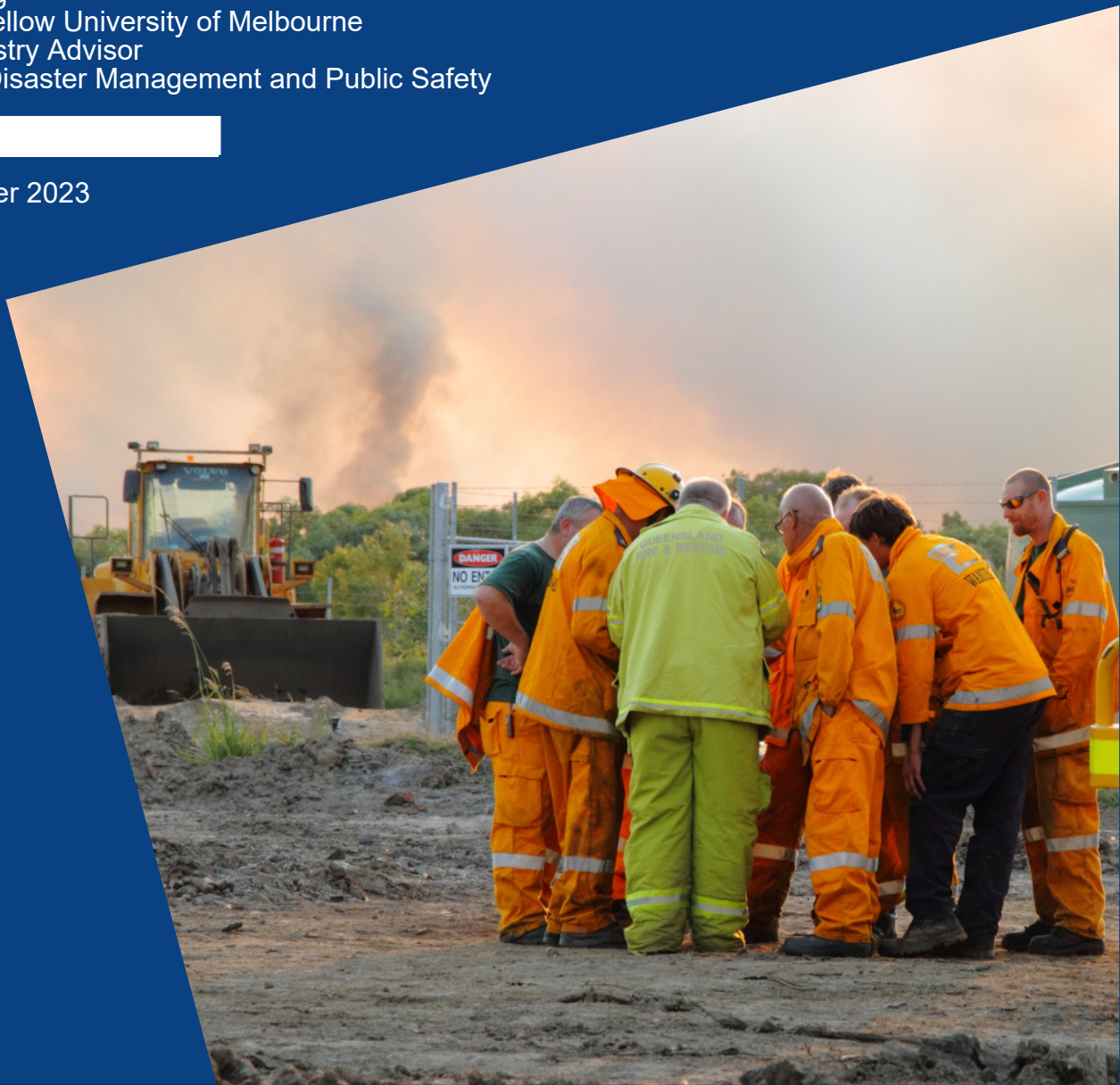# Inquiry into the Optus Network Outage

Author:

Geoff Spring
Honorary Fellow University of Melbourne
Senior Industry Advisor
Centre for Disaster Management and Public Safety

17 November 2023

16 November 2023

Mr. Sean Turner
Acting Committee Secretary
The Senate – Environment and Communications References Committee
Parliament House
Canberra

Dear Mr Turner

Inquiry Into the Optus Network Outage – 8 November 2023

Thank you for your correspondence dated 10 November 2023, inviting the University of Melbourne's *Centre for Disaster Management and Public Safety (CDMPS)*, to provide a submission to the inquiry being undertaken by the Senate – Environment and Communications References Committee into the Optus outage on 8 November 2023 and for providing the Terms of Reference for the inquiry.

