APCERT 2019
ANNUAL GENERAL MEETING & CONFERENCE

Internet-of-Things Security Landscape

CSA SINGAPORE

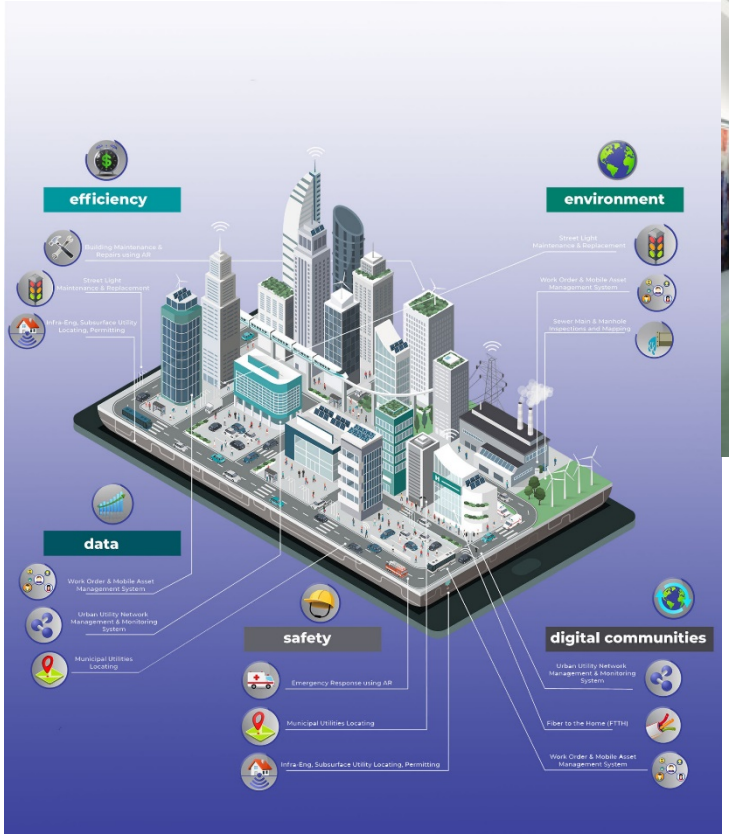
Eddy Ong

Senior Assistant Director

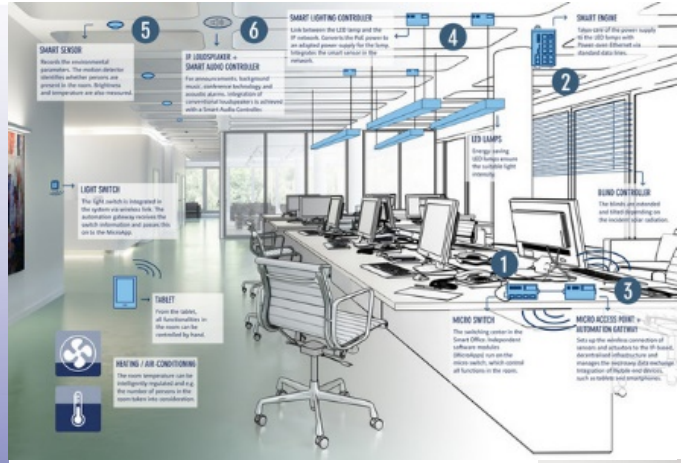
Cybersecurity Engineering Centre

The IoT Security Landscape Study was jointly commissioned by the Cyber Security Agency of Singapore (CSA) and Ministry of Economic Affairs & Climate Policy (MEAC) of the Netherlands, under the ambit of MOU with the National Cyber Security Centre of the Netherlands (NCSC-NL).

