

The Public Safety Communications Ecosystem in Australia

PSCE Conference - Lancaster UK

6 June 2019

Geoff Spring
ARCIA Project - Research Officer

Australian Radio Communications Industry Association

What ARCIA does for the radio industry



An Industry Association working on behalf of its membership to provide:

- Networking, information sharing and support
- Partnerships, linkages and accreditation
- Raising awareness and understanding
 - Education and Training

www.arcia.org.au

ARCIA has a MOU with PSCE <https://www.psc-europe.eu/>

ARCIA has a MOU with GWTC (USA) <https://gwtca.org/>

ARCIA has international affiliations with:

- FirstNet (USA) <https://www.firstnet.gov/>
- Federation of Communications Services – UK <http://www.fcs.org.uk/>
- Radio Frequency Users Association (RFUANZ) – New Zealand
<https://rfuanz.org.nz/>

ARCIA collaborates with the
University of Melbourne Centre for
Disaster Management and Public Safety

https://unimelb.edu.au/cdmeps/home?referrer=301_redirect

**How does ARCIA
continue to build it's
relationship with PSCE?**

Mission Critical Public Safety Communications Ecosystem

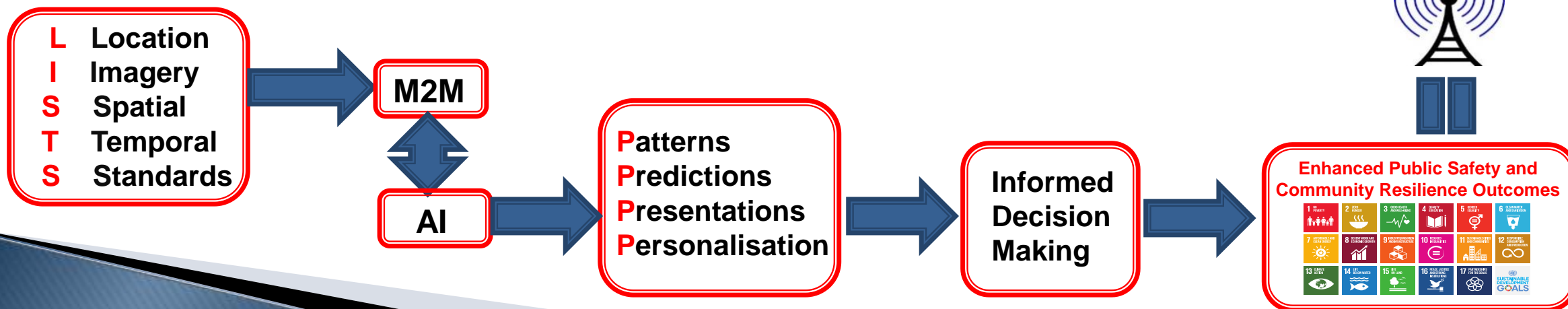
How Does It All Fit? – What's the emerging picture?

What's Trending

- Cyber Security (Public Expectations)
- Critical Control Rooms
- Public Safety Mobile Broadband (PSMB)
- LMR - LTE Interworking – 3GPP Standards
- Internet of (Public Safety) Things
- Mapping
- **Electric** Vehicles - Connected – Autonomous Vehicles and Infrastructure
- Blockchain
- **Ethics**