In response to your invitation, please find attached CDMPS's submission for consideration by the Committee.

Should you require any additional information about the submission, or any component of the submission, please feel free to contact the submission's author directly.

Once again, thank you for providing the opportunity to participate in the Senate Committee's inquiry into the Optus network outage.

Yours sincerely

Alexander V. Babanin
Professor, Ocean Engineering
Adjunct Professor, Swinburne University of Technology
Director, Centre for Disaster Management and Public Safety (CDMPS)

The Senate Environment and Communications References Committee

OPTUS Network Outage Inquiry

1.0   Context

On 9 November 2023, the Australian Government's Senate referred to its Environment and Communications References Committee an Inquiry into the Optus network outage that occurred on 8 November 2023 and its impact upon Australians and the services they rely on. The Committee is to report its findings by 9 December 2023.

2.0   Introduction

The University of Melbourne's Centre for Centre for Disaster Management and Public Safety (CDMPS)[1] welcomes the opportunity to make this Submission to the Environment and Communications References Committee Inquiry into the Optus network outage using the following Terms of Reference:

  a.   the communication from Optus to affected customers;

  b.   the steps that Optus is taking to ensure that this does not happen again;

  c.   the compensation offered to affected customers, including:
      i.   compensation offered by Optus,
      ii.   the role of the Telecommunications Industry Ombudsman and its compensation scheme, and
      iii. actions taken by the Federal Government to support affected customers to receive fair compensation

  d.   the role of government in ensuring Australians have reliable access to telecommunications technology;

  e.   steps taken by the Federal Government to ensure the access to essential service in response to the outage, including:

      i.   identification of affected government services,
      ii.   the establishment of alternative contact arrangements for affected government services, and
      iii. communication with Australians on those alternative arrangements;

  f.   actions taken by the Federal Government and the Australian Communications and Media Authority on the day of the outage;

  g.   any other related matters.

---

[1] Centre for Disaster Management and Public Safety (unimelb.edu.au)

3.0   Focus of this Submission

This Submission specifically focuses on items a, b, c and d contained within the Terms of Reference and by further consolidating these four items identifies the two questions that need to be asked by all Australians about the Optus Outage;

- The ability to" *access to essential service(s)"* in the circumstances of both emergencies and natural disasters;

  and

- The impact of telecommunications outages on the operational capacity and capabilities of Australia's Public Safety Agencies both now and in the future.

This consolidation also allows the Optus Outage to be considered in the context of the *"Mission Critical Public Safety Communications Ecosystem"* that currently provides Australia's Public Safety Agencies their operational capacity and capabilities and should continue to do so into the foreseeable future as *"critical infrastructure"* under cover of the Security of Critical Infrastructure legislation as a "System of National Significance".

3.1   "Mission Critical Public Safety Communications Ecosystem"

- *Assess the National Triple Zero System* in the context of the impact of the Optus network outage on Telstra as the contracted provider of Australia's Triple Zero service and in particular the ability of all Australian's to *"roam"* onto alternative telecommunications networks (Telstra, Optus and TPG) to access the Triple Zero Service;

- *Assess the Optus wireless network* in the context of the capacity and capability of the Telstra and TPG networks to seamlessly absorb the absence of the Optus network and the subsequent impact upon the operational capacity and capabilities of Australia's Public Safety Agencies;

- *Assess the Communications Centres of Australia's Public Safety Agencies* (Law, Enforcement, Ambulance, Fire and State Emergency Services and in the case of the State of Victoria "Triple Zero Victoria" (formally the Emergency Services Telecommunications Authority (ESTA)) within Emergency Management Victoria in the context of the impact of the Optus outage on the operational capacity and capability of these Centres to receive Triple Zero Calls from Telstra and the dispatch the resources on the Public Safety Agencies and provide on-going support to these Agencies during the course of the emergency;

- *Identification and assess Risk Mitigation Strategies* in place across the Ecosystem of Australia's Public Safety Agencies to provide continuity of service and resilience to all Australians in times of emergencies and natural disasters.

