

## AJTDE Volume 2, Number 4, December 2014

### Table of Contents

#### Editorial

##### [Stepping down and handing over](#)

Peter Gerrand

#### Australia's digital skills

##### [Australia's digital skills for peace and war](#)

Greg Austin

#### NBN policy

##### [Critique of the new NBN policy: Lower cost, faster roll-out, access competition, technology independence, future proof?](#)

Graham Shepherd

##### [A closer look at Deep-fibre FTTdp \(fibre to the distribution point\)](#)

Craig Watkins and Kelvin Lillingstone-Hall

##### [Australia's fixed broadband deficit: Indecision around industry structure could entrench Australia's laggard broadband position](#)

Gary McLaren

#### Telecommunications and disaster management

##### [Telecommunications and disaster management: Participatory approaches and climate change adaptation](#)

Marta Poblet, Hartmut Fünfgeld and Ian McShane

##### [Cheap Deployable Networked Sensors for Environmental Use](#)

Alex Antunes

##### [Locating disaster communication in changing communicative ecologies across the Pacific](#)

Jessica Noske-Turner, Jo Tacchi, Heather Horst and Evangelia Papoutsaki

##### [Updating warning systems for climate hazards: Can navigation satellites help?](#)

John Handmer, Suelynn Choy and Naohiko Kohtake

##### [Acoustic Coupled Disaster and Remote Communications Systems](#)

Ulf Müller-Baumgart, Paul Gardner-Stephen, Andrew Bettison, Romana Challans and Jeremy Lakeman

[Warrnambool Exchange Fire – Resilience and Emergency Management](#)

Mark A. Gregory, Kaye Scholfield, Khandakar Ahmed, Dorothy McLaren, James Williams and Helen Marshall

The Internet of Things (IoT)

[How the Internet of Things changes everything](#)

Kate Carruthers

[Enabling Technologies for Effective Deployment of Internet of Things \(IoT\) Systems: A Communication Networking Perspective](#)

Jamil Y. Khan, Dong Chen and Oliver Hulin

Wireless communication

[Project-Based Management Technique for Radiofrequency Spectrum Planning and Allocation.](#)

[Part Two: The Project Management Plan](#)

Andrew J Kerans

History of Australian telecommunications

[The Victorian Time Signal Service](#)

Simon Moorhead

Back to the Future

[Big Data meets Big Fridge \(a frolic\)](#)

Edouard Estaunié

## Stepping down and handing over

---

Peter Gerrand  
Managing Editor

---

### Stepping down



This issue is the 80<sup>th</sup> edition of the Journal that I have produced as Editor-in-Chief since June 1994, either under the publication's former name of the *Telecommunications Journal of Australia* or under its new name, since November 2013, as the *Australian Journal of Telecommunications and the Digital Economy*. It is also my 30<sup>th</sup> edition as Managing Editor, since converting the Journal to its online format in 2007. And it will be my last, as I am now stepping down from the job.

Over those past 21 years, the Journal has done some justice to airing and initiating public debate on some critical national policy topics. Members of the Journal's Editorial Board made brilliant contributions in sourcing articles from leading experts – and in many cases wrote fine articles as experts themselves – on, for example:

- Network interworking in a competitive environment (1994-96)
- Inputs to the seminal 1997 telecommunications legislation
- Internet governance (since 1998)
- Structural separation of Telstra: rekindling the national debate in 2004
- Telecommunications for environmental sustainability (2007-2014) – see below
- NBN policy – debunking broadband fictions in 2010
- Identifying NBN policy gaps on end-to-end performance in 2011
- Media reform proposals in 2012-13
- Digital rights protection including privacy, sovereignty and security (2005-13)
- The potential of new broadband applications and services (2005-13)
- Telecommunications and disability (2010-2013) – see below

- Access, affordability and social value in telecommunications services (2010-14)
- Critiquing the Turnbull changes to NBN policy since first announced in April 2013.