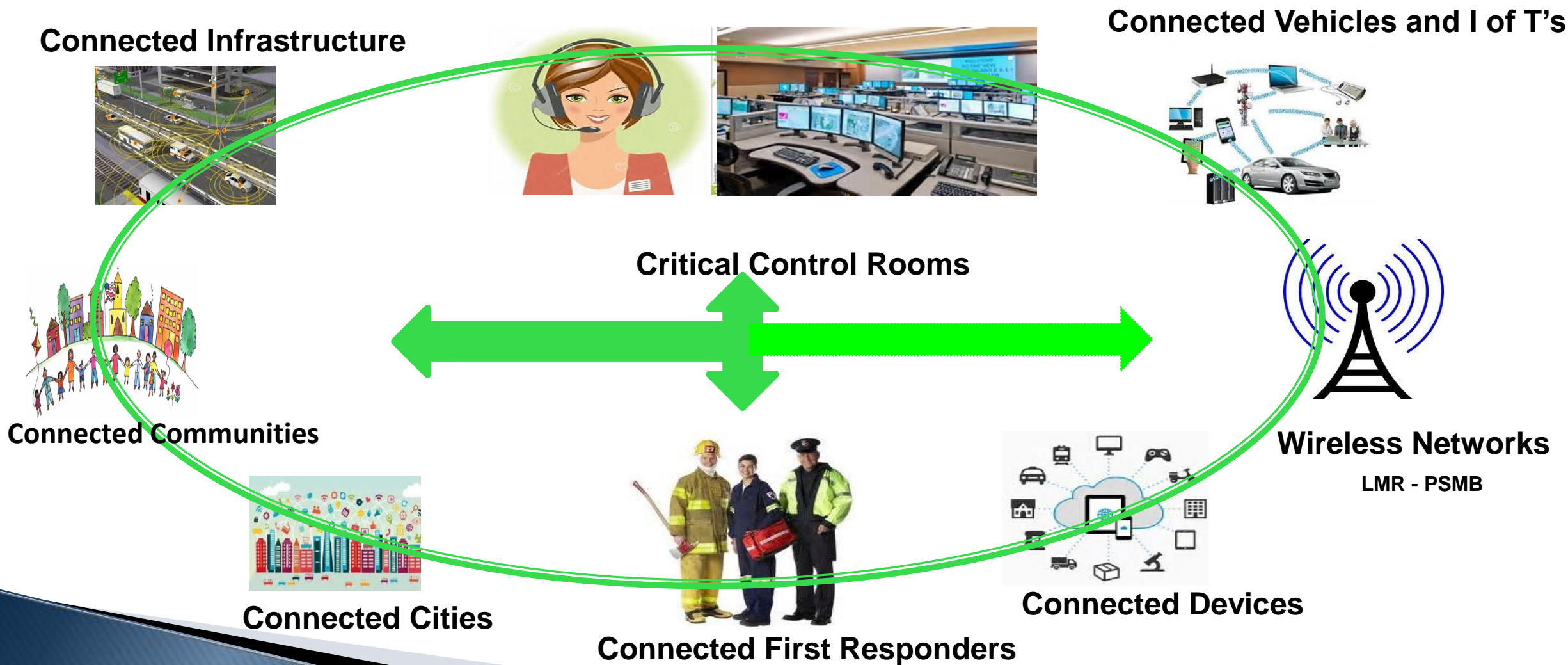
Strategic Policy Issues

- Public Safety Mobile Broadband
- Critical Infrastructure Framework
- **National Security** *will start in Australian homes, streets and communities through the use of technologies that provide global 24/7 connectivity.*
- Australia's Cyber Security Posture
- **National Public Safety Communications Ecosystem**
- Information Sharing
- Dispatchable Address
- Culture Change



Mission Critical Public Safety Communications Ecosystem

The need to raise awareness and education of key decision makers



Mission Critical Public Safety Communications Ecosystem

Next Generation Emergency Management Info-structure

The need to raise awareness and education of key decision makers



Mission Critical Public Safety Communications Ecosystem

USA Department of Homeland Security

The Cybersecurity and Infrastructure Security Agency (CISA)



USA National Emergency Communications Plan (NECP)

CISA will focus on implementing six goals that build on updates to the 2008 and 2014 plans.

- Developing and maintaining effective emergency communications governance and leadership across the **ecosystem**
- Developing and updating comprehensive emergency communications plans and procedures that address the evolution of risks, capabilities, and technologies across the **ecosystem**
- Developing and delivering training, exercise, and evaluation programs that target gaps in all available emergency communications technologies
- Improving effective coordination of available operable and interoperable public safety communications capabilities for incidents and planned events
- Improving lifecycle management of the systems and equipment that enable emergency responders and public safety officials to share information efficiently and securely
- Strengthening the cybersecurity posture of the Emergency Communications **ecosystem**.

