THE UNIVERSITY OF
MELBOURNE

CDMPS
CENTRE FOR
DISASTER MANAGEMENT
AND PUBLIC SAFETY

Australian Government Critical Infrastructure Centre

Strengthening the National Security of Australia's Critical Infrastructure

A Discussion Paper

Submission from

Centre for Disaster Management and Public Safety
University of Melbourne

21 March 2017

Response to the Critical Infrastructure Centre's Discussion Paper on Critical Infrastructure

Introduction

The University of Melbourne's Centre for Disaster Management and Public Safety (CDMPS)[1] welcomes the opportunity to respond to the Critical Infrastructure Centre's Discussion Paper on "Strengthening The National Security of Australia's Critical Infrastructure".

This Submission is consistent with the CDMP's strategic intent to support multi-disciplinary collaboration between researchers, government, industry, agencies and the community in delivering exceptional public safety outcomes.

Purpose

The purpose of this Submission is to identify in the context of the Department's Discussion Paper:

(a) The need to recognise Australia's Public Safety Communications Ecosystem (the Ecosystem) as Critical Infrastructure;

(b) The need to recognise the Discussion Paper as one of a series of Government and Department Discussion Papers independently addressing matters that will impact and/or influence the policy, strategic and regulatory settings associated with the evolution of the Ecosystem;

(c) To need to continue to raise the profile, understanding and awareness of the Ecosystem in the public safety market and amongst its key stakeholders.

Definition of Critical Infrastructure

This Submission is based upon the Trusted Information Sharing Network (TISN)[2] definition of critical infrastructure i.e.

"Those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security[3]".

Australia's Public Safety Communications Ecosystem

For the purpose of this Submission the Ecosystem will be considered to currently comprise the following components:

- Citizen communication devices
- The Emergency Call Person i.e. The Triple Zero Service

[1] www.cdmps.org.au
[2] www.tisn.gov.au

- Public Safety Agency Answering Points
- Public Safety Mission Critical Land Mobile Radio Networks
- The interfaces between each of these components that produce the interoperability capability and capacity that facilitates the receipt and transfer of information between each of these components

However, the Ecosystem is progressively moving from a complicated i.e. analogue – voice based environment, to a complex i.e. digital, data and IP based environment, within the information communications and technology mainstream. A simplified illustration of the Ecosystem is shown in Figure No1.

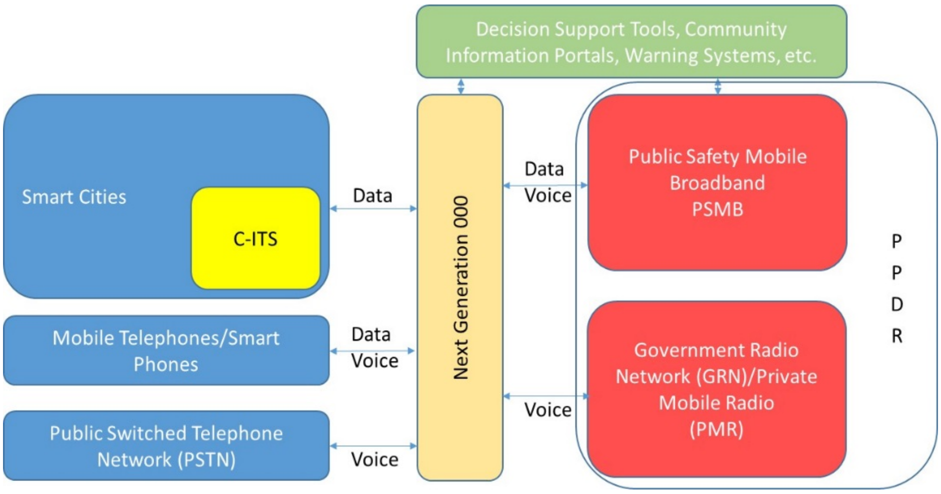
Decision Support Tools, Community Information Portals, Warning Systems, etc.
Smart Cities
C-ITS
Data
Mobile Telephones/Smart Phones
Data
Voice
Public Switched Telephone Network (PSTN)
Voice
Next Generation 000
Data
Voice
Public Safety Mobile Broadband PSMB
Voice
Government Radio Network (GRN)/Private Mobile Radio (PMR)
P
P
D
R

Figure No 1 – Simplified Illustration of the Public Safety Communications Ecosystem[4].

This transformation will be driven by Ecosystem stakeholders being able to produce Next Generation (NG) public safety communications capabilities by leveraging technologies developed to meet consumer/citizen expectations to be continuously connected anywhere anytime. Additionally the future Ecosystem must expand its services beyond the traditional emergency services sector and include a broader range of stakeholders, for example the owners and operators of critical infrastructure and their communications requirements as they pertain to public safety.

