Global Conference of the Youth Environmental Alliance in Higher Education

2nd International Conference of the YEAH

Dec 9th, 2:12 PM - 2:23 PM

Session 1B Internet Expansion Plan Proposal in Developing Countries: Peru as a Case Study

Garion Johnson

Gonzalo Jose Manuel

Neira Chacate

Paul Lavasseur

Andrew Goodolf

See next page for additional authors

Recommended Citation

Johnson, Garion; Manuel, Gonzalo Jose; Chacate, Neira; Lavasseur, Paul; Goodolf, Andrew; and Murphy Pauletto, Ally, "Session 1B Internet Expansion Plan Proposal in Developing Countries: Peru as a Case Study" (2020). *Global Conference of the Youth Environmental Alliance in Higher Education*. 7.
10.37099/mtu.dc.yeah-conference/2020/all-events/7

Presenter Information

Garion Johnson, Gonzalo Jose Manuel, Neira Chacate, Paul Lavasseur, Andrew Goodolf, and Ally Murphy Pauletto

Internet Instability

The risks and relationship between climate change and our Internet infrastructure

Luke Huels || 24189847 || 4403 words

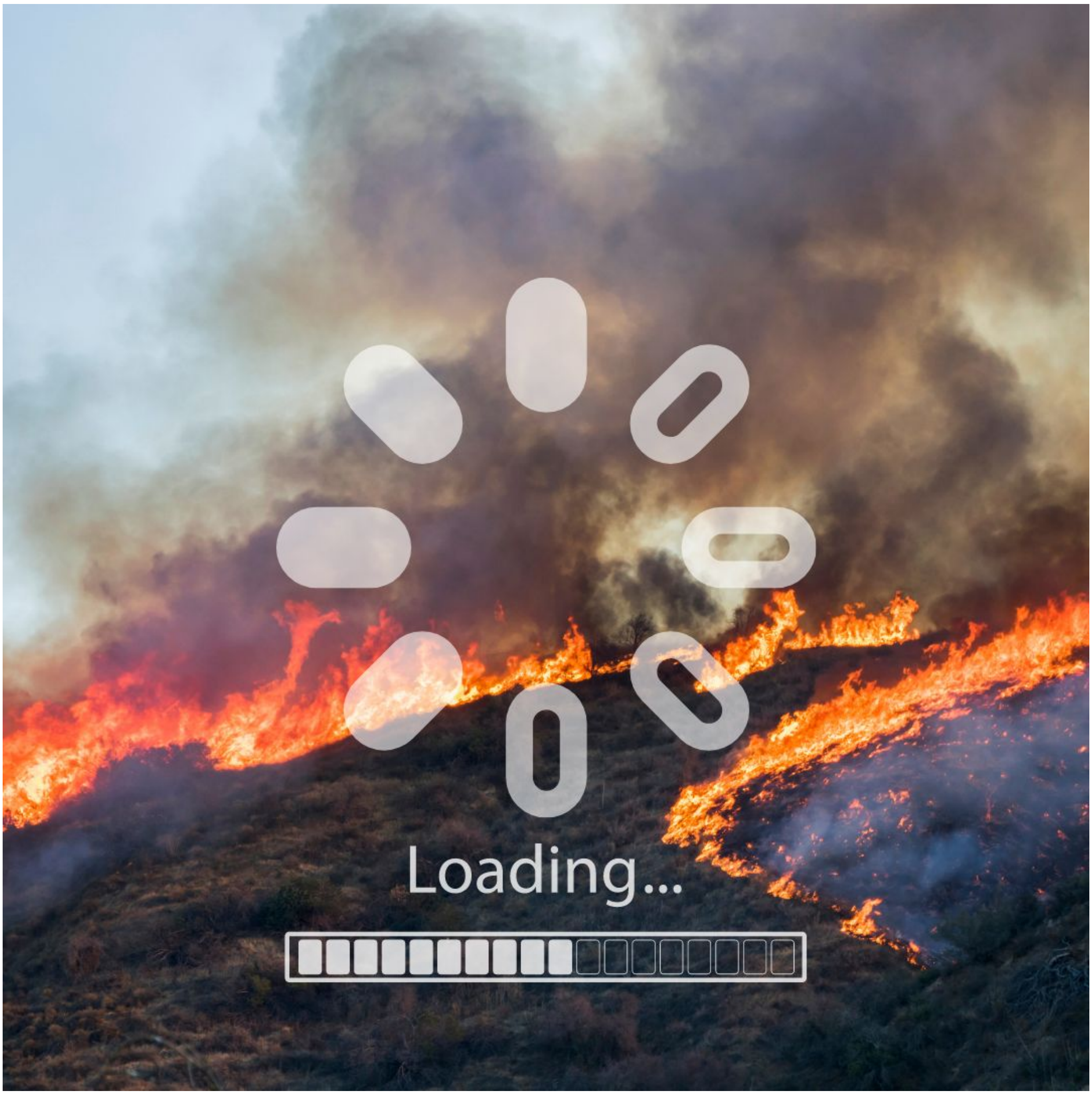


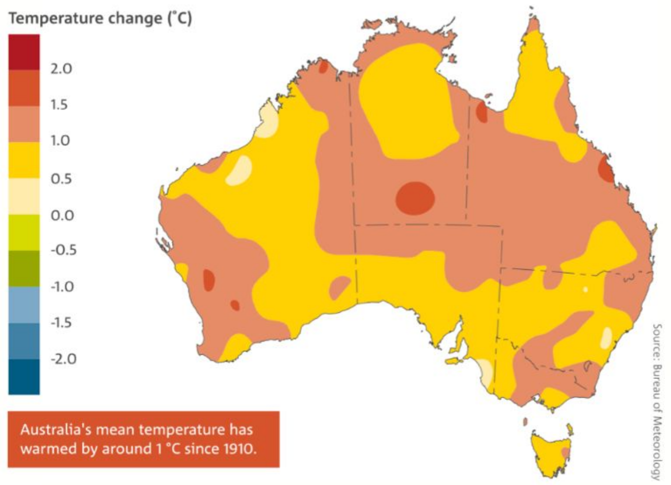
Table of Contents

Executive Summary

Whether it be the extreme bushfires Australia suffered over 2019 – 2020, or the six-year drought California suffered this decade – the impacts of climate change are making themselves increasingly clear. Our atmosphere is inundated with greenhouse-gas (GHG) emissions such as carbon dioxide (CO2) and methane (CH4+), and nations are fighting to keep global mean temperature increase below 1.5C by mid-century. Although mitigation efforts are ongoing, discourse is increasingly turning towards adaptation. In this context, careful consideration of the effects on, and ongoing maintenance, of built environments is of paramount importance. Unprecedented changes in our climate and weather systems will disrupt our critical infrastructure and bring severe and far-reaching consequences for our social, environmental and economic systems. However, while much research and attention has been directed at the vulnerability of various instances of critical infrastructure, very little has been afforded to a system that has become ubiquitous and, perhaps, taken for granted: the Internet. The daily operations of individuals, corporations, and government have become dependent on the provision of a widespread and reliable internet connection. Climate change poses risks to physical internet infrastructure. Here, the vulnerabilies pertinent to the Australian context – namely from wildfires, sea-level rise, and changing weather patterns – are explored. From this it is clear that there is both cause for concern and a need for a unified and coherent stetgic plan to protect Australia’s internet access. This is an under investigated topic in the Australasian region (and, arguably, internationally); the current research forms a baseline from existing knowledge and provides direction for future research and management actions.