Proposed updates reflect the expanding **ecosystem** of people, technologies, and functions involved in supporting emergency communications to aid public safety entities with addressing today's challenges while also planning for future advancements,"

The NECP includes traditional emergency responder disciplines including law enforcement, fire departments, emergency medical services, and dispatch. **Among other more non-traditional entities include medical facilities, utilities, nongovernmental organizations, media, and private citizens.**



Mission Critical Public Safety Communications Ecosystem

The need to raise awareness and education of key decision makers



Australia's Public Safety Communications Ecosystem

- Australian citizens and their use of communication devices
- The Emergency Call Person (ECP) the Triple Zero (000) service
- Public Safety Agency Answering Points (Control Rooms)
- Public Safety Mission Critical Land Mobile Radio (LMR) Networks
- Public Safety Mission Critical Long Term Evolution (LTE) Networks (under development)
- Interfaces between each of these components that provide interoperability capability and capacity to transfer data between these components.

Policy and Strategy

- The need to recognise the existence and importance of Australia's Public Safety Communications Ecosystem
- The need to recognise Government and Department Discussion Papers are independently addressing matters that will impact and/or influence the policy, strategic and regulatory settings associated with the evolution of the ecosystem
- The need to continue to raise the profile, understanding and awareness of the ecosystem in the public safety market and amongst its key stakeholders.

Outcomes being sought:

- The mission critical public safety communications ecosystem needs to be recognised as **Critical Infrastructure** by Australian Government(s)
- Spectrum allocation across the ecosystem needs to be based upon the needs of Australia's PSAs and take into account both current and emerging technologies used in conjunction with global open standards
- The policy decision to apply Highest Value Use or Opportunity Cost Pricing to spectrum allocation in the ecosystem should be revisited to ensure outcomes are related to the *economic, social and national security* issues that need to be addressed to improve the lives and *ensure the safety of all Australians*.

Mission Critical Public Safety Communications Ecosystem

New Cyber Security Legislation - The Cyber Security Posture of the Australian Economy(*)



Three new regulatory forces:

1. Notifiable Data Breach – Security that supports peoples' data (Parallels European GDPR)

- Came into operation in February 2018
- Encourage organisations to understand the personally identifiable information they have
- Understand the impact that unauthorised disclosure of this information could have on people
- Make informed decisions about how to protect this data

2. The Security of Infrastructure Bill – Technology that supports peoples' lives

- Came into operation in September 2018
- Identifies “critical infrastructure” organisations – electricity, water, gas, ports and telecommunications
- Requires “critical infrastructure” organisations to have a clear and current view of their assets and who can control them – financially and electronically
- Accurately forecast interactions between the physical and cyber domains; maturity in asset management; provide deep insight into the supply chain
- Telecommunications is considered so complex it is addressed by separate legislation – Telecommunications Sector Security Reform (TSSR) Legislation

3. Prudential Standards – Processes and governance that supports peoples' wealth

- Boards are ultimately responsible for ensuring the security of its information assets
- Commensurate with the size and extent of the threats to these assets
- Enables the continued sound operation of the entity

Expect cross organisation and cross industry comparisons to occur so collaboration will be critical

(*) The Australian Financial Review 8 May 2018 Cyber Risk by James Turner

The voice of the wireless communications industry

Mission Critical Public Safety Communications Ecosystem

Environmental Scanning



What's Trending

- Cyber Security (**Public Expectations**)
- Critical Control Rooms
- Public Safety Mobile Broadband (PSMB)
- LMR - LTE Interworking – **3GPP Standards**
- Internet of (Public Safety) Things
- Mapping
- **Electric Vehicles** - Connected – Autonomous Vehicles (V2V) and Infrastructure (V2X)
- Blockchain
- **Ethics**


What's Agreed

- The need to share information globally
- The need to ensure the adoption of open standards to provide interoperability
- The need to ensure a focus on mission critical standards - 3GPP Standards.
- LMR will be with us for a long time.
- The need to establish a focus on the mission critical public safety communications ecosystem.

