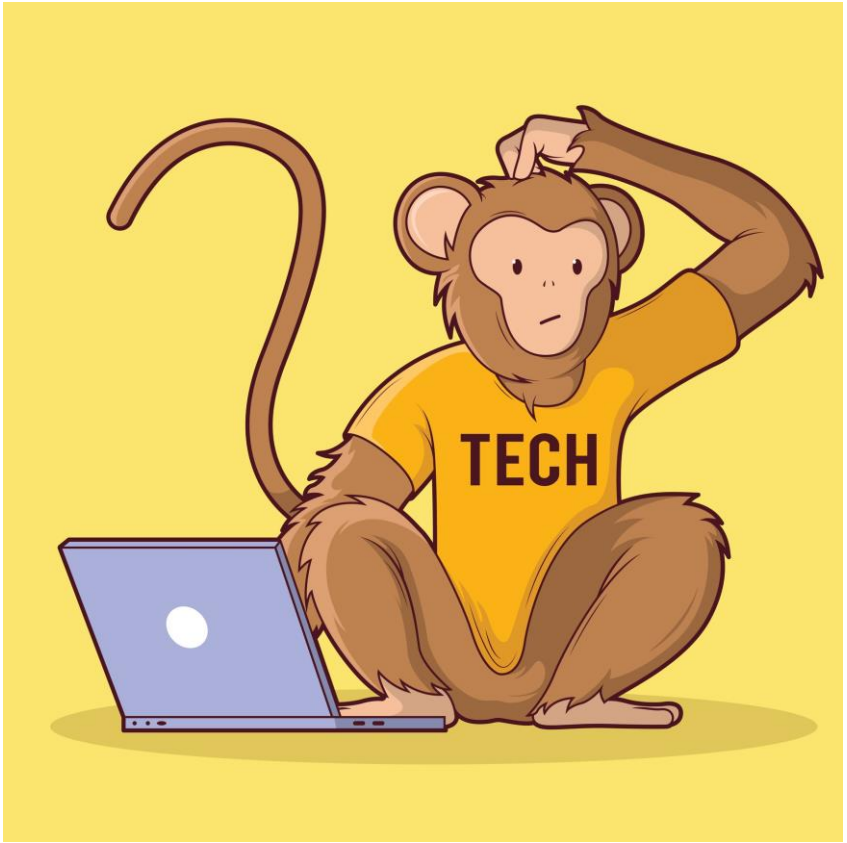



- 10 million IoT devices bricked
- Average user will return bricked device to the vendor
- Net effect of holding vendor accountable and making the Internet safer
- BUT… also ILLEGAL