IoT enabling Digitalization in various areas

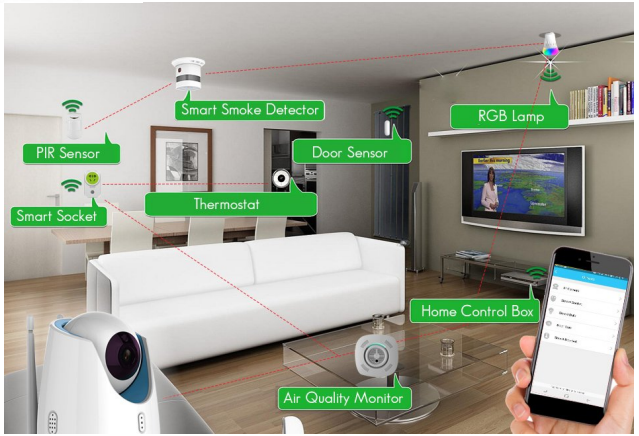


Smart City Sensors Infra



Smart Office

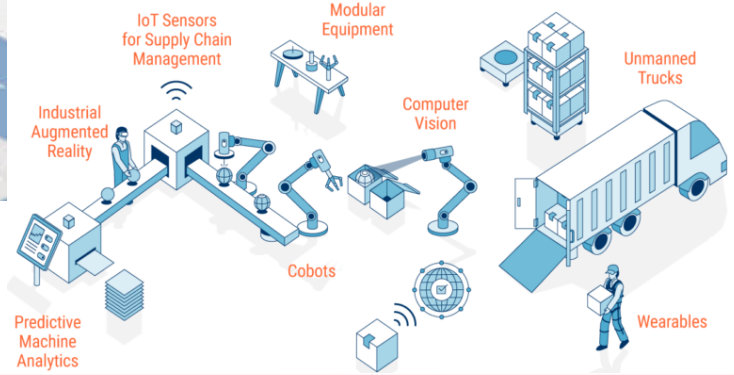
Smart Home



IoT enabling Digitalization in various areas

Smart Mobility

Smart Hospital



Smart Factory

Smart Nation SINGAPORE
Many Smart Ideas • One Smart Nation

Singapore's Smart Nation Journey

CSA SINGAPORE

Building a SMART CITY

A slew of initiatives are taking place islandwide, the goal of which is to sharpen the Government's response to city issues and hence improve people's day-to-day lives.

TOWN PLANNING
What: A modelling system to simulate a city's built environment and its impact on the natural environment, people, resources and costs
Who: HDB, Electricite de France, Veolia
Uses: Among other things, show how different land uses affect amenities and transport networks; how to design new housing blocks to get ideal wind flow; where best to build cycling paths
Status: Research collaboration / prototype stage

WATER QUALITY AND LEAKS
What: A network of wireless sensors that monitors water quality and detects leaks in real time
Who: PUB, Singapore-MIT Alliance for Research and Technology, Visenti
Uses: Allows PUB to repair leaks faster and reduce water loss
Status: About 300 sensors installed by end-2015

3D MAPPING
What: Mapping the country in 3D from the air by using light planes equipped with lasers and cameras
Who: Singapore Land Authority
Uses: PUB could use the map to model flood patterns, while the Civil Aviation Authority of Singapore could plan more efficient landing paths for planes
Status: Expected to be completed by 2016

DISEASE AND HYGIENE
What: Computer models that use sensors and mobile apps to help detect and forestall dengue and food poisoning outbreaks
Who: National Environment Agency (NEA), IBM
Uses: For example, if people complain on Facebook or Twitter of being sick after eating at a particular restaurant, the system would alert NEA officers
Status: Research collaboration

IMPROVING PUBLIC TRANSPORT
What: Analysing CCTV video feeds and anonymised location-based data from mobile subscribers to learn commuters' travel patterns
Who: Land Transport Authority, SMRT, StarHub, IBM
Uses: Help agencies respond better to unplanned incidents on the train and bus network, such as breakdowns or emergencies
Status: Research collaboration

NOTE: Artist's impression

GRAPHICS: MIKE M DIZON and DAVID EE

ERP II
What: A satellite-based electronic road pricing (ERP) system that can use an on-board monitor to charge motorists according to distance travelled
Who: Land Transport Authority, IBM
Uses: This may replace the current system, which charges motorists each time they pass through an ERP gantry during certain times
Status: Feasibility being studied

SECURITY
What: A public-private Safe City Test Bed that produced, for example, a mobile app for commanders to track security forces in real time
Who: Economic Development Board, Ministry of Home Affairs, AGT International, Airbus Defence and Space, NCS, NEC Asia Pacific
Uses: Could help commanders respond to incidents more quickly and precisely
Status: Test bed completed