One of the Journal's ongoing strengths, in a continuous tradition since its first appearance in 1935, has been its publication of timely articles by experts on promising new technologies. On my watch, we have tracked many of these, but in particular the evolution (and applications) of wireless communication, from AMPS and GSM to 5G, and broadband access techniques from ISDN via the DSL family to FTTN and FTTP; as well as innovations in fixed wireless and cloud computing. Furthermore journalist Liz Fell's series of interviews of industry leaders, spanning two decades from 1994 to 2013, has left a rich legacy for future historians of the industry.

Thanks to enlightened sponsorship by Alcatel-Lucent, the Journal was able to run an annual prize competition between 2007 and 2009 that produced many excellent papers on the application of telecommunications to sustaining the natural environment.

Generous sponsorship by Telstra enabled us to run an annual Christopher Newell Prize competition from 2010 to 2013, which produced a total of 19 valuable papers on the beneficial application of telecommunications to help people with disabilities.

From 2003 to 2010, the Journal worked closely with Mark Armstrong's Network Insight Institute (NII) to source substantial policy papers for publication in the Journal. This was especially so during the period 2005-2011 when NII organized its famous annual Communications Policy & Research Forum in Sydney, at which researchers and policy wonks from over six disciplines happily converged – often to debate convergence.

If I have two major regrets on national policy outcomes, they are firstly the failure of the Rudd and Gillard governments to effect reforms on media policy, despite having set the reform process in motion in 2012. My second regret is the failure of the Abbott government (to date) to develop any long-term vision for how a national Digital Economy can be created, underpinned by the National Broadband Network infrastructure they continue to fund, that would provide Australia with any internationally competitive advantage – and that would support a more inclusive, equitable, innovative and healthier society.

## Handing over

Fortunately for the Journal's readership, I am pleased to report that Dr Mark Gregory from RMIT University – already an experienced author and reviewer for this Journal, and a prolific columnist on NBN policy – has agreed to succeed me as Managing Editor.



**Mark Gregory**

Mark was profiled in my previous editorial as a new member of the Editorial Board.

He will be supported by the same talented and multidisciplinary Editorial Board that has helped me plan, source and review articles, and whose companionship has made being Managing Editor such an ongoing pleasure.

For the current December 2014 issue, I am indebted to our newest Board member Dr Marta Poblet for proposing the major theme of 'Telecommunications and disaster management', and for inviting her

colleagues Drs Hartmut Fünfgeld and Ian McShane from RMIT University's Centre for Urban Research to assist her as joint Guest Editors in sourcing and reviewing several valuable articles on this important and always timely and critical theme – especially for Australia.

I will continue as a member of the Editorial Board in 2015 to help keep the Journal well resourced with timely articles on telecommunications and the digital economy. And I am delighted to report that Blair Feenaghty has agreed to continue his now 21-year stint as Executive Editor. Blair has been my closest ally in producing the Journal since 1994, during times of both plenty and scarcity for the industry as a whole and the Journal in particular, and his contribution has been magnificent.

Furthermore Mark and Blair have been promised the same level of support and quality control by Graham Shepherd, the *Wunderwebmeister* of the Journal's platform, the TelSoc website. Without Graham's cheerful support it would not have been possible to create the new Journal in 2013 nor keep it flourishing and feature-rich.

*Peter Gerrand*

# Australia's Digital Skills for Peace and War

---

Greg Austin

East-West Institute (New York/Brussels/Moscow)

---

**Summary:** This article gives an overview of Australia's national military strategy for cyber space and the implied demands for a radical approach to development of our civil skills base. It then looks at developments in countries and groups of military interest to us in cyberspace. On this basis, the piece concludes with some recommendations for Australian policy.

