1st November 2025

[redacted]

Committee Secretary
Senate Standing Committees on Environment and Communications
PO Box 6100
Parliament House
Canberra ACT 2600

Submission on Inquiry into Triple Zero Service Outages

Dear Committee,

I hope all members are well.

As a retired police officer who operated a Triple Zero mobile patrol car, I have firsthand experience with the critical importance of a reliable communication system in emergency situations. I fully understand the dire consequences that arise when such a system fails. The reliance on seamless communication during crises is paramount for ensuring public safety, and my background equips me with a unique perspective on the challenges faced by both emergency responders and the communities they serve.

I wish to submit my thoughts on the critical issues surrounding Triple Zero service outages, with a focus on the Optus outage on 18th September 2025. I present this submission to underscore the urgency of improving our telecommunications infrastructure, particularly in the context of Australia's civil defence measures.

Thank you for advising the public about the incident on the 18th September 2025. As I understand it, the Optus Triple Zero service outage revealed significant vulnerabilities in emergency telecommunications that have dire implications for public safety. I understand the consequences firsthand from my experience as a first responder. The delays in emergency assistance, which resulted in loss of life, underscore the necessity for robust and resilient communication systems.

This incident serves as a wake-up call to not only address existing shortcomings but also to rethink and strengthen our emergency response framework to safeguard against future outages.

As a person considering the wide range of issues, I am particularly concerned about the vulnerabilities of our mobile phone system at a regional and national level to electromagnetic pulses (EMPs), the potential impacts of a Carrington-like event, and threats posed by terrorism.

In this context, I will be submitting relevant excerpts from our National Civil Defence proposal to the Australian Government for their consideration in the near future.

The following points are highly relevant to ensuring that large telecommunications corporations comply with the necessary standards for "emergency response at the local, regional, and national levels."

I will provide the following in relation to national-level events only:

The following are three reputable subject matter experts on the possibility of a national event significantly impacting communications.

October 2014, a presentation to Institute of Public Affairs' members, national security expert, Peter Jennings AO, said: *"We don't have an exit strategy from our own region, and so what I'm going to be talking about is something which, if it happens, and we all must hope that it doesn't, but if it happens it's going to involve Australia in a way that we can't escape from."*

April 2017, Former U.S. Army Intelligence officer James Wesley, Rawles said: *"Australia is vulnerable to invasion. This is because of your geographic isolation and relatively small military,' he told Daily Mail Australia."*

September 2021, Dr Alexey Muraviev said:
"The relative ease of attacking mainland Australia comes from the geographical distribution of our major industrial and population centres, which are located within Australia's littoral. Over 90 per cent of the country's population is spread along coastal areas, with a majority concentrated in a number of urban hubs located on the Pacific, Southern and Indian Ocean sides of the country."

Summary of the Major Threats to Telecommunications:

Electromagnetic Pulse (EMP) Attack:
An EMP can be generated by nuclear detonations at high altitudes or by non-nuclear means. An EMP disrupts or damages electronic devices and critical infrastructure, leading to widespread communications failures.

Solar Activity:
Solar flares and coronal mass ejections (CMEs) can have significant impacts on telecommunications by inducing geomagnetic storms. These storms can disrupt satellite operations, radio communications, and ground-based power grids.

Cyber Attacks:
State-sponsored or independent actors can target telecommunications infrastructure through

malware, ransomware, or denial-of-service attacks, disrupting services and compromising sensitive information.

Natural Disasters:
Events like hurricanes, earthquakes, and wildfires can damage physical infrastructure (e.g., cell towers, fiber-optic cables), interrupting services and isolating communities.

Technical Failures:
Faulty equipment, software bugs, or human error can lead to outages in telecommunications systems, affecting multiple users or regions.

Terrorism:
Physical attacks on telecommunications infrastructure can lead to service disruptions. This includes bombings or other targeted violence against critical installations.

Historical Impacts

The Carrington Event (1859):

A massive solar storm, the Carrington Event, produced one of the largest geomagnetic storms in recorded history. Telegraph systems across the United States and Europe experienced widespread disruptions; some operators received electric shocks, and systems were rendered inoperable. Auroras were visible at unusually low latitudes, and the event highlighted the vulnerability of early telecommunications to solar phenomena.