Mission Critical Public Safety Communications Ecosystem

Australia's PSMB Capability



- ❑ An RFI was released through the New South Wales Telco Authority on behalf of the Federal and State Governments on 27 November 2017 and closed 10 January 2018. The RFI advised that Australia's national interoperable PSMB capability will be based on:
 - A Federated Model i.e. the States and Territories can chose their time to provide this capability.
 - The use of a commercial mobile network operator
 - The potential for a pilot PSMB network.
- ❑ In October 2018 a RFP for a **Proof of Concept (POC)** was released closing in late December 2018 to test a specific delivery model for a PSMB capability. Expect the POC to include testing of a capability relating to the Objectives in the PSMB RFP. No further advice has been released about the outcome of the evaluation of the responses to the POC RFP.
- ❑ On 5 December 2018 the Prime Minster announced \$1.5M funding to expand the PSMB capability trial across Australia during 2019 and to establish a National Project Office to implement this capability within the public safety mission critical communications ecosystem.
- ❑ On 12 December 2018 the Council of Australian Governments (COAG) agreed to a Strategic Roadmap (#) that sets out a plan to design, implement and operate the PSMB capability and agreed to continue to work towards resolving the spectrum arrangements to support a PSMB capability.
- ❑ Further advice from the Department of Home Affairs is expected at the Comms Connect Conference in Sydney 12-13 June 2019 (*) 

(#) <https://www.coag.gov.au/sites/default/files/communique/public-safety-mobile-broadband-strategic-roadmap.pdf>

(*) <https://comms-connect.com.au>



Mission Critical Public Safety Communications Ecosystem Standards

3GPP Event – 18 September 2018



A Collaborative Event between 3GPP, CDMPS and Industry Associations (TCCA – ACCF & ARCIA)
The Event followed 3GPP TSG Plenary Meeting in Queensland Australia