JURONG LAKE DISTRICT – 'SMART CITY'
What: A government vision for the area to use smart technologies such as driverless cars to improve liveability for residents
Who: Singapore Government, various partners
Uses: For now, driverless cars will ply the Chinese and Japanese Gardens later this year. Expected to be used at Jurong East MRT next year
Status: Ongoing

PROTECTING THE SEA
What: Eight buoys along coastline with sensors that test waters for pollutants and send real-time updates wirelessly to the NEA
Who: National Environment Agency (NEA)
Uses: Early detection of oil or chemical spills
Status: In place

Smart Singapore

Singapore is expanding its use of technology to entrench its position as a leading global city and improve Singaporeans' quality of life. Here are some upcoming initiatives:

Punggol pilot: The first "smart" housing project will be launched in Punggol next year, and will include energy-efficient measures like motion sensor lights in carparks.

One ring to pay them all: An embedded chip could turn a ring, a watch or your identity card into a payment device, eliminating the need for cash or credit cards.

Remember me: A new digital platform is being developed to bypass the need for citizens to provide their personal data repeatedly for government transactions.

Mapping the future: A new 3D map project called Virtual Singapore will integrate layers of data about Singapore's buildings, land and environment. Government agencies and other organisations can use it to solve problems such as identifying the most flood-prone areas, while the public can contribute information like traffic patterns or the locations of their favourite nasi lemak stores.

Phone home: Controlling household appliances from a smart phone may be possible once HDB determines the digital infrastructure needed for an automated home. Trials start next year.

Where's my bus: By next March, commuters can use the MyTransport app to find out bus arrival times by the minute and how crowded each bus is.

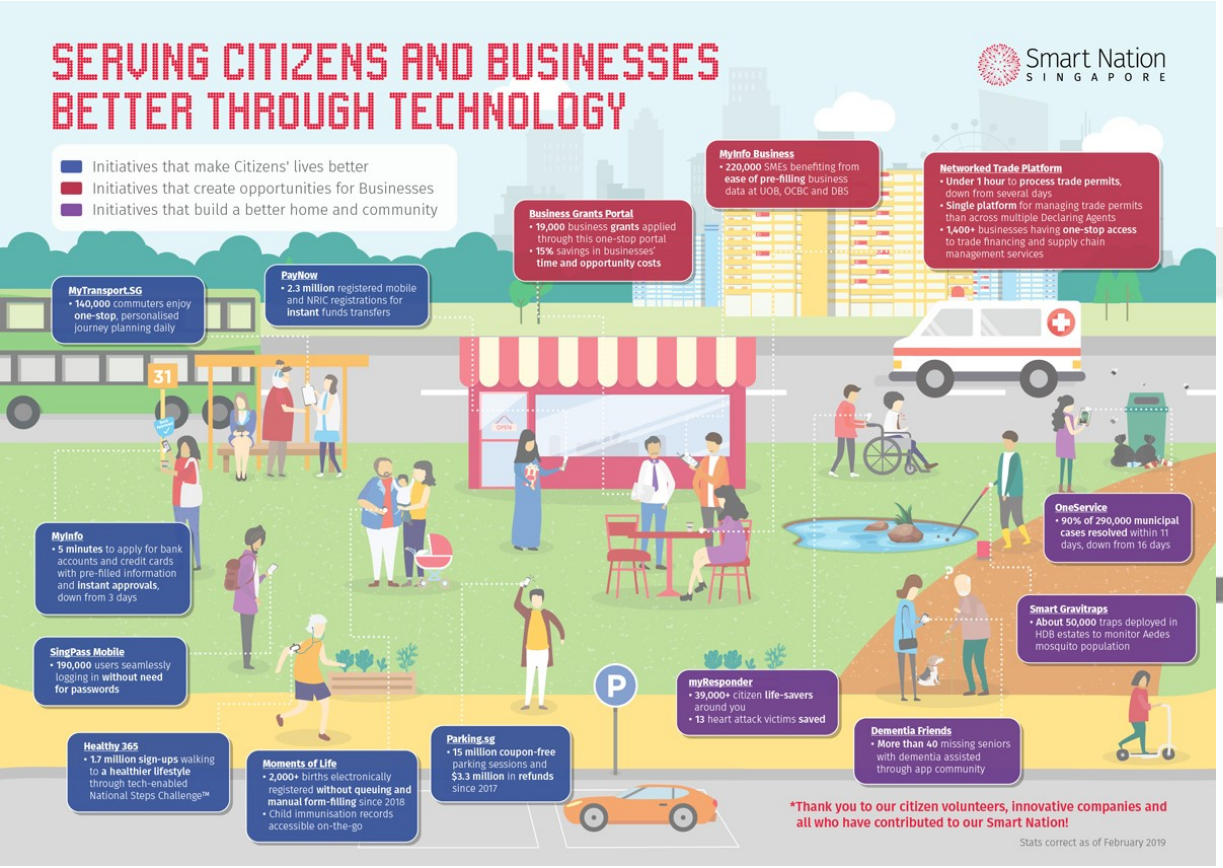
Senior sensors: Sensors in the homes of the elderly will monitor their movements and send alerts to caregivers if irregular behaviour is detected.