## Introduction

The last inspirational speech by an Australian Prime Minister on the country's digital future was made seventeen years ago by Paul Keating, one year after the he left the job ([Keating 1997](#)). He offered a comprehensive view of the transformative power of the information revolution, touching on both a “thriving IT industry and an information-educated workforce” and the impact of those “on all our industries from farming to manufacturing to health care”. He said it would need “ideas and a strategic framework within which local and overseas businesses can operate” that would “accommodate and provide for a growing IT presence in our whole economy and society”. Above all, he said, “developing the information industry does mean developing our people”. This article is about that theme: the country's digital skills. It reviews the broad policy settings in Australia for development of our digital skills for strategic gain at the national level in peace and war. We desperately need renewed political leadership for our digital future.

A country cannot hope to have cyber talents for war if it does not develop them in peacetime, and if it does not have a strategy for transitioning these skills from the civil economy to military uses when emergencies dictate. Moreover, the enhanced development of military cyber skills and strategies has flow-on effects to civil economy. This virtuous circle of innovation — what might be called our information technology (IT) industry base — is weak and definitely needs help. As elsewhere, we need to attract more venture capitalists, nationality unimportant, and get their money into university-based and industry-based R&D for IT. Weaknesses in our cyber security situation in the civil sector (vulnerabilities everywhere) are not unique to Australia, but our inability to provide the skills base we need to overcome them, and a lack of industrial options to address them, must translate into great dangers for the country, not just in peacetime

(cyber crime from overseas that may go unnoticed and unpunished) but most especially in the risk of large scale cyber attack on our civil economy during wartime.

The article gives an overview of our national military strategy for cyber space and the implied demands of that for a radical approach to development of our civil skills base. It then looks at developments in countries and groups of military interest to us in cyberspace. On this basis, the piece concludes with some recommendations for Australian policy.

## The Civil Economy

The four Prime Ministers since Keating, to the extent that they even followed the issue of the digital world, have seen it more often as a threat than an opportunity. (To review all Prime ministerial speeches, see <http://pmtranscripts.dpmc.gov.au> and <http://www.pm.gov.au/>.) In 2011, the Gillard government released plans for a new White Paper focusing largely on cyber security (following a 2009 white paper on that subject), which it later said would have an expanded scope to look at the digital economy in the broad. The plan to expand its scope was announced by Julia Gillard as she closed a Prime Minister's *Forum on the Digital Economy* in October 2012. The resulting paper, *Advancing Australia as a Digital Economy* ([Dept of Communications 2013](#)), was an update to the National Digital Economy Strategy of 2011. Neither paper went much further than e-government, online access, the broadband network or small grants to ICT undertakings. Neither paper had any concept of IT education beyond providing online access. While the current Minister for Communications, Malcolm Turnbull, is engaged regularly and earnestly with a vision of Australia's digital future, in all of its dimensions, the country lacks political leadership across the board in this area of policy, especially for promoting ICT education and stimulating industry/university R&D linkages. The coalition's policy for the digital economy going into the 2013 election ([Coalition 2013](#)) did not address the main concerns raised by industry at the Forum a year earlier, notably a lack of software engineers, and lack of translation of advanced information technologies into key sectors like agriculture, education and health. Political leadership in Australia for the information society appears to have been captured by two narrow issues (the debate about national broadband infrastructure or online government), with occasional references to small grants for new spending on advanced ICTs for this or that sector.

Apart from needing political leadership, the country will need time to be able to reverse the slide in Australia's digital competitiveness since 2007 that the coalition policy document of 2013 noted. According to annual edition of the *Network Readiness Index* published by the World

Economic Forum, Australia slipped from a ranking of 9th in 2004 to 18th in 2013 and 2014 ([WEF 2004](#), [2013](#), [2014](#)). In 2014, the affordability of our access to network infrastructure was one of the most costly in the world (we were ranked at 49th with 1st being the least costly). Between 1999 and 2013, our annual corpus of new domestic student graduates in information technology (IT) fell by 46 per cent ([Dept of Education 2104a](#)), though there has been an upturn in the last two years. (This reference to IT graduates does not include electrical engineers which saw an increase.)