Setting the (Anthropo) Scene

Since around the mid-20th Century, a number of extraordinary changes have occurred in human and natural systems. These changes began with the Industrial Revolution, but it was not until after WWII that they began to grow exponentially in number and impact: the so-called ‘Great Acceleration’ (Engelman, 2013). These changes – particularly the increase of GHG’s in the atmosphere – are dramatically altering the fundamental ways our planet functions. The rate of atmospheric CO2 rise, for example, is now 100 times faster than during the end of the last ice age (Steffen et al., 2011). The sum of changes catalysed by this Great Acceleration have marked a new geological epoch referred to as the ‘Anthropocene’ – the era of human influence over Earth systems. The evidence for these changes being human induced has become virtually certain (Hite & Seitz, 2016; Intergovernmental Panel on Climate Change, 2019) and the real and observable consequences of climate change on natural phenomenon are already being seen. **Fig.** 1 shows how Australia has already experienced observable warming. However, global change has been complex and variable. Increased temperature without moisture availability suppresses some regional rainfall while, elsewhere, increased temperature allows more moisture to be taken into the atmosphere, increasing potential energy of the system.



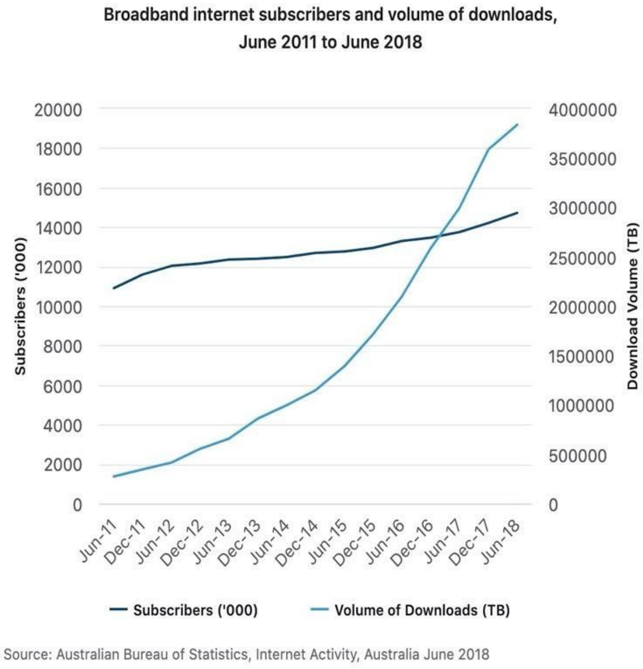
Australia's mean temperature has warmed by around 1 °C since 1910.

Source: Bureau of Meteorology

Change in temperature is relatively easy to quantify, but what about other parameters such as extreme events or weather patterns? Climate extremes are rare, high-impact weather events such as droughts, hurricanes, floods, or heat-waves: they typically fall in the tail ends of the probability distribution for a given phenomenon. There is evidence to support changes in the incidence patterns of many extreme events (Murray & Ebi, 2012). Whether it be the extreme bushfires Australia suffered over 2019 – 2020, or the six-year drought California suffered this decade – the impacts of climate change are making themselves increasingly clear. Climate influences nearly all the natural systems on Earth within which our societies are situated. While there are have been well observed consequences of this anthropogenic change on biodiversity and ecosystem services, the implications for built environments are also an area of increasing concern. So, what does a changing climate mean for the infrastructure that maintains our way of life?

Introducing…the Internet

The modern globalised economy is complex and highly interdependent. A great expansion of international trade has occurred throughout the late 20th Century, facilitated by the rise and rise of modern telecommunications technologies (Hite & Seitz, 2016). Without the steady uptake of radio devices during the two world wars or the proliferation of mobile cellular technology and the spread of wireless internet systems, the world would likely be a startlingly different place. By the early 21st century roughly 650 million people were using the internet – a growth of nearly 600% over the preceding 5 years (Hite & Seitz, 2016). The latest census on Australian activity by the Australian Bureau of Statistics (2018) found that broadband subscribers totalled 14,720,000, and the total volume of data downloaded had risen steadily, as **Fig. 1** shows. Any disruption will therefore have a widespread impact on the populace.


Broadband internet subscribers and volume of downloads, June 2011 to June 2018

Source: Australian Bureau of Statistics, Internet Activity, Australia June 2018

Social media and rapid information sharing have become the internet's poster-children, but they are just the tip of the iceberg. As Hite & Seitz (2016) describe, the internet now links the world. It has become a keystone in the archway of our modern industrialised world, a part of the progress trap we have laid for ourselves; there is no turning back from it and we are made vulnerable by our obligate mutualism with it. The internet has in particular facilitated a compression of time and space: instability in the Middle East can affect global oil prices in minutes; transgressions by corporations or politicians can be unearthed and dissected in real-time worldwide; the weather forecast for any town thousands of kilometres away is available at the tap of a finger. However, it is not just the extent of usage that makes the internet significant: after all, more than a third of the worlds population – at least – is not yet connected to the internet (International Telecommunication Union, 2020). The importance of the internet also lies in the indispendable nature of many of its applications.