https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/

# What can we do?

**LEGALLY**



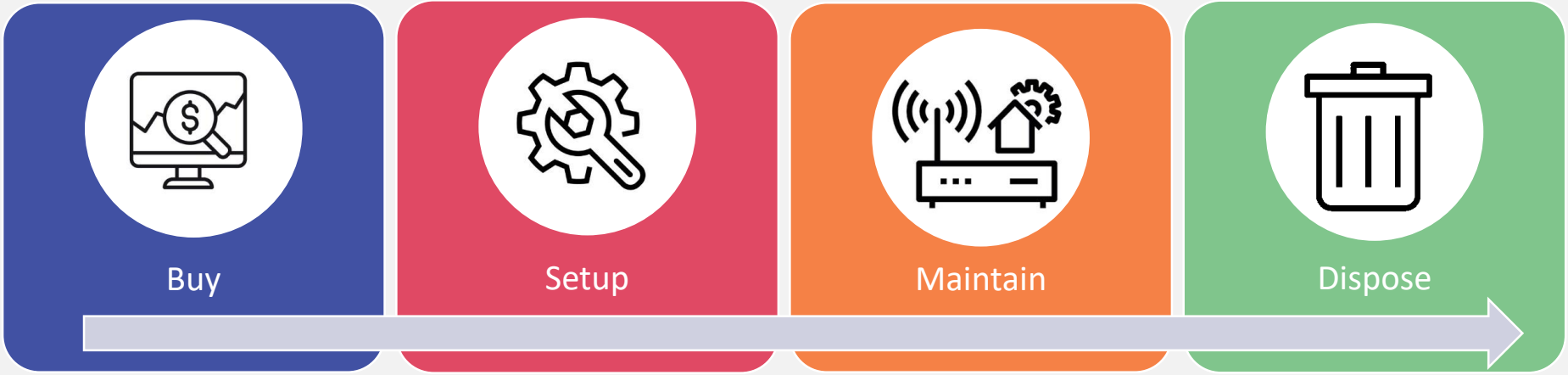
# Inform Consumers

ACSC Australian Cyber Security Centre

- The MikroTik Vigilante and Brickerbot both show that consumers aren’t patching their devices or showing good security hygiene

- Educating consumers is an important step to improve the situation

# Consumer Advice - Overview



# What about vendors? How do we influence them?

# What's being done overseas?

ACSC Australian Cyber Security Centre

- UK: NCSC and DCMS publish 'Secure by Design'.
  - https://www.gov.uk/government/collections/secure-by-design
- US: September 28th 2018, California Senate Bill 327 and Assembly Bill 1906 'Information Privacy: connected devices' signed off. To become law January 1st 2020.
  - SB-327: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
  - AB-1906: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB1906

# What's being done in Australia?

ACSC Australian Cyber Security Centre

- The ACSC and Department of Home Affairs are working together to lift the security of the Internet of Things.
- This involves both technical and policy approaches.
- We will work closely with industry in the coming months to make sure any approach has the right impact.
- We are also working with international partners to make sure Australia's standards align.
- IoTAA – a peak industry body – has been quite active in this space and has also developed some Security Guidelines.

Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security
Centre

# Industrial Control Systems

# Outline

- Intro to Control Systems
- Control System Lab
- Threats & Mitigation

# What is an industrial control system?

ACSC Australian Cyber Security Centre

- Industrial control systems are used to manage the industrial processes required to keep everything running smoothly.

- They’re used in a variety of critical infrastructure such as our water, electricity and gas systems.

# Terminology

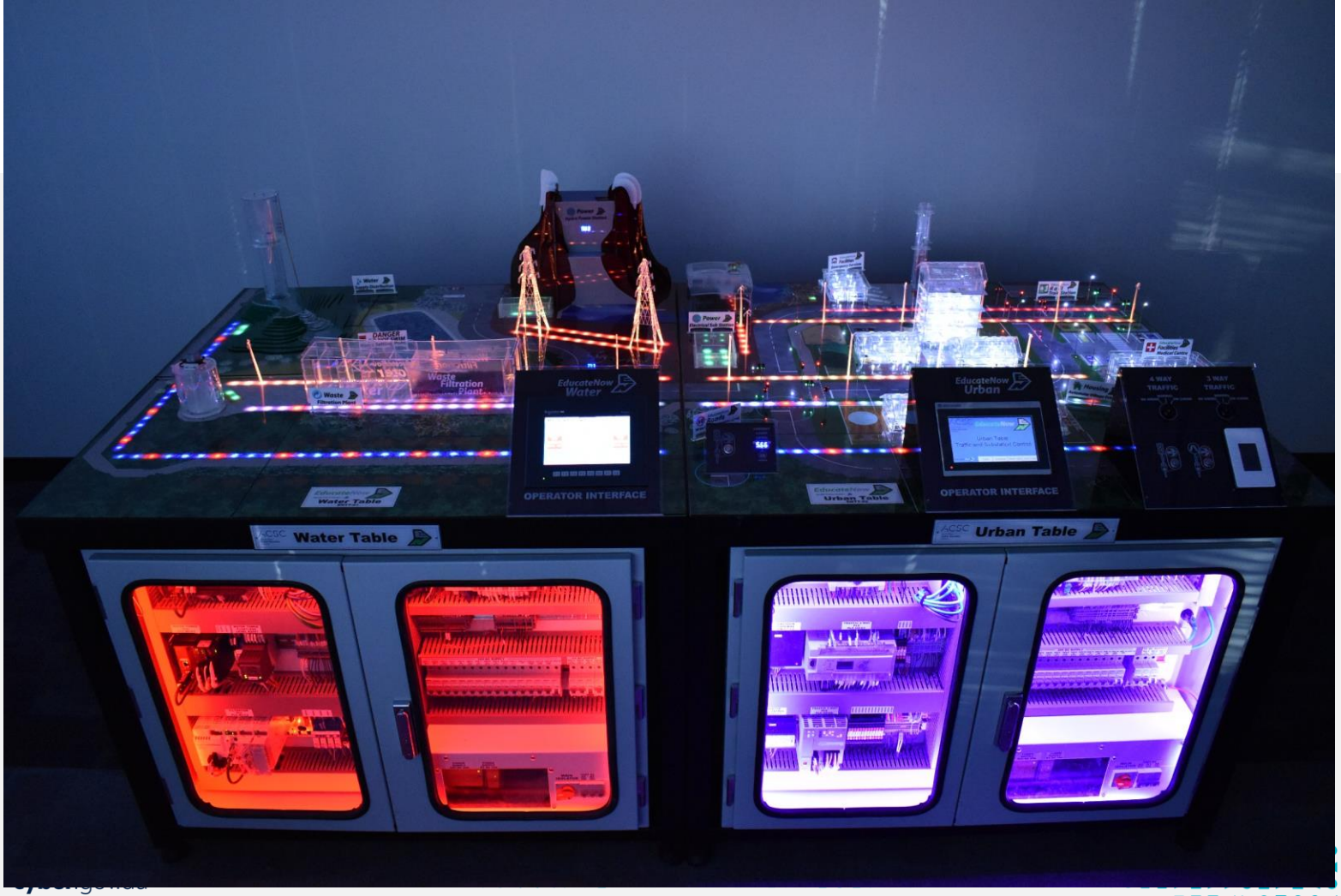
- ICS – Industrial Control System
- PLC – Programmable Logic Controller
- HMI – Human Machine Interface
- SCADA – Supervisory Control and Data Acquisition