We have been able to compensate for the sharp decline in IT graduates in part by temporary ICT migrants to Australia, which in 2009-10 numbered 8,530 – double the number of our own IT graduates for that year ([ACS 2011](#): 27-28). (Data for later years does not allow a similarly granular comparison.) In terms of student satisfaction with our IT tertiary offerings, data for 2005 to 2012, the latest available, shows that the completion rate for students enrolled in information technology over the period was only 61 per cent, significantly lower than for any other of ten general categories of study ([Dept. of Education 2014b](#)). The real situation of Australia's digital economy and society is much more complex than these few statistical snapshots suggest, but these are useful, if disappointing reference points. The 2014 WEF report observed about Australia: "Compared with individuals, businesses and government are less dynamic in taking up ICTs" ([WEF 2014](#): p. 23). This decline in digital competitiveness has been accompanied by a loss of scholarly interest in the subject. A review of the literature on Australia and the digital economy or information society reveals a decline in the volume of material on this issue. In academia in Australia, the issue is more or less out of fashion, barring a few brave souls, "crying in the wilderness".

Australia's Chief Scientist, Professor Ian Chubb, observed in September 2014 that Australia is the only country in the OECD without a national plan for science, technology or innovation ([Chief Scientist 2014a](#)). In the report he released at that time, on *Science, Technology, Engineering and Mathematics: Australia's Future*, Chubb outline an education plan for education with 21 recommendations ([Chief Scientist 2014b](#): 20-22). These recommendations paint a picture of a country that is falling off the pace in education for a technological future. In a newspaper article that same month, he went further: "Where science is concerned, I must part company with some of our economists. To transform our nation, we need to facilitate innovation in science on a scale we've never achieved. That's too important to be left to chance, or to 'market signals'" ([theguardian.com 08/09/2014](#)). As our universities become more marketised

and privatised, Australia will need not just political leadership to maintain our civil skills base in IT, it will need radical policy measures.

In 1989, a rather prescient economist in Australia anticipated the long term trend. He wrote: the “service economy in Australia is petering out as it does not offer much scope for undertaking information-intensive projects that will expand output, income or employment, rapidly. The impact analysis also reveals conflicts between long term goals of structural change and short-term stabilisation goals of maximising income and employment. ([Karunaratne 1989](#): 473). While there have been clear advances, captured well in a 2014 report by Price Waterhouse Coopers ([PWC 2014](#)), development of our IT skills base is still hostage – a quarter of a century later – to an overriding political ethic of full employment and traditional notions of a work force.

## In War as in Peace

A country’s military capability and strategic planning cannot escape the general trend of development in its economy and human resources. While the civil sector can compensate for a 50 per cent drop in IT graduates by massive increases in work visas for non-nationals, the national security sector cannot. Australian citizenship is usually a requirement for the sector. The low penetration rate of IT professionals in all echelons of military and strategic planning, a symptom of our desultory outcomes in information technology education, produces defence policy that looks strangely out of step with the emerging digital realities.

Recent defence policy statements describing our national level posture barely touch on the subject of cyber warfare (dependent on advanced information aggregation, analysis, and rapid exploitation for strategic strike). Our latest White Paper ([Dept of Defence 2013](#)) gives cyber warfare a primarily defensive function akin to physical protection of military command and control (C2) networks and other systems from cyber attack. In very rough terms, this represents about one per cent of military reality in the information age. It is akin to “C2 plus cyber security” when in fact leading world powers are operating a C4ISTAR vision: command, control, communications, computers, intelligence, surveillance, target acquisition, reconnaissance – all enabling “strategic strike in milliseconds”. In Australia, key strategy documents at the national level pay almost no attention to concepts like “information operations” and the word “digital” rarely appears. Policy documents and procurement efforts of the single services are much closer to the international best practice.