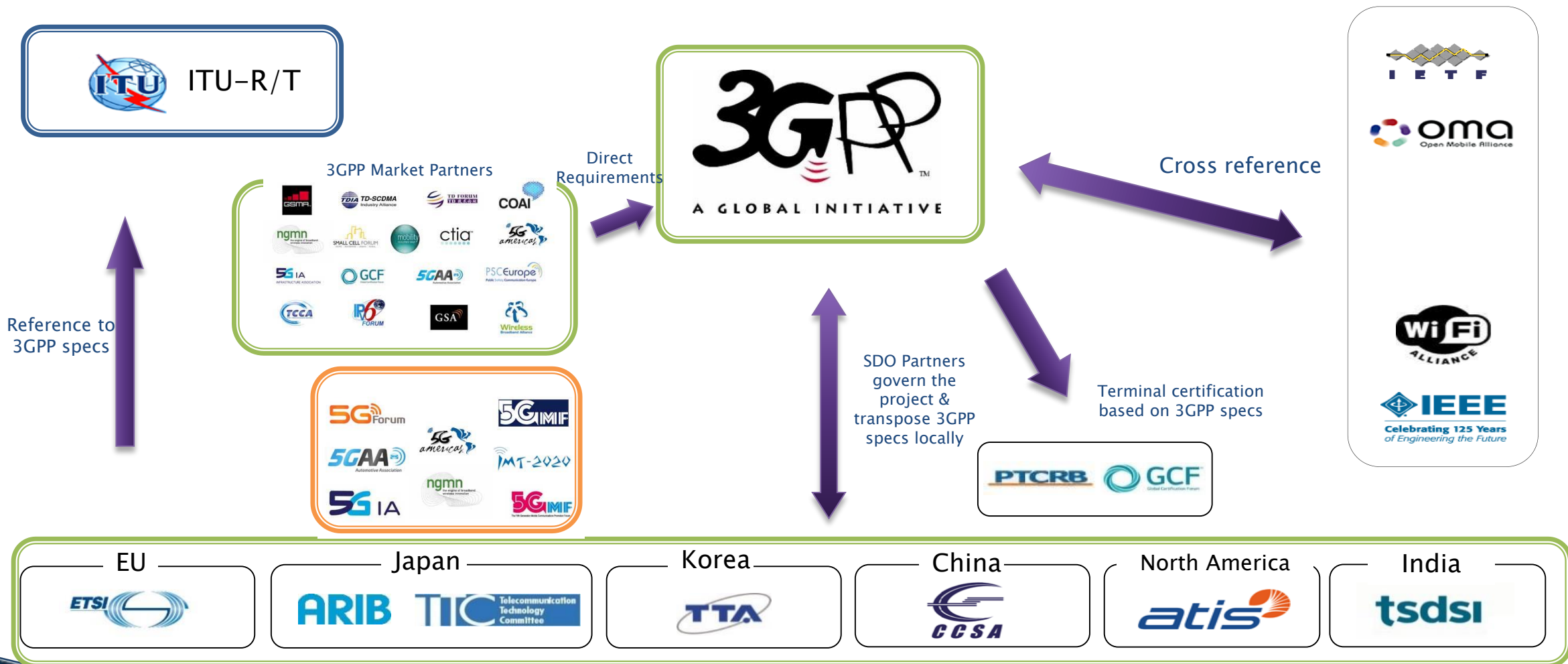


Key Highlights:

- ▶ Clarity of 3GPP Standards Development Ecosystem
- ▶ 5G
- ▶ Network Roaming
- ▶ Network Slicing
- ▶ Plug Tests @ Texas A&M University
- ▶ Mission Critical Open Platform (MCOP) NIST-PSCR funded research grant project (*)
- ▶ LMR will be with us for a long time

Mission Critical Public Safety Communications Ecosystem

The Eco-system for Global Mobile Standards



Mission Critical Public Safety Communications Ecosystem

Public Safety Internet of Things



Public Safety Internet of Things Working Group

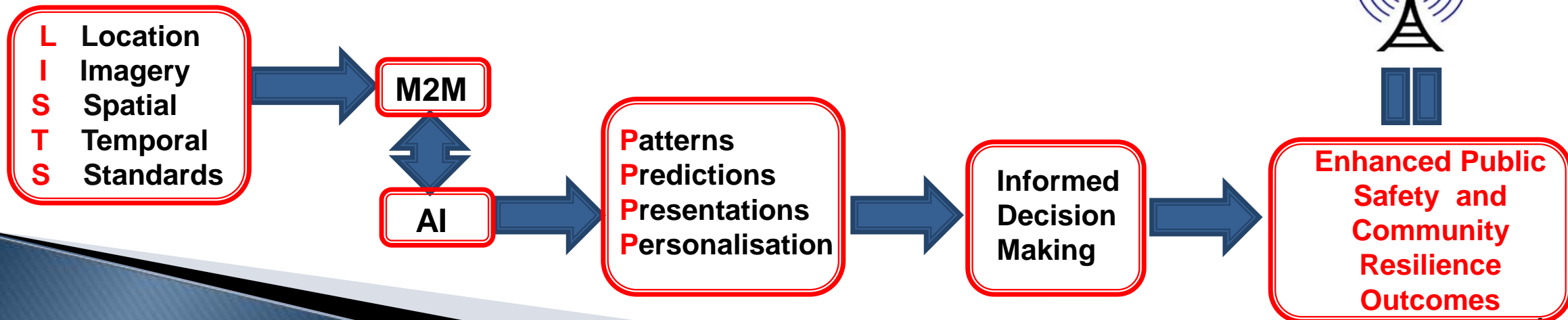
Use Cases Report

Due for Publication

Mission Critical Public Safety Communications Ecosystem

PSMB + Control Rooms - Its all about “data”

- The “public” is part of the public safety communications ecosystem
- The focus of the ecosystem at this point is about **DATA** and not Voice
- A large percentage of this Data will be spatially enabled
- “DATA” is the new “OIL”
- What is Mission Critical Data? - There is no definition for Mission Critical Data