Assess the impact of Telecommunications Outages on Future Technology Enhancements

- *Next Generation Triple Zero Service*

The current "voice only" Triple Zero service will be upgraded to allow callers to transfer data (pictures, videos, live feeds) and enhanced location information in support of their calls for emergencies and response by Public Safety Agencies. This upgrade will make the Ecosystem even more complex as its changes in technology and data flows through the existing Ecosystem.

This increased complexity will need to be reflected in increased investment in enhanced risk mitigation and redundancy arrangements

- *Public Safety Mobile Broadband*

The proposed *Public Safety Mobile Broadband (PSMB)* capability for Australia's Public Safety Agencies needs to be included in the consideration of the Optus Outage on the future operational capacity and capabilities as the PSMB it will provide data carrying and intelligence capabilities of Australia's Public Safety Agencies never seen before to the benefit of all Australians.

Optus has been a member of the PSMB Proof of Concept Team and the degree to which its network was involved in testing performed as part of the Proof Of Concept needs to be determined to assess the potential impact the operational capacity and capabilities of Australia's Public Safety Agencies.

- *Land Mobile Radio*

Land Mobile Radio (LMR) is the technology used by Australia's Public Safety Agencies to provide voice only radio communications between Agencies and Communication Centres and investment through both upgrades and expansion of these networks such as the new the Tasmanian Government Radio Network being the most recent example.

3.2 Risk Management - Cyber Security and Critical Infrastructure

On 13 November 2023 the Minister for Cyber Security announced[2] that Optus, Telstra and other major telco boards will be required to sign off on a new or updated cyber risk management program every year or face hundreds of thousands of dollars in penalties.

These changes are part of new laws to be introduced by the Minister for Home Affairs that will classify telecommunications as *"critical infrastructure"* for the first time under the Security of Critical Infrastructure Legislation. These changes are part of new laws to be introduced by the Minister for Home Affairs Minister that will classify telecommunications as *"critical infrastructure"* for the first time under the Security of Critical Infrastructure Legislation.

Dating back to 2015 the CDMPS and its industry partners has been making Submissions to various Government Committees regarding the need for the *"Mission Critical Public Safety Communications Ecosystem"* to be formally recognised as *"Critical Infrastructure"*.

The potential consequences of the Optus outage should reinforce the need for these changes but even more so now as a *"System of National Significance"*

While this enhancement is welcomed this requirement appears to only address the "network component" of the Ecosystem when it should also address any other services and/or components provided by telecommunications organisations for use within the Ecosystem.

Global Standards Organisations develop open standards designed to enable the interaction of the various components of the Ecosystem. The formal adoption of the use of these Standards in the design, construction, and operation of the various components of the Ecosystem together with an independent compliance testing process should be part of a Risk Mitigation Strategy for the Ecosystem.

4.0 CDMPS submissions to Government Committees, Departments and Agencies

The CDMPs and its industry partners have made a range of Submissions such as this one to various Government Committees consistent with the conclusions and recommendations made in the Submission. For consistency and record purposes the following sample is provided to demonstrate the linkages between the matters being considered by the various Committees

---

[2] Australian Financial Review

- 2023 – 2030 Australian Cyber Security Strategy

  On 15 April 2023, the CDMPS made a joint Submission with the Australian Radio Communications Industry Association[3] (ARCIA) in response to the Cyber Security Strategy Discussion Paper. The Australian Financial Review reported on 13 November 2023 that the Government's Cyber Security Strategy would be released later this month

- The House of Representatives Standing Committee on Communications and the Arts – Inquiry into co-investments in multi carrier regional mobile infrastructure – the experience opportunities and challenges (not including matters related to national security)[4] The Report from this Committee has not yet been published.