The 2013 Defence White Paper recalled the agreement in 2011 between the United States and Australia that the ANZUS treaty would apply to cyber attacks. It concluded as a result that Australia needed “capabilities that allow us to gain an advantage in cyberspace, guard the integrity of our information, and ensure the successful conduct of operations.” It said that the “the net effect on Australia’s position will depend on how well we exploit cyber power”. It acknowledged that “Once deployed, our forces will need to operate as a networked force in a contested environment.”

But beyond these and other references to security against cyber attacks, there is little hint that the country has a deep appreciation of the revolutionary impact of the information age in military affairs. There are many references in the White Paper to things that might relate in the most general terms to the information revolution, and its authors might refer to these to rebut this criticism, but there is no strategy visible in it for “how we exploit our cyber power”, let alone build a force structure and a recruit base around it. (Navy recruiting has said it can’t fill its vacancies with suitably qualified people to operate many of the advanced electronic systems.)

By contrast, a paper by the Australian Army, Future Land Warfare Report 2014, reveals a highly sophisticated awareness of the realities of the information age ([Australian Army 2014](#)). Here are just several excerpts:

- “Current cyber defence capabilities have not kept pace with technological change”
- “The land, sea and air domains will become further entwined with the cyber, electromagnetic and space domains. These domains will be the subject of constant competition, with land force operations increasingly enabled (or disabled) by access to digital networks.”
- “A fully digitised force will depend on access to space-based capability for battlefield management, communications and precision navigation and timing (GPS, for example).”
- “To what degree is the Army prepared for an interconnected battle space in which deployed theatres are not quarantined from the homeland and force generation base?”
- “To what degree is the Army prepared to rebalance its force structure into non-traditional capabilities and units (such as boosting the capability of the intelligence battalion or adding an Army cyber capability) in order to build greater capacity for intelligence-led targeting?”
- “Is the Army willing to fundamentally change its traditional command, control and communication structures and processes, in particular the Army’s unit and formation

headquarters, to maximise the advantages of access to joint effects and the enhanced networking of digital systems?”

This last point (“jointness”) is of particular importance. Single service tactical systems in Australia are becoming more “cyberised”, and we can probably assume that our special forces are quite advanced, but the maximum potential gains in capability at the strategic level of war can only be realised if forces are organised for joint operations and if intelligence and reconnaissance are fully integrated with joint force commands which have a mission for strategic strike.

The gulf between the 2014 Army paper and the 2013 White Paper on cyber war is bridged somewhat by the Information Activities doctrine of the ADF, approved in November 2013 and later declassified ([ADF 2014](#)). This manual does not appear to embrace the high end, transformationalist view of cyber power. It limits itself to “information activities” that are “are defined as the integration, synchronisation and coordination of two or more Information-related capabilities (IRC) that generate and sustain a targeted information advantage”. The manual contains all of the right concepts, but manifests confusion at the top end of capability between what sounds like the public relations or propaganda aspects of information policy (“strategic communications”) and the main purpose of high end information operations which is “strategic strike” to defeat or deter an enemy.

The 2013 ADF doctrine is not clear on this bigger set of questions. It does not fill the gap identified ably in a 2007 analysis of Australian cyber warfare strategies written by Lieutenant Commander Chris Watson, a former Royal Navy officer then serving in the Royal Australian Navy ([Watson 2007](#)). Writing in the *Australian Army Journal*, he concluded: “The unresolved issue now is not so much how to integrate Information Operations into military operations, but rather how to persuade politicians and public servants to coordinate the efforts of their respective departments into a National Effects Based Approach so as to provide whole-of-government forward planning with the direction, legitimacy and promise of success a nation is entitled to expect” ([Watson 2007](#): 96). As just one example of the deficiencies, he mentioned that within Australia’s smaller intelligence community, “there remain significant changes to be made if Information Operations planners are to be provided optimal rather than ad hoc intelligence support” ([Watson 2007](#): 93). But he correctly identified the main problem as a lack of commitment to the cognitive aspect of information operations: changing how the enemy

leaders think by directly attacking their knowledge environment and command relationships by cyber and other means.