Local and Worldwide Historical Examples:

1972 Solar Flare: A powerful solar flare caused communications disruptions for military and civilian radio operators, impacting air travel and tracking operations.
1994 Northridge Earthquake: Caused extensive damage to telecommunications infrastructure in Southern California, leading to widespread outages.
2003 Solar Storms: Several solar storms caused issues with power grids and disrupted satellite communications, highlighting vulnerabilities in modern infrastructure.
Recent Events Affecting National Communications
2020 Australian Bushfires:
Severe bushfires impacted telecom infrastructure across Australia, leading to service outages in affected areas, especially in rural regions.
2017 Hurricane Harvey:
The hurricane caused extensive flooding leading to communications outages as power systems failed and infrastructure was destroyed.
Cyber Attacks:
Incidents like the 2020 attack on Australia's telecommunications infrastructure, suspected to be linked to state-sponsored actors, highlighted vulnerabilities and caused service disruptions.
2023 Optus Outage: A nationwide outage affected calls to Triple Zero (emergency services) and raised concerns about the resilience of telecommunications infrastructures and their ability to handle crises.

Legislation Applicable to Wartime Communications:

The Warlike Act of 1945, formally known as the National Security Act 1945, was enacted in Australia in the aftermath of World War II to establish a framework for national security and defence. While its original intent was to prepare Australia for the possibility of invasion and to manage wartime resources, its principles can be directly related to the creation of a robust National Civil Defence framework today.

Here are several ways in which the Warlike Act can guide current and future civil defence initiatives.

Structure of Civil Defence Governance:

The Warlike Act established a foundational framework for organized civil defense efforts, outlining a clear governance structure focused on national security. In today's context, this legislation serves as a vital model for ensuring that telecommunications companies understand their responsibilities during wartime. As the potential for major conflict in our region affecting Australia remains low, the consequences of inaction are severe. We must emphasize the importance of compliance within the telecommunications sector to facilitate coordinated emergency responses.

1. Emergency Preparedness and Resource Management:

A key objective of the Warlike Act was to guarantee effective resource allocation in times of crisis. This principle is crucial for today's National Civil Defence strategy, which should prioritize preparedness, resource mapping, and inventory management. Telecommunications providers need to be held accountable for ensuring that essential communication services remain available during emergencies, enabling access to vital resources such as food, water, and medical supplies.

2. Community Involvement and Training:

Recognizing public involvement in national defence was a cornerstone of the Warlike Act. It is essential to foster a culture of readiness and resilience in our communities today. Modern initiatives should encourage volunteerism and training, equipping citizens with the skills necessary for emergency response, first aid, and effective communication. Telecommunications companies must engage with communities to facilitate training programs that reinforce the importance of reliable communication during crises.

3. Legislative Support for Emergency Measures:

The legal framework set forth by the Warlike Act empowered the federal government to implement necessary emergency measures. Today, contemporary civil defence initiatives should advocate for updated legislation that clarifies the responsibilities of telecommunications providers.

This legislation must ensure that these corporations are prepared to respond swiftly and effectively to potential threats, whether from natural disasters, acts of terrorism, or vulnerabilities in technology.

In summary, drawing on the principles established by the Warlike Act is essential for developing a modern National Civil Defence strategy that holds telecommunications companies accountable. Their role is crucial in maintaining communication infrastructures that safeguard public welfare during both peacetime and wartime, especially given the potentially devastating consequences of any conflict affecting Australia.

The Need for Long-Distance Encrypted Radio Communication

In light of the failures highlighted by this outage, I propose the development of long-distance encrypted radio communication networks that can serve as reliable alternatives during emergencies. This initiative is particularly crucial in a vast country like Australia, where geographical limitations often hinder effective communication.

Key Proposals:

1. **Upgradation of Registered Firearm Ranges to Hubs:**
    - Transform existing firearm ranges into EMP-protected local hubs equipped with mobile stations for long-distance radio communication.
    - This infrastructure will ensure secure connectivity, especially in remote areas, remaining operational even when traditional networks fail. It is to be noted that ballistic sports ranges are typically located away from pre-targeted cities, airports, bridges, and other infrastructure. Many were originally established during World War Two.

<u>Explanatory Notes Point One Above:</u>

Telecommunications companies can play a vital role in supporting national civil defence efforts, particularly in scenarios where high-frequency (HF) radio operations and mobile phone systems are compromised.