The Victoria State Government (2020) defines the communications sector as enabling "*all internet, phone, radio, television and online transactions that involve the exchange of data and information through interconnected telecommunications networks*" (p.16). Despite being posed as separate functions (i.e. radio *and* internet *and* phone use), these activities are increasingly predicated on and intertwined with internet availability. The proliferation of radio and telecommunication infrastructure since 1980, for example, has been driven in part by our need to facilitate wireless internet transmission via radio waves (ACMA, 2015). ‘Online’ transactions, of course, occur over the internet. Lastly, in 2018, 90% of Australians were using their phones to access the internet (Infrastructure Australia, 2019) and in 2020 we have seen the necessity of online telecommunication to commercial persistence. What this represents, as the audit by Infrastructure Australia (2019) makes clear, is a fundamental change to the way we live, work and do business, with telecommunications taking centre stage. This is evident in such examples as the ubiquity of Global Positioning System (GPS) use; the collection, coordination, and collaborative analysis of climate data for initiatives such as the Global Climate Observing System (GCOS); or the efforts to catalogue biodiversity change by the International Union for Conservation of Nature’s (IUCN) Red List. **Fig. 2** presents some key metrics that demonstrate the extent of our internet reliance. Aside from enabling a huge volume of today’s economic and social activity however, the internet is inreasingly involved in the provision of many of our essential services through the advances in big-data, ‘cloud’ storage, and the Internet of Things (IoT) (IoT Alliance Australia, 2016).

The IoT is the infrastructure of interconnected objects, systems, information resources, and people together with intelligent services to allow them to share and process information (Heydon, 2015). This has led not just to smart phones or homes, but smart warehouses, manufacturing plants, and farms (PwC, 2018). Examples of IoT include:

- automatic notification by vehicles to emergency service organisations of serious road accidents
- tracking of assets such as fleet vehicles, trucks, ships, trailers, containers and equipment
- security and surveillance systems
- monitoring of smart meters by electricity, gas and water utilities

- monitoring and coordination of wastewater treatment

Thus, any threat to the security of the internet is by neccessity also a threat to the security of water supply, food provision, energy production, and human safety. The integration of the IoT will only grow over coming years, with the market size for the hardware components alone valued by PwC (2018) at $6.1bn by 2021. Many of these IoT applications are also gaining traction as solutions for sustainability problem-areas such as energy and food production. Systems for ongoing real-time monitoring and data collection have become indispensable to modern farming. Abioye (2020) describes how the combination of unmanned drones and machine learning is providing a data-driven agricultural technique that maximizes output while minimizing input for small and developing countries. Similarly, decentralised peer-to-peer energy sharing networks facilitated by IoT platofrms such as Solshare in Bangladesh or RedGrid in Australia have garnered global attention. The more we place our time and effort into technologically-based climate-change responses such as these, the more we stand to lose if the security of the internet is compromised. Though the internet itself is intangible, it arises from physical infrastructure. So what exactly are its physical supports – what is it one refers to when considering the infrastructure of the internet – and what are they vulnerable to?

Embodying the Internet

In essence, this infrastructure network is made up of physical links that carry communication data traffic around the world. The main components could be summarised as follows:

- Copper cable networks
- Fibre-optic cable networks and Hybrid fibre-coaxial networks
- 3G and 4G technology (particularly mobile telephone and wireless internet towers)
- 5G technology
- Satellite and base stations
- Exchanges, or points of interconnection
- Data centres
- Intercontinental submarine cables

Fibre conduits form the bulk of the network and are deployed overland as well as under the ocean. Submarine cables provide communication connectivity between continents: these conduits are afforded the most weather resistant materials and design protocols we are currently capable of, with a large amount of protective sheathing to keep seawater out (Durairajan, Barford, & Barford, 2018). Nearer land they are thick and trenched below the marine terrain but deeper out they are much thinner and usually not trenched. Typically, these are not thought to present a vulnerability to the system, though this may change in the future. Submarine cables have been severed by undersea landslides in the past: in a warming ocean, frozen slopes will thaw, and landslides and avalanches could become a greater hazard to deep-sea fibre (Barford, 2018). Some of Australia's key submarine cable connections are shown below in **Fig. 3**.

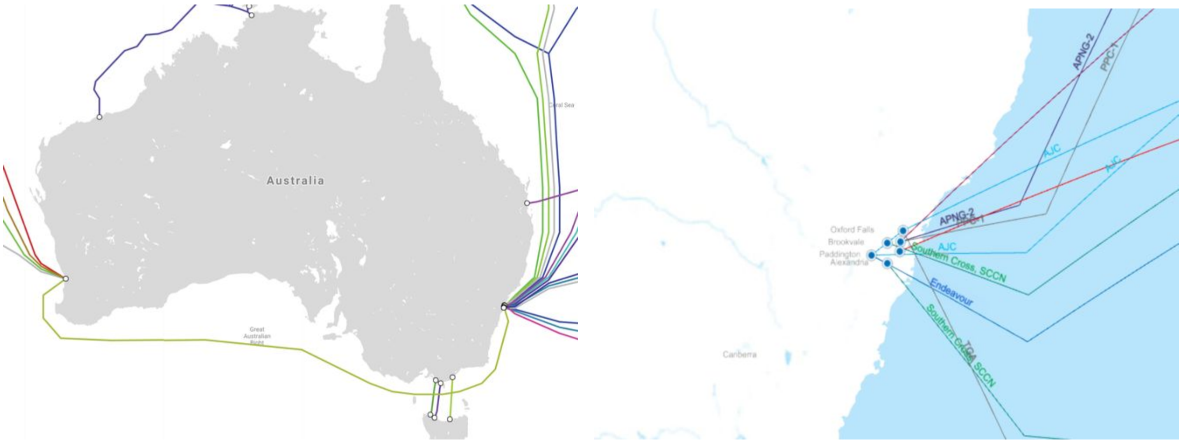


*Figure 4: **Left**: An overview of Australia's submarine cable landing points Adapted [reprinted] from The Submarine Cable Map. **Right**: A detailed view of Telstra managed submarine cable assets and their landing points throughout Sydney (right). Adapted. [reprinted] from Telstra Global*

Overland cables meanwhile are not built to the same superlative standards and are simply trenched under a shallow layer of earth – usually along public causeways or roads of some kind (Durairajan et al., 2018). Thus, they are more vulnerable to any saline ingress, water exposure or heat stress that may fall outside the mean. These cables distribute traffic from the submarine cable landing points in a widespread network throughout a region, connecting to points of presence (PoP's), nodes, data centres and transmission towers. This network is constantly growing. Current installement of 5G technology will require higher densities of towers and PoP's both to enable the use of higher radio frequencies and to address the higher traffic loads (Infrastructure Australia, 2019). Likewise, the rise of IoT systems and the expanding take-up of cloud computing services in Australia will drive a massive increase in the number of centres required to facilitate the transfer and storage of data, as well as a growth in physical links (Heydon, 2015). The cloud, data, and M2M processes that the ACMA (2015) describe as necessary for the IoT in **Fig.** 4. require a substantial physical network for their operation. This is illustrated by current estimates of the size of the 'digital universe' as 44 trillion gigabytes: six and a half stacks of 128GB iPads reaching from earth to the moon, a volume that will continue growing (Heydon, 2015). One consequence is that just as much as the