The Centre's Discussion Paper adds to and informs the policy, strategy and regulatory settings associated with the Ecosystem. More recent examples of this broader conversation include:

Next Generation Triple Zero

The Department of Communications Triple Zero Review in May 2016 has resulted in;

- Expression of Interest invited for Location Based Services for Triple Zero Service
- Expression of Interest invited for Emergency Call Person to provide the Triple Zero Service
- Advice sought on research access to the Integrated Public Number Database.

[4] Ged Griffin Industry Advisor CDMPS University of Melbourne

Public Safety Mobile Broadband

The Ecosystem needs a Public Safety Mobile Broadband capability to provide the capability and capacity to carry data, the majority of which will be spatially enabled, and support applications necessary to allow Australia's Public Safety Agencies to provide services that meet community expectations and build community resilience. It is assumed that this capability will also be utilised by Commonwealth Departments with responsibilities for national security and that these Agencies will supply data and information to the Critical Infrastructure Centre.

In the absence of a Public Safety Mobile Broadband capability many of Australia's Public Safety Agencies have utilised commercial networks from the Telecommunications Sector and should be expected to do so until the new national capability becomes available.

The Australian Government appointed the Productivity Commission to undertake a cost benefit analysis of the best way to deliver a mobile broadband capability to meet the long term needs of Australia's Public Safety Agencies. The Commissions' Report was provided to the Government on 22 December 2015 and released to public domain on 12 January 2016[5].

The Australian Government released its response to the Commissions' Report on 24 November 2016 in which the Government:

- Supported in principle the Productivity Commission's findings and recommendations that commercial mobile networks are the most efficient, effective and economical way of delivering a public safety mobile broadband capability.

- Recognised that mobile broadband offers significant potential to improve the efficiency of the emergency services and the safety of its officers.

- Committed to working with all States and Territories towards achieving an interoperable PSMB capability, and will establish a committee of Commonwealth, State and Territory officials to consider fully scoped proposals and report to the Council of Australian Governments in 2017.

The Government's expectation that this capability is to be provided using a *commercial* carrier places this capability in the context of the Telecommunications Sector Security Reforms (TSSR)[6] introduced in recognition of the limitations of current mechanisms to manage the national security risks in the telecommunications sector.

Collaborative Intelligent Transportation Services

In September 2016 the Australian Communications and Media Agency released a discussion paper on the proposed regulatory measures for the introduction of Collaborative Intelligent Transportation Services (C-ITS) in Australia in preparation for the introduction of connected vehicles into the Australian market. The Short Range Digital Communications associated with C-ITS is expected to become part of the Ecosystem.

[5] http://www.pc.gov.au/inquiries/completed/public-safety-mobile-broadband/report

[6] https://www.ag.gov.au/telcosecurity

The House of Representatives Standing Committee on Infrastructure, Transport and Cities

The House of Representatives Standing Committee on Infrastructure, Transport and Cities report on the Committee's Inquiry into the role of smart ICT in the design and planning of infrastructure released in March 2016 which made the following recommendations:

Recommendation 4

*The Committee recommends that the Australian Government recognise public safety communications systems as **critical infrastructure**, and continue to support the development of these systems, including funding research, promoting implementation, and providing national coordination.*

Recommendation 5

The Committee recommends that the Australian Government continue to support the development of disaster planning and emergency response systems, including funding research, promoting implementation, and providing national coordination.

Responses to the Questions raised in the Centre's Discussion Paper

Question: Are the proposed functions of the Centre adequate to better manage the national security risks to our critical infrastructure?

Response:

The Centre's Discussion Paper makes no reference to the role of academic research in Australia's ability to respond to the complex and evolving national security risks associated with critical infrastructure. Similarly, the Discussion Paper makes no mention of how the Centre will provide any leadership or coordination regarding research on critical infrastructure.

The Discussion Paper makes no reference to training and education. Raising the level of risk awareness and knowledge across all critical infrastructure sectors are key steps for reducing the residual risk as part of a broader risk management strategy.

Whilst the supply of liquid fuels is mentioned as part of the operation of "Ports", the criticality of liquid fuel within Australia's transport sector is understated in the Discussion Paper. Recent studies have identified the increasing vulnerability of Australia's fuel supply and have estimated that 90% of Australia's fuel comes from vulnerable fuel sources[7]. This gap indicates that the Centre's approach would be enhanced with the inclusion of Liquid Fuel as a key sector or as part of a key sub-sector within the Energy Sector. Additionally the Centre should consider the inclusion of the strategic forecasting of supply issues pertaining to the operation of critical infrastructure as part of its key functions.

[7] See Blackburn, J., (2014), Australia's Liquid Fuel Security Part 2: A report for NRMA Motoring and Services. http://www.mynrma.com.au/media/Fuel_Security_Report_Pt2.pdf

Question: What role could you play in assisting the Centre to undertake these key functions?

Response:

The University of Melbourne established the CDMPS to be able to undertake research to provide evidence based policy and strategy development related to disaster management and public safety through the utilisation of the Government – Industry – Academia Partnership. There is no mention of this Partnership or Academia specifically in the Discussion Paper.