He said that one problem was that the Defence organisation was in danger of being swamped by the “transformationalist” approach (the idea that informatisation changes everything) that is now dominant in the U.S. doctrine ([Watson 2007](#): 93). The 2013 ADF doctrine on information operations borrows from U.S. doctrinal manuals, but does not in its totality reflect the core concept of cyber warfare as reflected in U.S. strategy or in emerging worldwide realities. One reason may be, as the Army publication mentioned above has suggested, that Australia is not ready to modernise its force structure to accommodate the changing reality of military affairs. There is little mention of the concept of cyber warfare or information operations in a 2012 Force Posture Review commissioned by Defence from two former Secretaries of the Department. Arguably, their terms of reference did not allow them the opportunity though the section of ADF capabilities might have been an obvious place to cover this ground.

## United States

Australia appears out of step with its principal ally, the United States, which has a military strategy premised on information dominance as the foundation for strategic strike. Our ally is investing heavily in military uses of cyberspace. In classic cyber war terms, this refers not just to the Internet, computers and networks, but also to conventional telecommunications networks on the one hand and, on the other, to processors and controllers in any automated system. “Cyber effect operations” in wartime seek to impair the confidentiality, integrity or availability of not just the machines but the data contained therein. This can include penetrating enemy intelligence systems and altering the information about one’s own forces or even information about the disposition of the opposing country’s forces. A Presidential Directive says that the United States will seek to apply “cyber effect operations” (COE) in all spheres of national activity affecting war, diplomacy and law enforcement ([United States 2012a](#)). It says that offensive COE (OCO) “can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging”.

But there is a deeper dimension to the concept of cyber war. It relates to the role of information and how a country’s military power and strategic impact in war can be magnified by cyber means. In November 2012, the U.S. Joint Chiefs of Staff issued a new joint training manual on “Information operations” ([United States 2012b](#)). It identified the information environment as

the aggregate of “individuals, organisations, and systems that collect, process, disseminate or act on information”. This is a strategic level orientation in which the United States aims above all else to disrupt the enemy’s decision-making as a prelude to and adjunct for kinetic operations: the integrated employment during military operations of information capabilities “in concert with other lines of operation, to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.”

One key element of U.S. military policy is its recognition in a 2011 “Department of Defense Strategy for Operating in Cyberspace” of the need to “Leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation” ([United States 2011](#): 11). In fact, this is one of the Department’s five principal strategies for cyberspace. While the United States is clearly in a different and superior league of cyber military power from Australia, we might learn from its plans for developing our cyber war skills. It makes the obvious commitment to catalysing new education opportunities in a situation of high and unmet) demand: “catalyse U.S. scientific, academic, and economic resources to build a pool of talented civilian and military personnel to operate in cyberspace”. But it says that its plans in this area of skill development will be paradigm changing and will include the private sector:

- streamline hiring practices for its cyber workforce
- exchange programs to allow for “no penalty” cross-flow of cyber professionals between the public and private sectors to retain and grow innovative cyber talent
- adoption and scaling of cross-generational mentoring programs
- the development of Reserve and National Guard cyber capabilities
- infusing an entrepreneurial approach in cyber workforce development
- preserving and developing DoD’s intellectual capital
- replicate in the DoD the dynamism of the private sector
- harness the power of emerging computing concepts (especially speed and incremental development rather than a single deployment of large, complex systems)
- opportunities for small and medium-sized businesses and entrepreneurs to move concepts rapidly from innovative idea, to pilot program, to scaled adoption across the DoD enterprise
- emphasise agility, embrace new operating concepts, and foster collaboration across the scientific community.