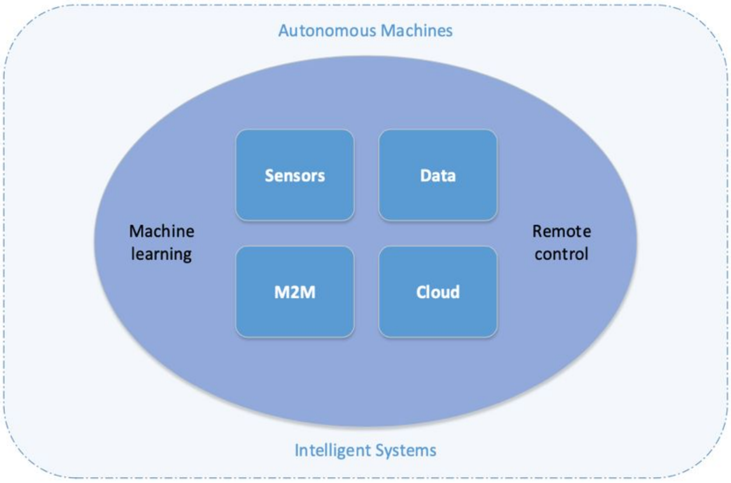


*Figure SEQ Figure * ARABIC 5: Components necessary for IoT: three out of four of these (data, cloud, and M2M) require dedicated infrastructure points. Adapted [reprinted] from ACMA (2015).*

internet is at risk from climate-change, and just as much as it has enabled efforts to combat climate-change, it has also been a contributing force to climate-change. The vast expanses of infrastructure required, and the rapid growth in its usage have made the internet an emissions producing behemoth in its own right. Operating data centres alone produces a carbon footprint equivalent with the airline industry, consuming 3% of global energy supply; growth in this area is not sustainable beyond the coming 10 – 15 years (Bawden, 2016). The manufacture of 'smart' devices also has an environmental toll, contributing significantly to the expected 14% of global emissions that the telecommunications industry will be responsible for by 2040 (Patel, 2018). The internet is, in a sense, at risk from its own balloning success. Whether or not these contributions can be reduced, it is clear that the internet is a point of serious vulnerability for our society. Like other infrastructure, these large volumes of internet infrastructure will be exposed to risks from a changing climate. These may be slow and diffuse such as increased weathering of materials, or rapid and acute such as from extreme weather events.

Threats from fire and heat

Infrastructure elements located above the ground such as masts, antennae, overhead wires, cables and transmission towers are at risk from precipitation, wind, unstable ground conditions, heat, fire, and more. In Australia, the risks posed by wildfires are one of the most pertinent. Scientific assessment has concluded that increased risk of fires, including extreme fires, can be expected as a consequence of climate change – particularly in Australia (Abram, 2020). In many parts of the world, fire seasons are increasing – so too the frequency of long fire weather events (Harris, Tapper, & Mills, 2019). Concerning the various influences on fire potential, temperature is of great relevance. Extremely high temperatures are increasingly frequent, while extremely low temperatures are decreasing (Steffen et al., 2011). Thus, even without a fire breaking out, infrastructure is already threatened by such record high temperatures and increased frequency of heatwaves (VicRoads, 2015). Data centres require air conditioning to prevent overheating and system failure - during Perth's third hottest day on record in 2015, iiNet services collapsed due to failure of both the main and backup air-conditioning systems (iTNews, 2015). High temperatures also tend to increase vapour pressure deficit (VPD), which, combined with high radiation and wind speeds, increases evaporative demand and causes drying of the landscape, increasing fire risk (Abram, 2020).

The severity and spread of wildfire incidence also seem to be changing, which will increase the risk potential for internet infrastructure. For example, the western USA has seen a doubling in volume of area burnt during wildfires, and Australia has seen a roughly 170% increase in fire occurrence in Victoria between 1972- 2014, with 25% of this attributed to changes in climate (Harris, Tapper, & Mills, 2019). In Australia, the Forest Fire Danger Index registered above '25' ten times in the 15 year period between 2002 – 2017; as compared to only five times between the 30 year period 1972 – 2002 (S. Harris, Mills, & Brown, 2017). This trend can be seen below in **Fig.** 6. A recent example,Australia's 'Black Summer' fire season of 2019 – 2020, was unprecedented in its extent and impact. More than 23% of south-eastern Australia's temperate forest were burned as a result. (Abram, 2020). This led to 5.1 km of copper cable and 8.8 km of optical fibre cable that needed to be replaced as well as damage to other enabling infrastructure. A resulting 888 outages of more than four hours occurred (ACMA, 2020), seen in **Fig. 7**, across various states. The total financial cost in economic losses and damage of these fires (to all infrastructure) was upwards of AUD $150bn (Resilience 360, 2020).

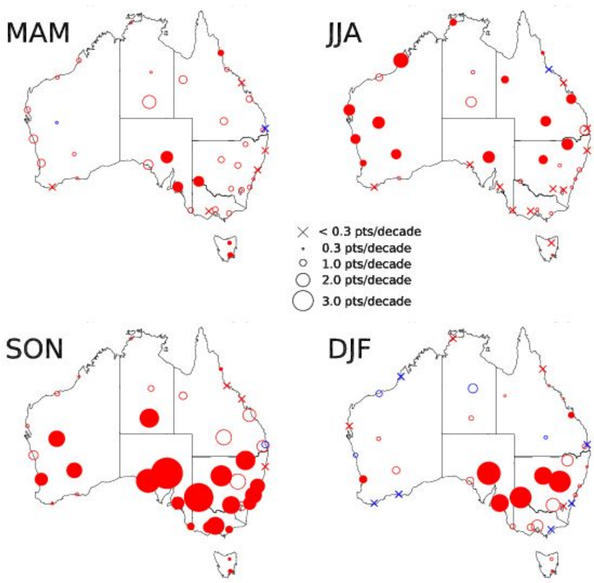
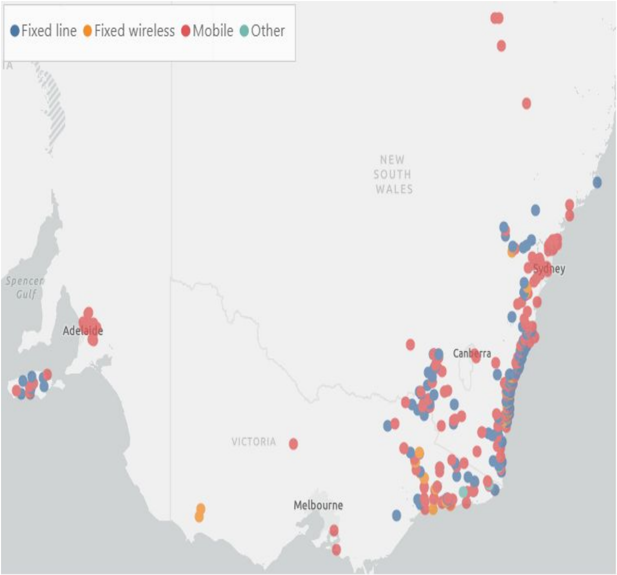