Virtual therapy: A "tele-rehab" system being tested at community hospitals will allow patients to perform therapy exercises at home, while sensors attached to their limbs transmit data back to the hospitals.

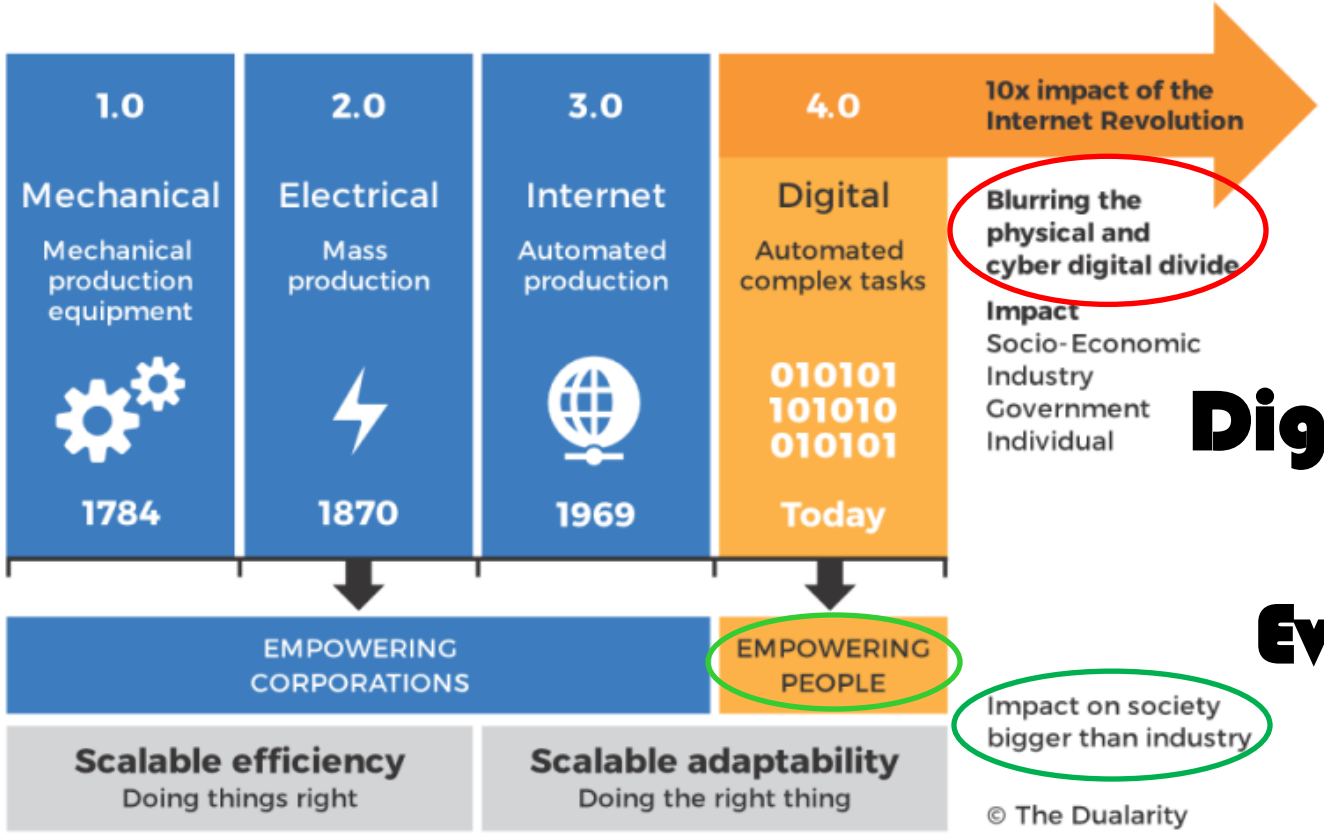
"Public" transport: Self-driving cars will be tested on public roads for the first time come January next year, in One-North at Buona Vista.