# How do Industrial Control Systems work?

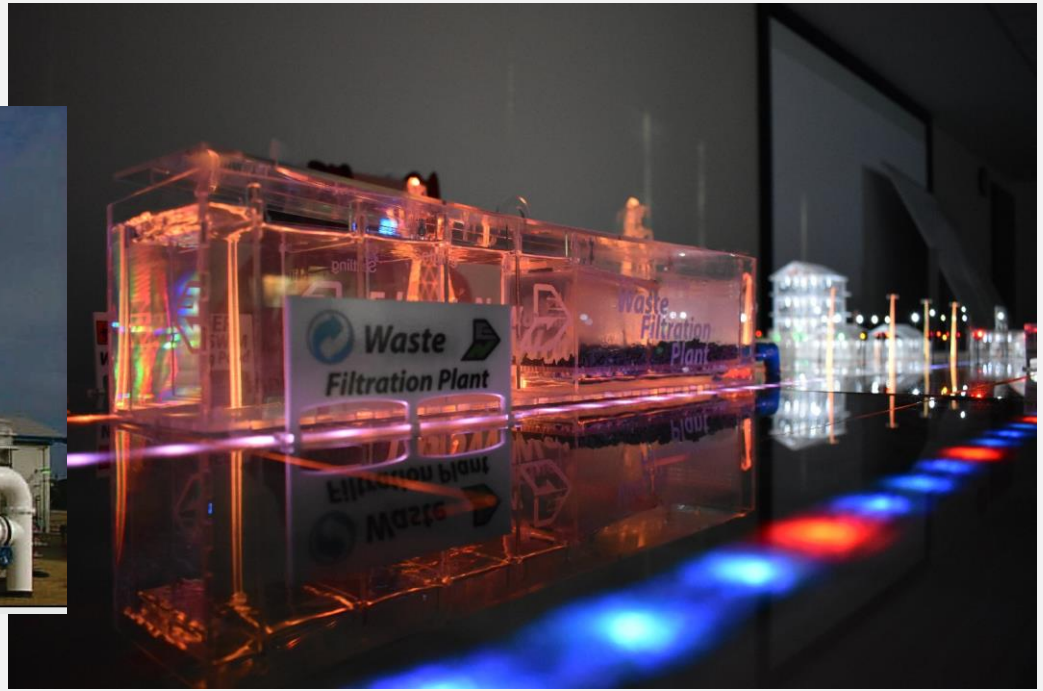
- PLCs are used to control whether things are on or off, and under which circumstances things should be on or off.