*Figure SEQ Figure * ARABIC 7: Trends in seasonal 90th percentile FFDI. Adapted [reprinted] from Harris and Lucas 2019*

*Figure SEQ Figure * ARABIC 6: Outage incidents, by location and network type. Adapted [reprinted] from ACMA (2020)*



These outages were caused primarily by power outage rather than direct fire damage. This is in line with recent work by Anderson (2020) establishing that the primary risk to cellular communication was not equiptment damage but power outage. However, **Fig. 7** shows only resolved outages – at the end of the ACMA review period there were still 39 ongoing outage incidents. A much larger portion of these were caused by direct fire damage and other physical damage to downstream or upstream facilities in the network, indicating that fire damage has longer lasting impacts. Additionally, the changing nature of fire incidence in Australia features increased complexity and variability – past trends may no longer accurately predict future trends. For example, an unprecedented number of violent pyroconvective storms during *Black Summer* was recorded, and this pyroconvective risk is believed to be increasing (Harris, Tapper, & Mills, 2019). This brings a different potential for infrastructure damage as well as for the impedence of broadband signals by thermal bubbles in fire areas (Boan, 2009; Mphale, Heron, & Verma, 2007).

Threats from water

Infrastructure elements above and below ground are vulnerable to flooding and sea-level rise as well as storm surges. Those elements below ground are additionally threatened by rising water tables, water ingress, and subsidence caused by drought or flooding.

The increasing temperature of the oceans has lead to thermal expansion and the thawing of glaciers and ice caps, bringing sea-levels up: this gradual rise may lead to the evacuation of some coastal cities around the world (Hite & Seitz, 2016). Low-lying coastal infrastructure points may be impacted by closure or reduced access from permanent or temporary flooding (Guze & Kołowrocki, 2017): submarine cable landing points are a prime example. Research by Durairajan et al. (2018) found that within the next 15 years, 4,067 miles of fibre conduit and 1,101 nodes (PoP's and colocation centres) would be submerged by water. Even before inundation however, there are likely to be noticeable impacts. Guze and Kołowrocki (2017) find that telecommunications infrastructure would be exposed to increased saline ingress and possibly amplified corrosion. Sea-level rise may also impact our telecommunications sector in the absence of physical damage to our infrastructure. Island nations are at particular risk of sea-level inundation, including Australia's neighbours in South-East Asia. Catastrophic human impacts aside, the inundation of locations such as the Solomon Islands would entirely void the billions of dollars of investment Australia has put into projects such as the Coral Sea Cable System.

The increased thermal energy in the oceans combined with changes in temperature are allowing for higher peak wind speeds and heavier precipitation events, leading to an increase in the intensity of extreme weather events like hurricanes. Severe storms in 2012 took down Amazon's Elastic Compute Cloud service, briefly knocking out Instagram and Netflix. Verizon learned a hard lesson that same year when Hurricane Sandy wreaked significant damage on their Lower Manhattan infrastructure: kilometres of cable were submerged by storm water, and one cable vault suffered 'catastrophic' failure (Bogle, 2015). Australia's precipitation and storm patterns will have a varied response to climate change: dryer regions getting drier and wetter regions getting wetter (MDBA, 2019). In areas with increased total precipitation or with less frequent but more intense severe precipitation events, the regular operation of the telecommunications sector is likely to be impacted by flooding of underground facilities or assets that are located in flood plains and urban environments i.e. data centres and exchanges (Guze & Kołowrocki, 2017). Importantly, it’s not clear that current storm infrastructure criteria are suitable in an era of non-stationary climate trends (Markolf, Chester, Helmrich, & Shannon, 2020). Thus, increased maintenance and repair of internet infrastructure will be neccessary to ameliorate degredation from longer-term water exposure (VicRoads, 2015). Floods are Australia’s most expensive extreme weather phenomenon – the exposure of internet infrastructure to water hazards as demonstrated by Durairajan et al. (2018) means this sector is likely to see increasing costs and service failures. This was borne out in 2011 during intense flooding throughout Queensland that caused severed overland fibre cables and inundated exchanges.

A cursory case study

Physical vulnerability of internet infrastructure has been discussed above but as **Fig 8.** shows, this is just one element of risk.

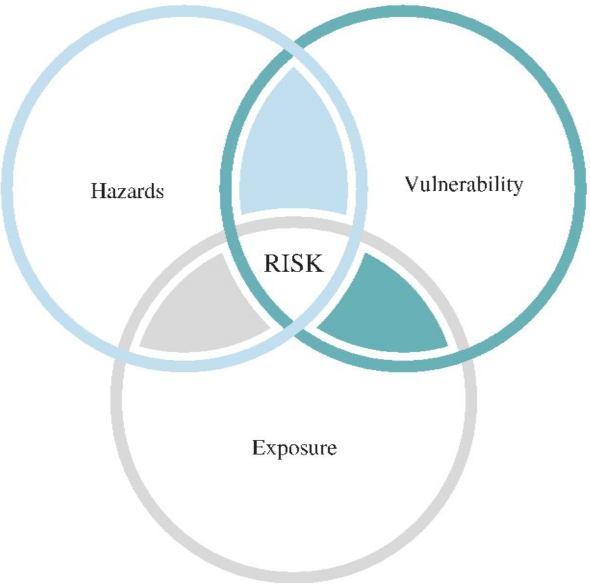


*Figure SEQ Figure * ARABIC 8: Delineating commonly assessed elements of risk*

To make a proper assessment of infrastructure vulnerability, it is necessary to quantify the extent of relevant hazards and the exposure of assests to those risks (Environment and Communications References Committee, 2018; Guze & Kołowrocki, 2017). In this context, a method such as the GIS overlay analysis utilised by Durairajan et al. (2018) has shown itself to be valuable. Executing such a methodology for this research was prohibitive due to the inaccessability and cost of the relevant data. However, a similar exercise has been conducted to assess the risk posed by sea-level rise and inundation. Although less rigourous, it provides beneficial real-world insight into the risk of climate change to Australia's internet infrastructure and is indicative of the sort of future research required.