GRAPHICS: MIKE M DIZON AND CHING CHOON HIONG TEXT: RACHEL AU-YONG

Singapore's Smart Nation Journey

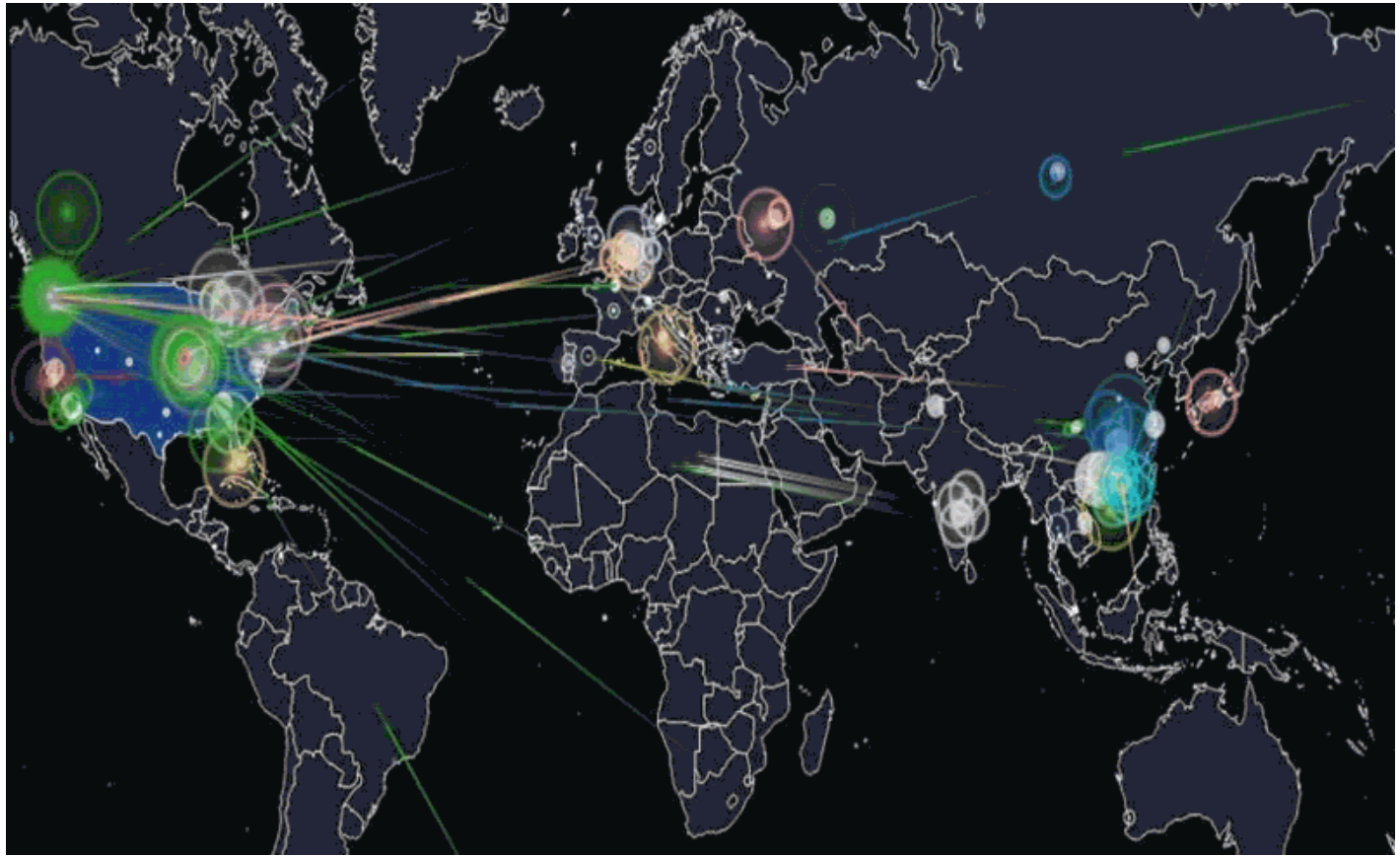


Welcome to the Industrial Revolution 4.0



Digitalisation of Everything

IoT Threat – as Massive Botnet for DDOS



Mirai IoT botnet DDOSed Dyn DNS & nearly crippled internet access for most US users & major US websites used by rest of the world - e.g. Twitter, Spotify, Reddit, etc