- SCADA systems are used to visualise how the ICS is running.

# Control System Lab

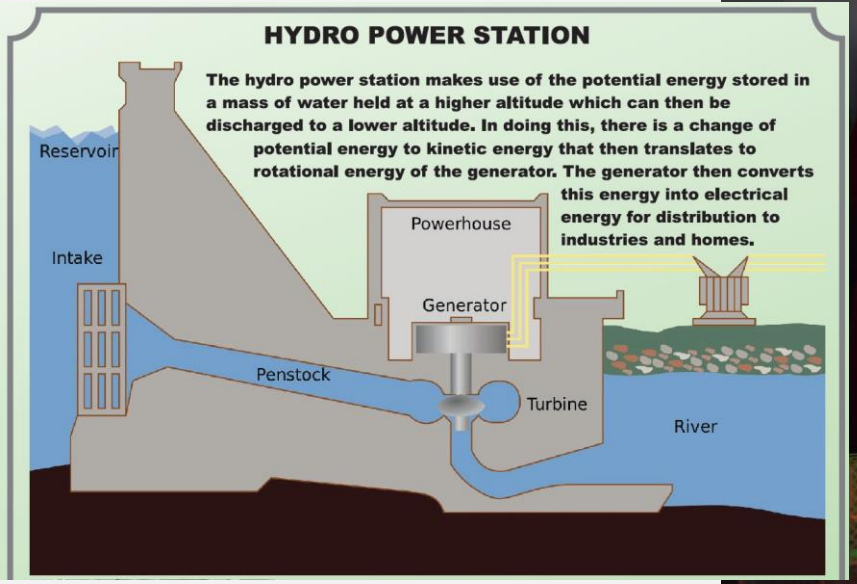

EducateNow Water
OPERATOR INTERFACE
EducateNow Urban
OPERATOR INTERFACE
Water Table
Urban Table