Methods

Using publicly available information from online resources DataCenterMap.com and Telstra Global's network infrastructure map, the location data centres in Sydney, NSW were collated. These addresses were looked up and manually superimposed over interactive maps from Coastal Risk Australia to discern the exposure of this infrastructure to sea-level rise and inundation under a 'High' predicted inundation scenario for the year 2100.

Results and Discussion

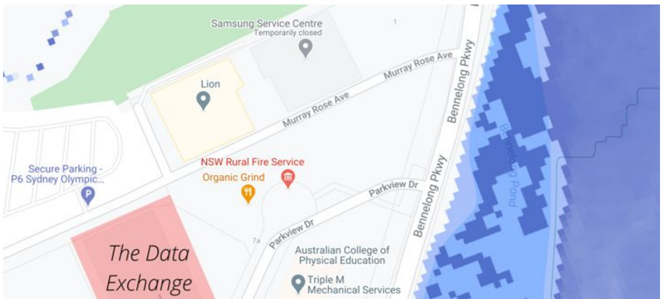
The findings are presented in **Table 1.** Of the 27 sites examined, three were found to be in locations that would be under water. A further seven were outside of, but within a short radius of, the flood-risk area, as seen in **Fig. 9**. These should still be given consideration because their proximity is close enough that issues discussed previously such as storm surge and ingress could reasonably be considered relevant risks.

Table 1: Correspondence of Sydney data centres with sea-level rise by 2100

1-12 Templar Road Digital Realty	Outside of coastal flood-risk area	Outside central Sydney
13-23 Templar Road Digital Realty	Outside of coastal flood-risk area	Outside central Sydney
Metronode Sydney 1 < 10km CBD	Unknown	Inside central Sydney
AmazeDC S1 Amaze 2/340 George ST	Outside of coastal flood-risk area (<5km)	Inside central Sydney
NEXTDC S1 4 Eden Park Road	Outside of coastal flood-risk area	Outside central Sydney
AAPT 187 Thomas Street	Outside of coastal flood-risk area	Inside central Sydney
IC1 Sydney CBD Macquarie Data Centres 477 Pitt St	Outside of coastal flood-risk area	Inside central Sydney
iseek Communications 5 Broadcast Way	Outside of coastal flood-risk area	Inside central Sydney
IC 2 Macquarie Park Campus Macquarie Data Centres 17-23 Talavera Road	Outside of coastal flood-risk area	Outside central Sydney
IC 3 Macquarie Park Campus Macquarie Data Centres 17-23 Talavera Road	Outside of coastal flood-risk area	Outside central Sydney
DCI Sydney Huntingwood	Outside of coastal flood-risk area	Outside central Sydney
Metronode 2 Silverwater 2128 <20km CBD	Inside coastal risk area	Inside central Sydney
Global Switch 400 Harris Street	Inside coastal risk area	Inside central Sydney
TechFlow Services 400 Harris St	Inside coastal risk area	Inside central Sydney

Datacom at AirTrunk Sydney 2148 Sydney	Outside of coastal flood-risk area (<5km)	Outside central Sydney
Pacnet 133 Liverpool Street	Outside of coastal flood-risk area	Inside central Sydney
Equinix IBX SYD1 Mascot 2020	Unknown	Inside central Sydney
AAPT 30 Ross Street	Outside of coastal flood-risk area	Outside central Sydney
Syncom Australia Pty Ltd Unit 17, 39 Herbert St	Outside of coastal flood-risk area	Outside central Sydney
Interactive Pty Ltd Tower B, 39 Herbert Street	Outside of coastal flood-risk area	Outside central Sydney
Australia Sydney 1 Data Center NTT Communications Corporation 2745 Sydney	Outside of coastal flood-risk area	Outside central Sydney
Keppel Data Centres 3 Broadcast Way, Artarmon	Outside of coastal flood-risk area	Outside central Sydney
Vocus Communications 59 Doody Street	Outside of coastal flood-risk area (<5km)	Inside central Sydney
The Data Exchange Network 5 Parkview Drive, Olympic Park	Outside of coastal flood-risk area (<5km)	Outside central Sydney
PIPE Networks Limited 2 Park St, Level 13	Outside of coastal flood-risk area (<5km)	Inside central Sydney
Vocus Communications 12 Brookhollow Avenue, Norwest Business Park	Outside of coastal flood-risk area (<5km)	Outside central Sydney
Metronode Illawarra 1 2526 Unanderra	Outside of coastal flood-risk area (<5km)	Outside central Sydney

A remaining 15 locations were found to be outside of the flood-risk area and are unlikely in this context to be at risk from sea-level rise. The final two locations could not be identified. For security reasons, some data centres do not publish their addresses. It should be noted that, although their exact location is



unkown, the suburbs for each were available. Both these suburbs were within central Sydney, adjacent or in close proximity to boundaries of identified flood-level risk. Thus, they should be considered as potentially vulnerable. As previously mentioned, impacts of climate-change can be both short or long term, acute instances or diffuse trends. Those data centres not directly at threat from sea-level rise may still be impacted by short-term extrems like flooding or intense rainfall, or long-term trends like ingress, corrosion and disrepair from accompanying changes in temperature and water exposure.

*Figure SEQ Figure * ARABIC 9: An example of the analysis process. This data centre facility, The Data Exchange Network, is one that does not sit under the projected extent of sea-level rise by 2100 (shown in blue pixels).*