## Japan

In June 2013, Japan released a new national cyber security strategy ([Japan 2013](#)). It is largely civil in character, but it represents something of a landmark for Japan. On the diplomatic front, it talks of strengthening the active collaboration with the United States while leaving open a broad strategy of cooperation with other countries. But its military defence element is just as prominent. It pays attention not just to the Japanese armed forces but to the country's critical cyber infrastructure. It identifies ten sectors – ICT, finance, aviation, railway, electricity, gas, government-to-government services (including regional municipalities), medical, water, and logistics. This evolution has been inevitable but it also forces interested observers to understand that for Japan the operational environment for military scenarios will now be a more heavily cybered one.

This has its implications for development of the skills base. In what may be a unique national qualitative audit of IT skills, the paper says the country by itself will not meet its personnel needs in information security and that much more than half of its work-force don't have the right skills: "approximately 265,000 individuals are employed in information security within Japan, however there is a potential deficiency of approximately 80,000 such security personnel. In addition, of these 265,000 individuals, the number of individuals who actually possess the required level of skills is thought to be slightly over 105,000, meaning that some sort of education or training is necessary for the remaining 160,000 individuals" (p10).

In addition, the role of Japan and its international alliances and military partnerships are of some significance to Australia. In October 2013, the defence ministers of Japan and the United States called for the US military to provide cybersecurity training to Japanese forces in the context of a broader new policy to cooperate in developing the right human skills base (Japan Times 2013).

## China

In August 2014, China's President, Xi Jinping, told a Politburo meeting that the country needed a new cyber military strategy ([Reuters 2014a](#)). China's leaders are concerned about U.S. and Western technological superiority in the ICT sector and about China's difficulty in building a high-performing national innovation system ([Austin 2014](#)). China's speed in exploiting cyber technologies for espionage has not been matched in the pace of the overall development of its armed forces for cyber warfare. When in 2003 the Central Military Commission (CMC)

approved a new doctrine for war “under conditions of informatisation” (cyber war), it did so without wanting to sacrifice the efforts being made to catch up in classic forms of military capability (mechanised forces on land and power projection forces at sea and in the air). For this reason, the CMC approved a dual track policy of “mechanisation and informatisation”. This was a sop to the traditionalists in China’s armed forces who did not want a wholesale commitment to cyber war.

The pace of penetration of automated systems in China’s armed forces has been slow, evidenced by relatively slow introduction of simulators for weapons training. In 2008, the CMC approved a new regulation on space security, since the United States was giving pride of place in its cyber military strategies to space based assets. China lags behind the United States in space-based military assets. In 2011, China made important changes to its General Staff Department to begin to mirror the development by the United States of its Cyber Command. It was only in June 2013 that China conducted its first joint military exercise using digital technology to simulate “non-contact assaults” (that is cyber attacks intended to disable opposing military forces). The slow pace in the armed forces mirrors an equally dilatory pace of informatisation in the civilian economy. China ranks 62nd of 148 countries, according to the World Economic Forum’s 2014 Global Information Technology Report, having slipped progressively from 36th in 2011 ([WEF 2014](#), [WEF 2011](#)).

The statement from Xi in August 2014 followed several related announcements in the past year, including in February 2014 when he took over the leadership group directly responsible for all of China’s cyber development, civilian and military. His statement is especially noteworthy for two reasons. He called on the armed forces to do better at innovation in general, especially because of the problems (unspecified) with the reform process. But the more radical measure was his call to “change our fixed mindsets of mechanised warfare”.