The CDMPS is currently undertaking research into applications that will be carried by the Ecosystem's future networks which will further illustrate the need for the Ecosystem to be recognised as Critical Infrastructure.

The CDMPS has developed a network of international contacts in the public safety communications sector and has developed a relationship with the Australian Radio Communications Industry Association (ARCIA)[8]. ARCIA produced a study of the value of Land Mobile Radio to the Australian economy which produced the following findings:

- *The economic benefits of LMR spectrum use is between $1.99 billion and $3.72 billion per annum.*
- *This is compared to an annual opportunity cost of only $39.7 million, indicating the benefits of LMR are at least 10 times greater than the next best alternative.*
- *The report raises serious questions about the substitutability of alternatives to radio, which need to be carefully considered by ACMA and the Australian Government.*
- *Organisations that use LMR, particularly emergency and first responder services, are highly dependent on mission critical radio to provide essential public services.*
- *Users are highly committed to LMR technologies that provide important advantages, including 'one-to-many' communication, immediate and continual voice connectivity, and ability to operate effectively without mobile cellular infrastructure.*

Question: How should the Centre work with owners and operators when performing its functions, including understanding existing mitigation mechanisms?

Response:

The relationship with industry has to be based upon trust and transparency to encourage the sharing of information relating to existing risk mitigation mechanisms. Particular arrangements will need to be developed where commercial competitive advantage and intellectual property may be attached to these risk mitigation mechanisms. Industry Associations, such as ARCIA, should be actively involved in risk mitigation activities for critical infrastructure as the majority of submissions received in response to Government Discussion Papers come from Industry Associations on behalf of their membership bases.

[8] www.arcia.org.au

Question: What other type of information would be important for the Register to collect and why?

Response:

The type of information should be related to the significance of the risk associated with the particular asset and the relationship to other associated assets which may or may not be owned/controlled by the same organisation. For example, it would be an advantage to record critical inputs associated with the operation of the particular asset so that the cascading impact of an unrelated event could be understood. This step would allow an appropriate business continuity plan to be developed. Similarly, recording the downstream services delivered by the asset would support a broader impact analysis based on the loss or degradation of services from the asset.

Question: What other types of information would improve our understanding of foreign involvement in outsourcing, offshoring and supply chain arrangements?

Response:

In the case of organisations listed on stock exchanges the monitoring of organisational activity in the market should be a source of information.

Question: Does the 30 day period provide sufficient time for owners to register their interest in a critical infrastructure asset? If not, what alternative(s) do you propose and why?

Response:

In the case of organisations listed on stock exchanges timeframes apply regarding advice to the market of changes in ownership, shareholders and acquisitions etc. The same time frame could be applied in notification to the Centre and the Asset Register.

Question: Is a six-month transition period appropriate? If not, what alternative(s) do you propose and why?

Response:

This is a matter for consultation with Industry; however, any possible alignment with governance arrangements already in place lessens the administrative load on industry.

Question: What are the main advantages and disadvantages of a register administered by the Australian Government?

Response:

Refer to the previous responses about the relationship with industry being built upon trust and transparency and the ability to protect commercial competitive advantage and intellectual property. The main advantage has to be the opportunity to build confidence in Government's ability to build, maintain and use the Register to mitigate risk both to individual organisations and to the critical infrastructure sector as a whole. The main disadvantage has to be the cost of effectively and efficiently managing and maintaining the accuracy of the Register in a manner that firmly establishes credibility i.e. the Register itself has to be the subject of strong risk mitigation strategies.

Government's performance in these areas should generate confidence for further investment by industry in critical infrastructure projects in Australia e.g. the proposed Public Safety Mobile Broadband capability.

Question: What are your views on the introduction of a 'last resort power' to address significant risks where all other risk management avenues have been exhausted?

Response:

The reason for use of a "last resort power" and the control processes underpinning this power would need to be clearly explained to the key stakeholders e.g. the community, and would bring into play the role of Australia's Public Safety Agencies both in the implementation and consequence management of the use of the power. This would be one instance when the Ecosystem capability and capacity supporting these Agencies would need to be in place as a ''last resort".

Question: What other protective measures or safeguards could be applied to enhance national security risk mitigation in those rare cases where risk cannot be appropriately mitigated via current mechanisms?

Response:
Continuous capture of the lessons learned from risk events, adjustment to risk mitigation strategies and futures thinking based scenario planning incorporating contingency planning developed from market monitoring would contribute to the lessening of this risk.

In closing, the University of Melbourne's Centre for Disaster Management and Public Safety congratulates and continues to support the Australian Government's ongoing efforts in providing strategic leadership regarding the protection of Australia's critical infrastructure and the enhancement of community resilience across the nation.

For further information regarding this Submission please contact:

Geoff Spring
Senior Industry Advisor
Centre for Disaster Managment and Public Safety
University of Melbourne