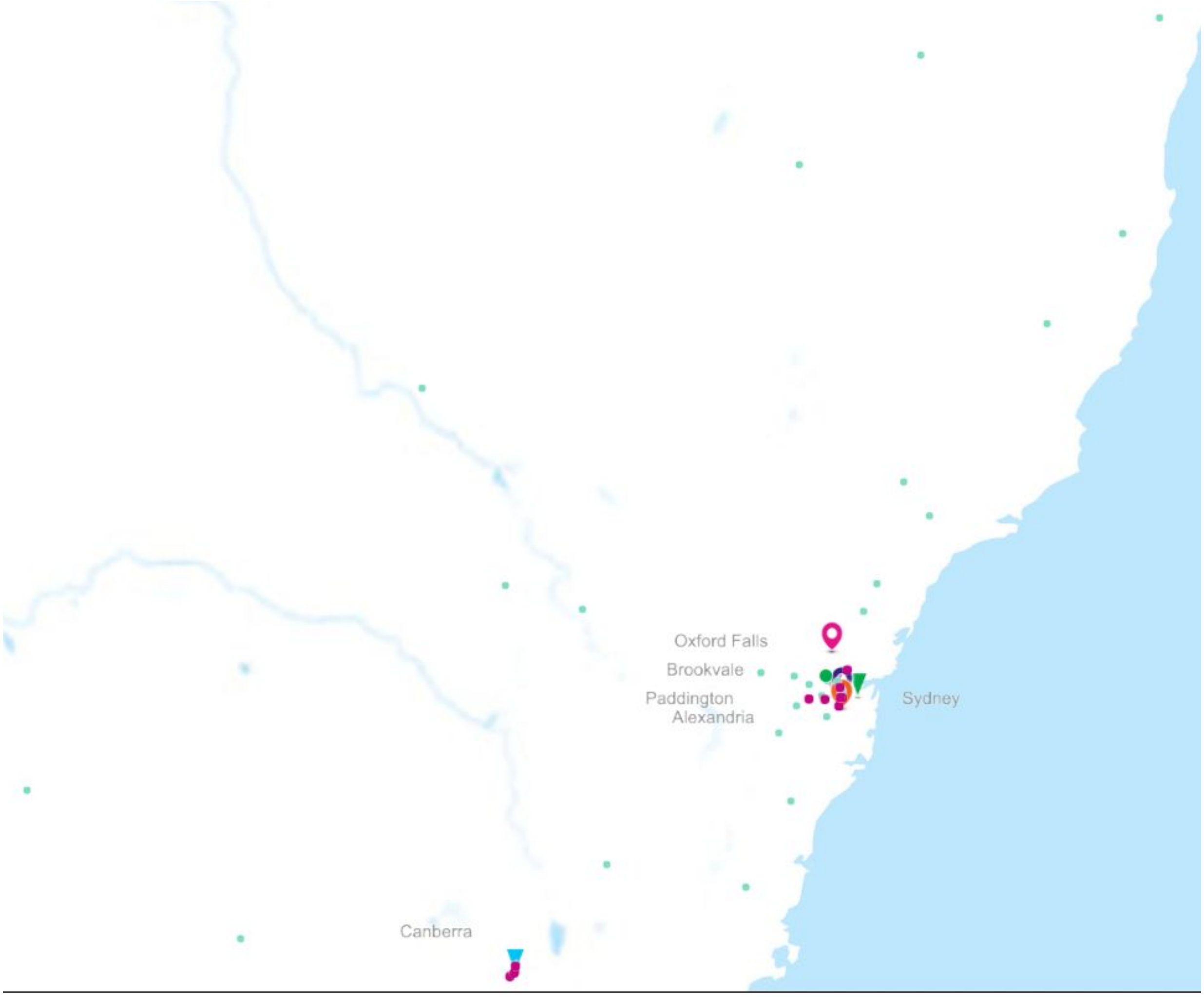


Figure 10: PoP's, data centres, and other nodes in Telstra's NSW network

Lastly, it is important to recognise that this brief analysis looked only at data centres, and that these locations may not be an exhaustive list even of that single category of infrastructure points. As can be seen from a view of Telstra infrastructure in **Fig. 10,** there are many instances of physical internet infrastructure besides data centres alone, and in many locations across the region.

Implications

Climate-change poses a varied and complex set of risks to the internet. Firstly, it is clear that long-term trends are likely to have a lasting impact on the persistence of structures because of changes like increased temperature. NCAARF (2018) demonstrates that infrastructure from all sectors faces additional and costly repair and maintenance work as a direct result of climate-change. Secondly it is also clear that aside from average climate trends, extreme weather poses an immense risk to telecommunications networks. While this paper has looked at various threats in isolation, the examined literature indicates that the greatest hazards are likely to be from a concatenation of climate pressures. The combined impact of drought, wildfire fires and extremes of temperature have a significant impact on energy generation and distribution required to maintain internet provision. Likewise, the combined impacts of sea-level rise with extreme precipitation events and storm surge will impact low-lying coastal infrastructure that supports the operation of the internet. The performance of telecommunications infrastructure can be very unpredictable when under stress and its interconnected nature means that damage or compromise of a key element (i.e. a node or exchange) can cause a cascading service failure (ACMA, 2020). The integration of the internet in various critical public and private activities across national boundaries and across diverse sectors indicates that any disruption is likely to have far-reaching and severe consequences.

Bridle (2018) explores a kind of future in which measures to ration internet use may eventuate, and where the most vulnerable are left behind withou access to critical aspects of the modern developed world. Many would balk at such a future – especially in the context of a culture in which unfettered internet access is now considered a right, as Bawden (2016) accurately explains. However, it it is crucial to recognise that this may happen anyway, like it or not, in the event that infrastructure is sufficiently impaired. To move forward it is important that we engage with this possibility. Unfortunately, as Guze and Kołowrocki (2017) explain, the evidence base for this topic is extremely limited – quantified studies are nearly non-existent. Further research is critically important to identify the risks and available responses. In particular the sort of spatial analysis attempted here and demonstrated by Durairajan et al. (2018) would be of great benefit for many of the aforementioned risks. As discussed, the internet is both a contributor to, and a possible victim of, climate-change. Therefore it is important that in moving forward, ambitious mitigation strategies are pursued while at the same time consideration is given to forward-thinking adaptation measures. Such a strategy would provide the best way to secure the future of the internet.

Reference List

Abioye, A. (2020, September 21, 2020). *An RGB sensor-based aerial robotic platform for sustainable precision agriculture.* Paper presented at the 2020 International Conference on Sustainable Development, Multiple.

Abram, N. J. H., B.J.; Gupta, A.S.; Lippman, T.J.R.; Clarke, H.; Dowdy, A.J.; Sharples, J.J.; Nolan, R.H.; Zhang, T.; Wooster, M.J.; Wurtzel, J.B., Meissner, K.J.; Pitman, A.J.; Ukkola, A.M.; Murphy, B.P.; Tapper, N.J.; Boer, M.M. (2020). *Connections of climate change and variability to forest fire disasters in southeast Australia*. Journal Article.

ACMA. (2015). *The Internet of Things and the ACMA's areas of focus: Emerging issues in mediaand communications Occasional paper*. Retrieved from Melbourne: https://www.acma.gov.au/sites/default/files/2019-08/Internet%20of%20Things_occasional%20paper%20pdf.pdf

ACMA. (2020). *Impacts of the 2019–20 bushfires on the telecommunications network: Report for the Minister for Communications, Cyber Safety and the Arts*. Retrieved from Australia: https://www.acma.gov.au/publications/2020-04/report/impacts-2019-20-bushfires-telecommunications-network

Anderson, S. B., C.; Barford, P. (2020). *Five Alarms: Assessing the Vulnerability of US Cellular Communication Infrastructure to Wildfires*. Paper presented at the Proceedings of the ACM Internet Measurement Conference, Virtual Event, USA. https://doi.org/10.1145/3419394.3423663

Australian Bureau of Statistics. (2018). Internet Activity, 2018. Retrieved from https://www.abs.gov.au/statistics/industry/technology-and-innovation/internet-activity-australia/latest-release#data-download

Barford, C. (2018). Key Internet Connections and Locations are at Risk from Rising Seas: Maps that combine projections of sea-level rise with networks of internet infrastructure show extensive flooding within decades. *American Scientist, 106*(6), 348-352.