Here are several ways in these companies may be required to assist:

1. Establishing Redundant Communication Systems:

HF Radio Networks: Telecommunications companies can develop and maintain HF radio networks that are independent of existing mobile infrastructures. HF radio communication can cover vast distances and is less susceptible to local disruptions, making it a reliable alternative during emergencies.

Satellite Communication: They can enhance satellite communication capabilities, providing another layer of redundancy to ensure that critical communication can continue even when ground-based systems fail.

2. Integration with Emergency Services:

Collaboration with Civil Defence and other Agencies: Telecommunications providers can work closely with national and state emergency services, ensuring that their radio systems are interoperable with those used by emergency responders.

Dedicated Channels for the use by the National Civil Defence. They can allocate specific frequencies or channels for emergency communications to the training base stations located at registered ballistic sports ranges, ensuring that vital information can be transmitted even during severe national disruptions.

3. Training and Support for Emergency Personnel:

Training Programs: Telecommunication companies can offer training for civil defence personnel and volunteers on using HF radios and other alternative communication systems. This preparedness can improve response times during emergencies.

Technical Support:

Providing technical support and expertise to civil defence agencies can enhance their operational effectiveness, ensuring that communication systems are properly maintained and utilized.

4. Resource Sharing and Logistics:

Equipment Provision:
Telecommunication companies can support civil defence by providing necessary communication equipment, such as portable HF radios, for use in emergency situations.

Logistical Support:
Establishing logistical frameworks that allow for quick deployment of communication resources to affected areas can significantly enhance emergency response efforts.

5. Public Information Dissemination:

Emergency Alerts:

Even when mobile phone networks are compromised, telecommunications companies can utilize HF radio to disseminate emergency alerts and information to the public, keeping communities informed about safety measures and resources.

Community Engagement:

By engaging with local communities through HF radio broadcasts, telecommunication companies can educate citizens on safety protocols and updates during crises.

6. Testing and Drills:

The following are extracts from: **https://cpb.life/index.php/summary-of-findings/long-distance-encrypted-radio-communication/**

Conducting Regular Drills:
Organizing regular emergency drills that incorporate HF radio communication can help ensure readiness and identify potential issues in the integration of radio systems with civil defence operations.

System Testing: Regularly testing the resiliency of HF networks and ensuring that emergency communication protocols are effective can enhance overall response capability.

1. **Integration of Swiss National Security Model:**
    - Drawing from the Swiss national security model, we can bolster our civil defence capability by involving members from ballistics sports clubs. This would enhance community involvement and ensure that reserve units are prepared and equipped to respond swiftly during crises under the instruction of the Australian Defence Force (ADF).
2. **Implementation of Comprehensive HF Radio Networks:**
    - Establish a comprehensive HF radio communication network linking reserve units and training base stations at ballistic sports ranges throughout Australia. This will facilitate coordination and resource sharing, particularly when conventional communication channels are compromised.

Resource Coordination and Community Preparedness

We must also consider the importance of resource mapping and community supply chains. By encouraging reserve members of the National Civil Defence to document local resources and develop community-based supply networks. The goal is to ensure that essential supplies are quickly accessible to communities during emergencies. It is important to recognize that many individuals involved will be members of both the State Emergency Services and the National Civil Defence.

This group will include active and retired personnel from the military, police, security, and other emergency service sectors, providing the leadership and expertise necessary for effective response in times of crisis.

The Role of Government and Regulatory Bodies

The findings from the inquiry should strongly emphasize the responsibilities of the Minister for Communications, the Australian Government, and the Australian Communications and Media Authority (ACMA) in ensuring the reliability of emergency telecommunications. It is critical that the existing regulatory frameworks and emergency response protocols be reevaluated and strengthened.

Conclusion

The recent outages have distinctly illustrated the vulnerabilities in our telecommunications infrastructure. In anticipation of future crises, particularly in light of potential regional conflicts, it is crucial to adopt a precautionary approach. We must act decisively to mitigate risks associated with communication breakdowns by investing in alternative communication methods such as encrypted radio networks.

In conclusion, I urge the committee to consider these proposals and the overarching need for a National Civil Defence initiative based on the Warlike Act of 1945. Ensuring the safety and preparedness of our population should be our foremost priority.

Thank you for considering my submission.

Sincerely,

[redacted]

Bio not for publication:

[redacted]