Delivered shocking **1.2Tbps** - *big leap from biggest DDOS not on IoT botnet !*

IoT Threat – as Entry Vector to Enterprise

Microsoft: Russian state hackers are using IoT devices to breach enterprise networks

Microsoft said it detected Strontium (APT28) targeting VoIP phones, printers and video decoders.

In multiple cases, Microsoft saw Fancy Bear get access to targeted networks because the IoT devices were deployed with default passwords. In another case, the latest security update was not applied. Using those devices as a starting point, the hackers established a beachhead and looked for further access.

Microsoft has said a high-profile Russian state-sponsored hacking group is actively attacking businesses through internet of things (IoT) devices.

The Redmond-based tech giant attributed the
called STRONTIUM, also known as APT28 or F
behind the cyber attack on the 2018 Winter C

Target attack shows danger of remotely accessible HVAC systems

Qualys says about 55,000 Internet-connected heating systems, including one at the Sochi Olympic arena, lack adequate security

IoT Threat – impacting Cyber-Physical divide

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

Researchers hack Philips Hue lights via a drone; IoT worm could cause city blackout

Researchers hijack Philips Hue lights with a drone to show how IoT worm could take over smart lights in a city.

IoT Threat – Compromising Privacy

FBI Warns Parents of Privacy Risks With Internet-Connected Toys

Many of these smart toys have a combination of sensors, cameras, microphones, data storage or other components, such as voice recognition and GPS, the warning said.

"These features could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed," the FBI said.

Strangers can talk to your child through 'connected' toys, investigation finds

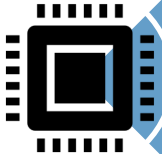
Hackers Found a (Not-So-Easy) Way to Make the Amazon Echo a Spy Bug

Researchers found they could turn the smart speakers into surveillance devices—if they could get their own attack tool on the same Wi-Fi.

IoT Threats – Summary

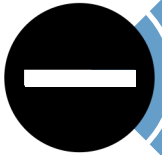
Vulnerable Device Software

- Buffer overflows, lack of authentication



Firmware-Level Attack

- Replacement of firmware during commissioning or routine upgrade



Denial of Service

- Devices can be DoSed due to limited resources
- Device botnets can launch distributed DoS attacks

Privacy Threat

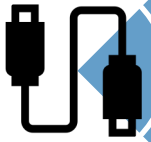
- Due to device location tracking or personal information collection

Device Cloning or Substitution

- Cloned devices can be sold cheaply and include backdoors

Weak Credentials

- Poor password choices and lack of 2FA for user and admin interfaces of devices, gateways or back-ends



Eavesdropping

- Including network attacks such as man-in-the-middle and message replay

Data Leakage

- Confidential data may be captured from devices or from the back-end

Malware

- Devices can be infected with software designed to perform unauthorized actions

The IoT Security Landscape Study was jointly commissioned by the Cyber Security Agency of Singapore (CSA) and Ministry of Economic Affairs & Climate Policy (MEAC) of the Netherlands, under the ambit of MOU with the National Cyber Security Centre of the Netherlands (NCSC-NL).