Mission Critical Public Safety Communications Ecosystem

Sustainable Development Goals

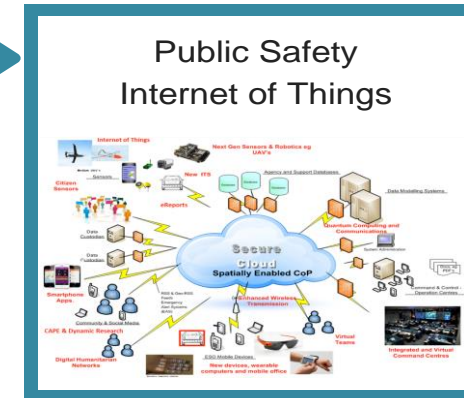


Emerging alignment



UNITED NATIONS

Current alignment



Enhanced
Community
Resilience

A BLUEPRINT FOR DISASTER MANAGEMENT
RD&D SUPPORTING THE SDGS – 2018
www.unimelb.edu.au/cdmeps

Mission Critical Public Safety Communications Ecosystem

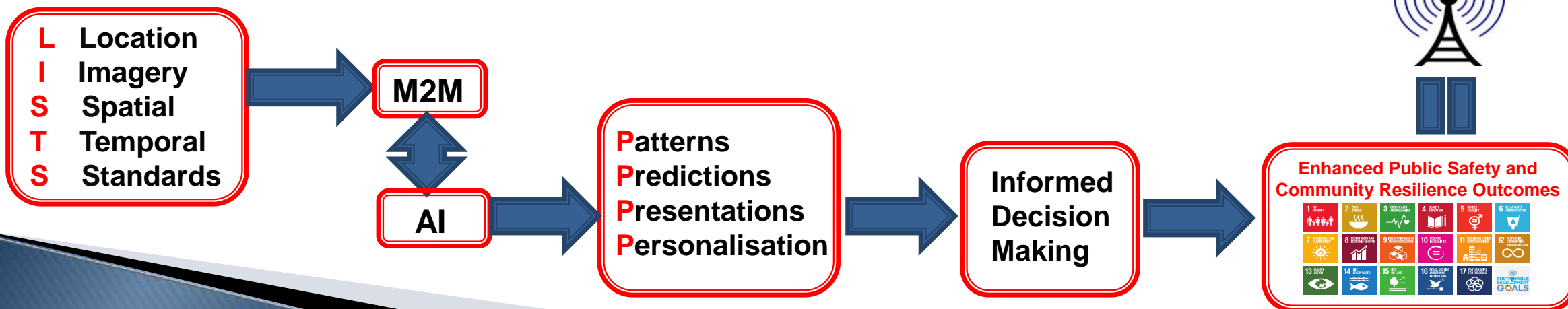
How Does It All Fit? – What's the emerging picture?

What's Trending

- Cyber Security (Public Expectations)
- Critical Control Rooms
- Public Safety Mobile Broadband (PSMB)
- LMR - LTE Interworking – 3GPP Standards
- Internet of (Public Safety) Things
- Mapping
- **Electric Vehicles** - Connected – Autonomous Vehicles and Infrastructure (V2V, V2X)
- Blockchain
- **Ethics**

Strategic Policy Issues

- Public Safety Mobile Broadband
- Critical Infrastructure Framework
- **National Security** *will start in Australian homes, streets and communities through the use of technologies that provide global 24/7 connectivity.*
- **National Public Safety Communications Ecosystem**
- Australia's Cyber Security Posture
- Information Sharing
- Dispatchable Address
- Culture Change



Mission Critical Public Safety Communications Ecosystem

Global conversations have to continue to share information



❑ May Comms Connect Auckland New Zealand



❑ June 2019: PSCE Lancaster UK



❑ June 2019: Critical Communications World Malaysia



❑ June Comms Connect Sydney Australia



❑ July 2019: PSCR Chicago USA



❑ August 2019: FirstNet Public Safety Leaders Meeting (TBC)



❑ October – November 2019: World Radio Conference Egypt



❑ November 2019: Comms Connect Melbourne Australia



❑ December 2019: PSCE Paris France

For Further information contact:

Geoff Spring

E-Mail: geoff.spring@gapstrategic.com

Mobile: +61411130184

<http://www.arcia.org.au/>