  The CDMPS made a joint Submission with the Australian Radio Communications Industry Association (ARCIA) and was invited to give evidence to the Committee, The Police Federation of Australia[5] (PFA) made a separate but supporting Submission to the Committee and The Police Association of Victoria (TPAV) provided separate and supporting evidence to the Committee.

- Submissions to the Government and the Cyber and Infrastructure Security Centre[6] (CISC) during the drafting of the Security of Critical Infrastructure Legislation.

- The Royal Commission into the 2029/2020 Bushfires – 28 October 2020

  The CDMPS made a Submission to the Royal Commission and was subsequently invited to provide evidence to the Commission recognized in Chapter 6 National Emergency Response Capability Recommendations 6.1 to 6.5 of the Commission's final report.

- 2015 House of Representatives Report on the use of Smart ICT

  This Report was tabled in Parliament and contained a recommendation that public safety communications be recognized as *"Mission Critical Communications Ecosystem"* – There has been no Government response to this Report and assistance to locate a response was sought in evidence given to the Inquiry into co-investments in multi carrier regional mobile infrastructure

Related

- The 21 June 2023 Australian Competition Tribunal decision stopping the proposed Telstra – TPG spectrum sharing proposal regarding *"roaming"* across telecommunications networks and the sharing of spectrum in natural disasters arising should be revisited for its impact on the operational capacity and capabilities of Australia's Public Safety Agencies.

5.0 International Experience

The United Kingdom's OfCom is undertaking an investigation into British Telecom in relation to the disruption to 999 emergency call services on 27 June 2023.

It is understood the OfCom Investigation is on-going, but its findings and recommendations should be valuable in contrasting the nature of the British Telecom and Optus outages and the incorporation of their respective findings into both Risk Mitigation and Lessons Learned outcomes for all parties concerned.

---

[3] Home | ARCIA - The Australian Radio Communications Industry Association
[4] Inquiry into co-investment in multi-carrier regional mobile infrastructure – Parliament of Australia (aph.gov.au)
[5] Police Federation of Australia - The National Voice of Policing (pfa.org.au)
[6] https://www.cisc.gov.au/

6.0 Conclusion and Recommendations

Conclusion

The outcome from the Committee's Inquiry needs to assure all Australians regarding their ability to have *"access to essential service(s)"* in the circumstances of both emergencies and natural disasters and that its recommendations have identified the impact of telecommunications outages on the operational capacity and capabilities of Australia's Public Safety Agencies both now and in the future.

Recommendations

The Optus Outage needs to be considered in the context of the following recommendations:

1. The *"Mission Critical Public Safety Communications Ecosystem"* that currently provides Australia's Public Safety Agencies with the operational capacity and capabilities should be formally recognised as *"critical infrastructure"* and as a *"System of National Significance"* supported by suitable legislation.

2. The role of Optus in the Proof of Concept for the Public Safety Mobile Broadband (PSMB) Project in determining its impact on the future operational capacity and capabilities of Australia's Public Safety Agencies as the PSMB is expected to provide data carrying and intelligence capabilities never seen before to the benefit of all Australians.

3. As part of a Risk Mitigation Strategy for the Ecosystem the use of the global standards should be formally adopted in the design, construction, and operation of the various components of the Ecosystem together with an independent compliance testing process.

4. The 21 June 2023 Australian Competition Tribunal decision stopping the proposed Telstra – TPG spectrum sharing proposal regarding *"roaming"* across telecommunications networks and the sharing of spectrum should be revisited for its impact on operational capacity and capabilities of Australia's Public Safety Agencies in responding to emergencies and use in natural disasters.

5. The recommendations from the Royal Commission into the 2029/2020 Bushfires relating to the *"Mission Critical Public Safety Communications Ecosystem" i.e.* Chapter 6 National Emergency Response Capability Recommendations 6.1 to 6.5 need to be implemented on a national basis with progress being publicly reported at regular intervals.

6. The outcome of the United Kingdom's OfCom investigation into British Telecom in relation to the disruption to 999 emergency call services on 27 June 2023 should be considered in preparing the Committee's findings and recommendations.

Author:
Geoff Spring
Honorary Fellow University of Melbourne
Senior Industry Advisor
Centre for Disaster Management and Public Safety
17 November 2023