IoT Security Challenges

Principles, Governance and Legislation

- Cybersecurity and Privacy by Design
- IoT Security Standards and Guidelines
- Evaluation and Certification
- Future-Proof Legislation

Ecosystem Development

- Responsible Industry
- Supply Chain Security
- Product Life Cycle Support

Technical References and Standards

- Device Identities and Root of Trust
- Secure OS, Cloud and Applications
- Secure Communications and Infrastructure
- Security Monitoring and Analytics

Evaluation and Certification

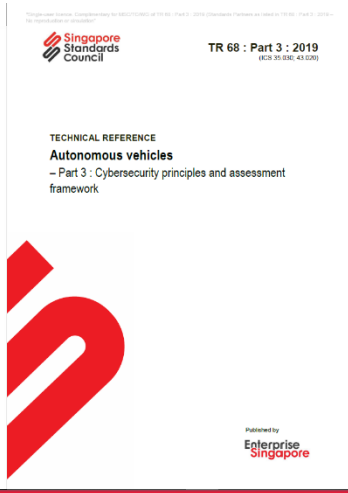
Key Findings

- **C**ommonality – No commonly agreed evaluation criteria
- **C**ertification regime – Demanding in time and resources/costs
- **C**ollaboration – Nascent and yet to be mutually recognised widely

Possible Approaches

- Harmonise & Adapt existing certification regime for IoT
- Innovate a Lite-version evaluation scheme for IoT
- Garner support towards mutual recognition

Evaluation and Certification



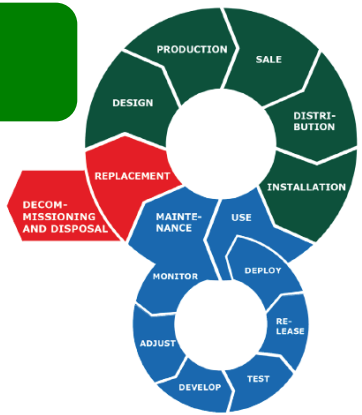
Responsible Industry

Key Findings

- Immature ecosystem – IoT industry still evolving & rapid innovation
- Incentive – Little incentive to implement security vs time-to-market, nor to provide continuing product life-cycle security maintenance
- Inadequate pressure – on industry to foster responsible behaviour

Possible Approaches

- Responsible industry via demand-driven and/or liability-legislation
- Product security assurance regime through evaluation scheme
- Continuing life-cycle support to provide patches for vulnerabilities



Responsible Industry

EU Cybersecurity Act

- In December 2018, the EU passed the Cybersecurity Act to reinforce ENISA's mandate to support Member States in tackling cybersecurity threats.
- The Act also establishes an EU framework for cybersecurity certification.
  - Certification is voluntary unless future EU legislation makes it mandatory.
  - This Act is not specific to IoT security, although it does cover IoT products.

California Senate Bill 327

- Due to take effect in January 2020, this law requires all "connected devices" to have a "reasonable security feature."
- Security experts point out that the law is well-intentioned and while it may not actually solve the problems that plague IoT security, it is nevertheless a good start.

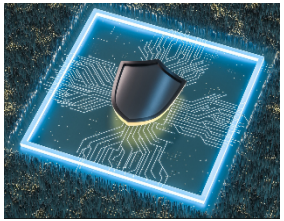
Device Identities and Root of Trust

Key Findings

- **U**nique identity – Poor asset visibility nor traceable authentication
- **U**ntrusted security – Lack trust anchor & chain of trust for security
- **U**biquitous usable – even for low-cost or resource-constrained IoT

Possible Approaches

- Targeted measures to address IoT's resource-constrained limitation
- Trust Anchor & chain of trust specially to support IoT use-cases
- PUF can help alleviate need for Key-mgt on massive numbers of IoT



Device Identities and Root of Trust

IoT Security Challenges

Principles, Governance and Legislation

- Cybersecurity and Privacy by Design
- IoT Security Standards and Guidelines
- Evaluation and Certification
- Future-Proof Legislation

Ecosystem Development

- Responsible Industry
- Supply Chain Security
- Product Life Cycle Support

Technical References and Standards

- Device Identities and Root of Trust
- Secure OS, Cloud and Applications
- Secure Communications and Infrastructure
- Security Monitoring and Analytics

IoT Security Landscape Study – Conclusion

- IoT Security Landscape Study is a good starting point of identified challenges and possible approaches for action
- Create an ecosystem that is secure, from design to disposal, a challenge that requires global approach
- Foster strong international collaboration amongst countries at the government, industry and academia ("*triple-helix*") thru International IoT Security Roundtable, &/or other international platforms like GFCE
- Prioritise 3 focus areas to tackle for the initial phase :
  - Evaluation and Certification
  - Responsible Industry
  - Device Identities and Root of Trust

Thank You