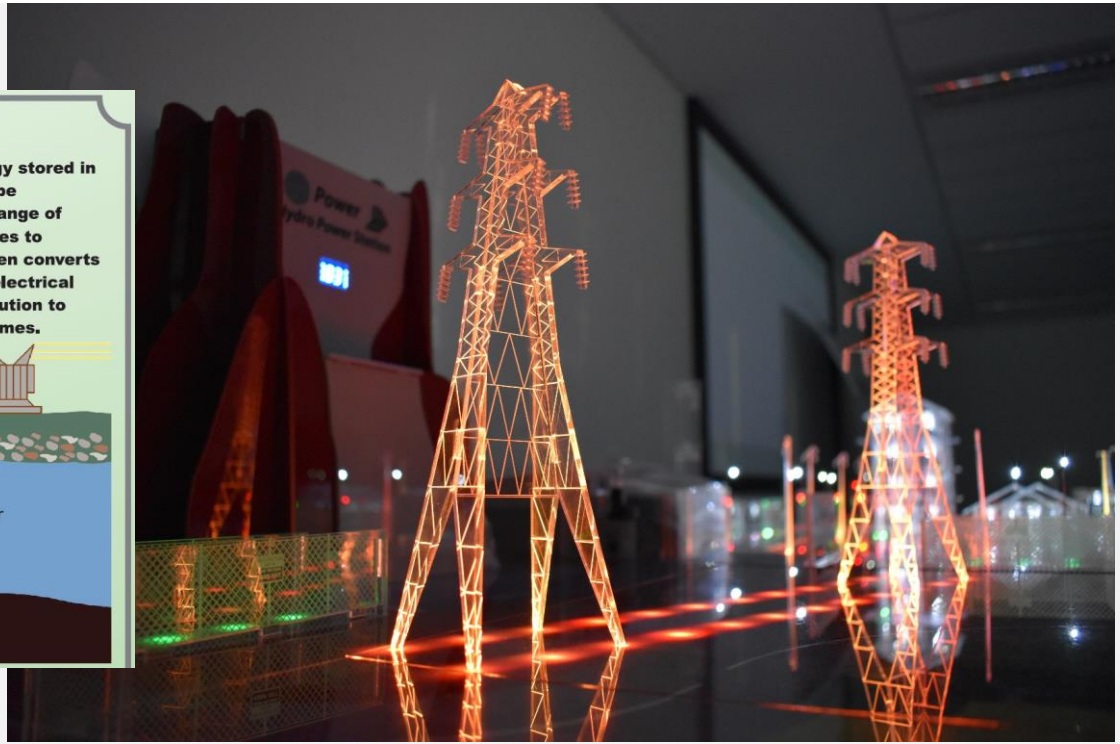
# Water Distribution & Filtration

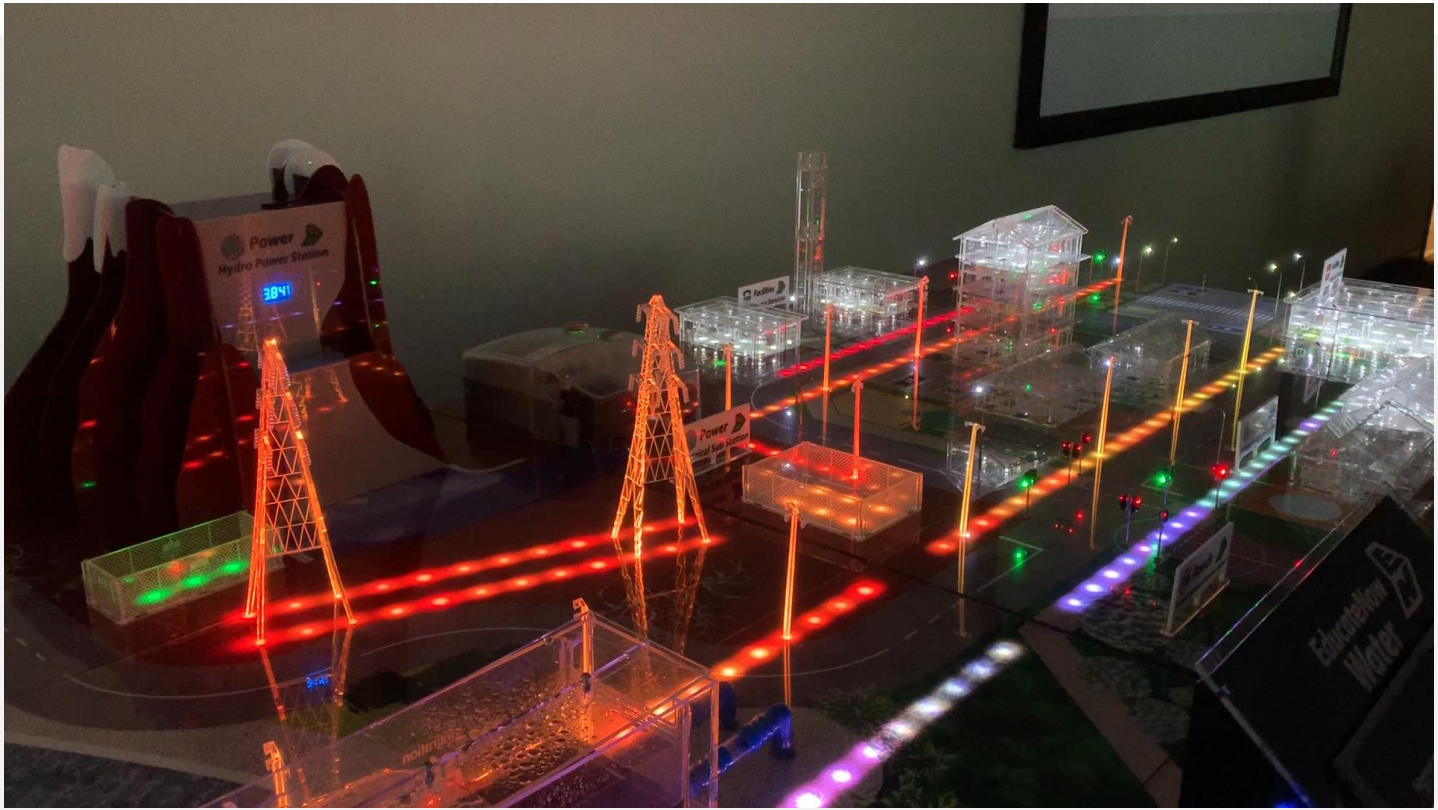
# Attacking the water supply

# Hydro Power Station

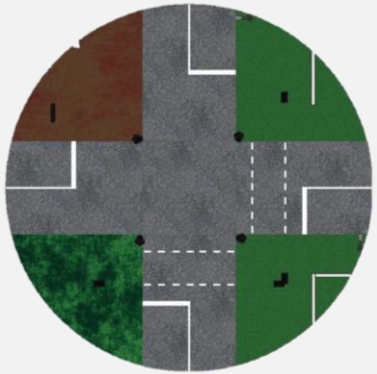


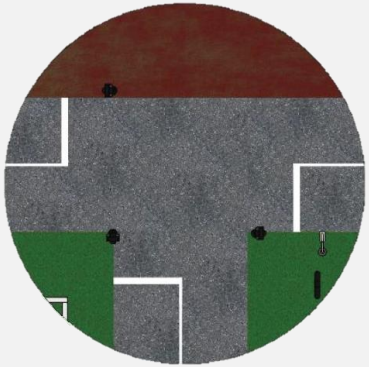



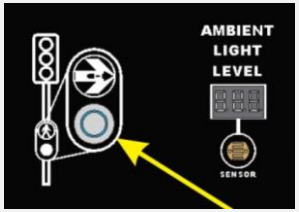
# Attacking the Power Supply



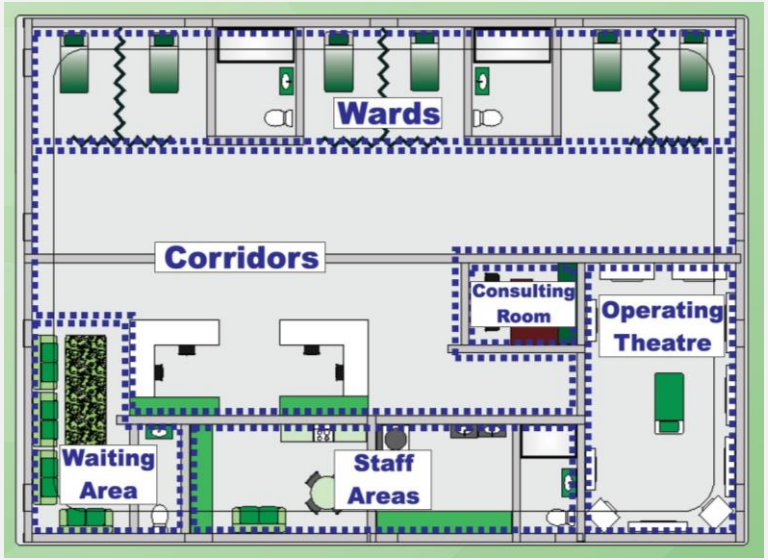
# Intersections & Lights

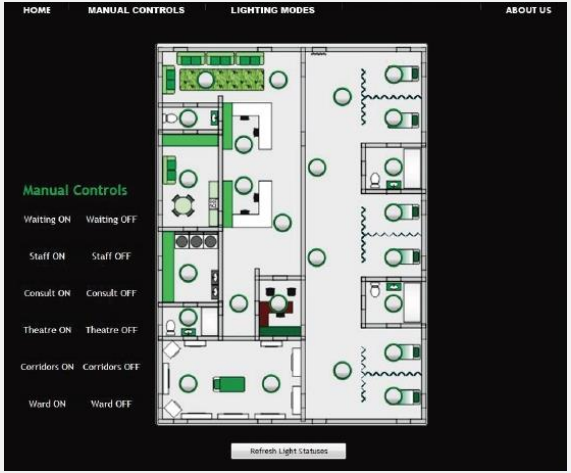






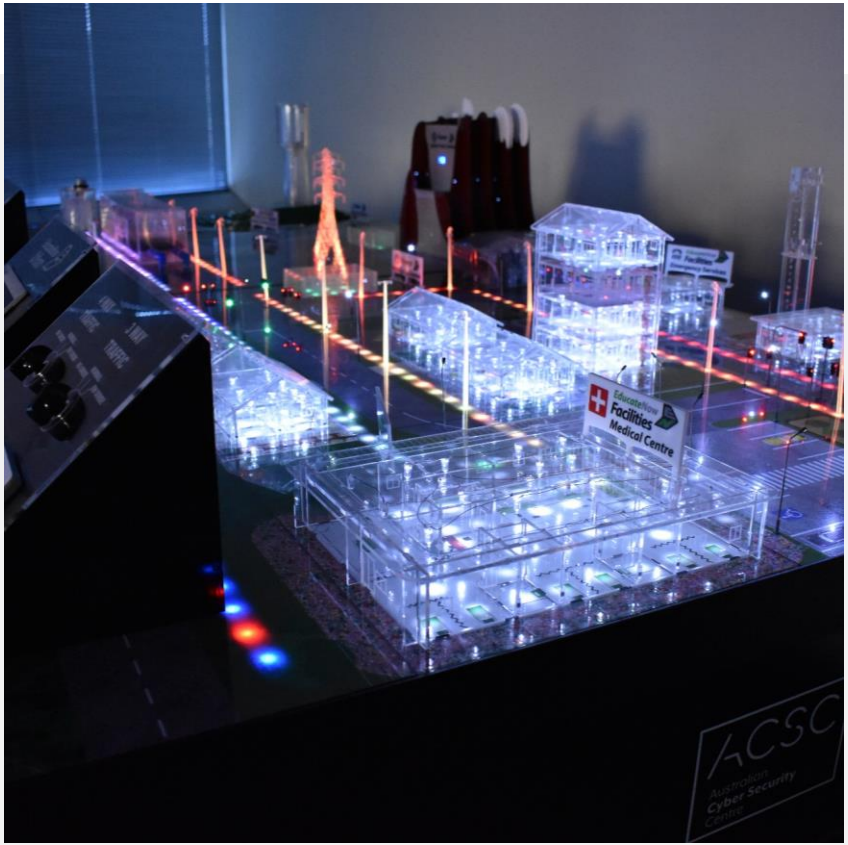

# Medical Facility



# Threats and Mitigations

How do we protect these systems?



# Why does the ACSC care about ICS?

Industrial control systems are essential to our daily life. They control the water we drink, the electricity we rely on and the transport that moves us all. It is critical that cyber threats to industrial control systems are understood and mitigated appropriately to ensure essential services continue to provide for everyone.

# Why is mitigating hard?

ACSC Australian Cyber Security Centre