Bawden, T. (2016). Global warming: Data centres to consume three times as much energy in next decade, experts warn. *The Independent*. Retrieved from https://www.independent.co.uk/environment/global-warming-data-centres-consume-three-times-much-energy-next-decade-experts-warn-a6830086.html

Boan, J. A. (2009). *Radio propagation in fire environments.* Retrieved from https://digital.library.adelaide.edu.au/dspace/bitstream/2440/58684/8/02whole.pdf

Bogle, A. (2015). Will climate change burn up the internet? Retrieved from https://grist.org/climate-energy/will-climate-change-burn-up-the-internet/

Bridle, J. (2018). *New dark age : technology, knowledge and the end of the future*: London Brooklyn, NY : Verso.

CSIRO. (2007). *Infrastructure and climate change risk assessment for Victoria: Report to the Victorian Government.* Melbourne: Victorian Government.

Durairajan, R., Barford, C., & Barford, P. (2018). *Lights out: Climate change risk to internet infrastructure.* Paper presented at the Proceedings of the Applied Networking Research Workshop.

Engelman, R. (2013). Beyond Sustainababble [Chapter 1]. In E. Assadourian, T. Prugh, SpringerLink, & L. Starke (Eds.), *State of the world 2013: is sustainability still possible?* (pp. 3-16). Washington, DC: Island Press.

Environment and Communications References Committee. (2018). *Current and future impacts of climate change on housing, buildings and infrastructure.* Canberra: Commonwealth of Australia.

Guze, S., & Kołowrocki, K. (2017). EU-CIRCLE: A pan-European framework for strengthening critical infrastructure resilience to climate change Project taxonomy and methodology: Resilience terminology and methodology. *Journal of Polish Safety and Reliability Association, 8*.

Harris, S., Mills, G., & Brown, T. (2017). Variability and drivers of extreme fire weather in fire-prone areas of south-eastern Australia. *International Journal of Wildland Fire, 26*(3), 177-190. doi:10.1071/WF16118

Harris, S. L., C. (2019). Understanding the variability of Australian fire weather between 1973 and 2017. *PLoS ONE, 14*(9). doi:10.1371/journal.pone.0222328

Harris, S. N., N.; Tapper, N.; Mills, G.; . (2019). The sensitivity of fire activity to interannual climate variability in Victoria, Australia. *Journal of Southern Hemisphere Earth Systems Science, 69*(1), 146-160.

Heydon, G. Z., F. (2015). *Enabling the Internet of Things for Australia: Measure, Analyse, Connect, Act*. Retrieved from Australia:

Hite, K., & Seitz, J. (2016). The Environment: Part 1. In K. Hite, & J. Seitz, *Global Issues: An Introduction Fifth Edition.* West Sussex: John Wiley & Sons.

Infrastructure Australia. (2019). *Telecommunications*. Retrieved from Canberra: https://www.infrastructureaustralia.gov.au/australian-infrastructure-audit-2019-telecommunications

Intergovernmental Panel on Climate Change. (2019). Climate change and land: an IPCC special report on climate change, desertification, land degradation, sustainable land management, food security, and greenhouse gas fluxes in terrestrial ecosystems. Retrieved from https://www.ipcc.ch/srccl/

International Telecommunication Union. (2020, 1/11/2020). Individuals using the Internet (% of population). Retrieved from https://data.worldbank.org/indicator/IT.NET.USER.ZS

IoT Alliance Australia. (2016). *Seizing the Internet of Things opportunity for Australia*. Retrieved from Sydney: https://www.iot.org.au/wp/wp-content/uploads/2016/12/Seizing-the-Internet-of-Things-Opportunity-for-Australia.pdf

iTNews. (2015). iiNet's Perth data centre melts in heatwave. Retrieved from https://www.itnews.com.au/news/iinets-perth-data-centre-melts-in-heatwave-399128

Markolf, S. A., Chester, M. V., Helmrich, A. M., & Shannon, K. (2020). Re-imagining design storm criteria for the challenges of the 21st century. *Cities*, 102981. doi:https://doi.org/10.1016/j.cities.2020.102981

Mphale, K., Heron, M., & Verma, T. (2007). Effect of wildfire-induced thermal bubble on radio communication. *Progress in Electromagnetics Research (PIER), 68*, 197-228.

Murray–Darling Basin Authority (2019). Climate change and the Murray–Darling Basin Plan: MDBA Discussion Paper. Retrieved from: https://www.mdba.gov.au/sites/default/files/pubs/Climate-change-discussion-paper-Feb-19.pdf

Murray, V., & Ebi, K. L. (2012). IPCC special report on managing the risks of extreme events and disasters to advance climate change adaptation (SREX). In: BMJ Publishing Group Ltd.

Patel, P. (2018). Smartphones are warming the planet far more than you think. Retrieved from https://www.anthropocenemagazine.org/2018/04/the-energy-hogging-dark-side-of-smartphones/

NCCARF. (2018). *Infrastructure. Synthesis Summary 8.* Gold Coast: National Climate Change Adaptation Research Facility. Retrieved from https://www.nccarf.edu.au/sites/default/files/attached_files/Synthesis_Summary_Infrastructure_WEB.pdf

PwC. (2018). *Australia's IoT Opportunity: Driving Future Growth*. Retrieved from https://www.acs.org.au/insightsandpublications/reports-publications/iot-opportunity.html

Resilience 360. (2020). Unprecedented bushfires in Australia impact infrastructure and local supply chains. Retrieved from https://www.resilience360.dhl.com/resilienceinsights/unprecedented-bushfires-in-australia-impact-infrastructure-and-local-supply-chains/

Steffen, W., Persson, Å., Deutsch, L., Zalasiewicz, J., Williams, M., Richardson, K., . . . Svedin, U. (2011). The Anthropocene: From Global Change to Planetary Stewardship. *A Journal of the Human Environment, 40*(7), 739-761. doi:10.1007/s13280-011-0185-x

VicRoads. (2015). *Climate change risk assessment.* Melbourne.

Victoria State Government. (2020). *Victoria's Critical Infrastructure: All Sectors Resilience Report.* Melbourne: Victorian Government.