Providing cyber security for control systems present several unique challenges, including:

- lack of security in engineering protocols
- the need to re-test engineering systems after upgrades
- long life-cycles (20 through to 50 years)
- the addition of many IT protocols, such as network time protocol (NTP) and address resolution protocol (ARP), to the engineering environment
- control environment devices may not be set up to receive or respond to messages from standard IT debugging and analysis tools

# ACSC Essential Control System Mitigations

1. Tightly control or prevent external access to the control system network; segregate it from other networks such as the corporate network and the Internet.
2. Implement two-factor authentication for privileged accounts and access originating from corporate or external networks.
3. Disable unused external ports on control system devices.
4. Visibly mark authorised devices inside the control system environment with organisation-unique anti-tamper stickers.
5. Make regular backups of system configurations and keep them isolated. Test the restoration procedure and validate the backup integrity periodically.

# Essential Control System Mitigations

6. Regularly review firewall settings are in an expected state.
7. Prevent devices inside the control system network from making connections to the corporate network or the Internet.
8. Enable logging on control system devices and store logs in a centralised location. Institute regular monitoring and incident response practices to ensure that anomalies are identified, investigated and managed in a timely fashion.
9. Define a process for introducing external software and patches into the control system. Where necessary (on exceptionally critical components), review code and whitelist approved binaries.
10. Use vendor-supported applications and operating systems, and patch associated security vulnerabilities in a timely manner.

https://www.cyber.gov.au/advice/protecting-control-systems

Australian Government
Australian Signals Directorate

ACSC
Australian
**Cyber Security**
Centre

# Questions?