## Islamic State

The forces of Islamic State (IS) depend on a range of communications systems that are susceptible to disruption by opposing forces. According to the new Director of the National Security Agency (NSA), Admiral Mike Rogers: “We need to assume that there will be a cyber dimension increasingly in almost any scenario that we’re dealing with” ([Reuters 2014b](#)). Rogers, who is also head of the U.S. Cyber Command, an operational joint command under the President, told a Congressional Committee in September 2014 that NSA was actively “involved

in” the cyber dimension of IS capabilities, meaning both monitoring and attacking them. These capabilities include not just social media platforms and web-based activities, but also traditional forms of communication, including encrypted communication. Also in September 2014, the U.S. Special Envoy for the coalition against IS, retired General John Allen, told a meeting in Kuwait that there needed to be a cyberspace strategy from its members ([Haaretz 2014](#)). The need for Australia to combat irregular and low-technology forces is not a reason to de-emphasise information warfare. On the contrary, clever exploitation of advanced ICT technologies can be used to undermine any organised military and political force regardless of its level of technology. At its most basic, advanced cyber espionage techniques allow more effective and timely preventive action of an irregular enemy. But the opportunities for disinformation and disruptive cyber operations are also enormous.

## Conclusion

Outside Australia, military actors of high interest to us are moving rapidly into higher levels of digital war and operations. Inside Australia, the environment for decision-making on defence policy for the information age is severely hamstrung by the national environment in the civil domain. The picture in that domain is one of falling competitiveness and only medium (to low) levels of innovation. Australia needs a digital age strategy for its civil sector before it can have a digital military strategy. Australia is falling behind the pace in entrenching digital innovation in our society. Perhaps the Defence organisation in Australia can take something of a lead to reverse this situation in the country as a whole. But it would need to recognise at the outset that the level of expertise in Australia in military applications in this field, as in many other countries, is low. We need new foreign allies in this field. The experience levels that key decision-makers in defence policy have of the IT sector do not in many cases match the nature of the problem. There would have to be a commitment to deeper organisational change, especially in force structure. The effort would need to be multi-national, multi-sector (including the Communications and Education Departments) and private-public. Stuart Robert, the current Minister Assisting the Minister for Defence, and a former military officer, does have a Master’s degree in Information Technology. Perhaps he could help drive the policy changes needed. Above all, the Australian government needs to match its obsession with cyber espionage threats with an equal passion for IT innovation across the board: in health, in agriculture, and in education.

The following steps of high relevance to the defence sector may be usefully considered:

- As a matter of urgency, appoint a specialist panel to analyse Australia's digital work force and to develop a new national strategy dedicated exclusively to its rapid development
- Use the Chubb 21-point plan for STEM education as the foundation for that report
- Use the Chubb 21-point plan for STEM education as the national benchmark for evaluating Australia's year on year educational improvements in our civil IT skills base
- As a matter of urgency, commission a report on community and business attitudes to cyberspace as they pertain to national security needs.
- Invite the Australian Army to do an audit of Australia's military digital readiness, especially focused on the White Paper concept of "how we exploit our cyber power" for military advantage
- Set up a high level review team including distinguished U.S. serving and/or retired military personnel (four star level) to report in two phases on improvements to Australia's military digital readiness: one short term (say 6-12 months) and the second in the medium term (say two years)
- Promote the convening of a public inquiry by the Australian Senate Committee on Foreign Affairs, Defence and Trade into Australia's military digital readiness
- Establish a working group with peak industry bodies on the contribution of the private sector to Australia's military digital readiness (to complement existing bodies looking merely at cyber security)
- Consider the establishment of powerful but flexible digital militia forces (reservists) capable of rapid mobilisation in major capital cities in highly secure spaces in the capitals or other nearby locations.

## References

ADF. 2014. *Information Activities*, ADDP 3.13, Canberra: Australian Defence Force. Available at: [http://www.defence.gov.au/FOI/Docs/Disclosures/330\\_1314\\_Document.pdf](http://www.defence.gov.au/FOI/Docs/Disclosures/330_1314_Document.pdf)

Australian Army. 2014. *Future Land Warfare Report 2014*. Available at:

[http://www.army.gov.au/~/\\_media/Files/Our%20future/Publications/FLWR\\_Web\\_B5\\_Final.pdf](http://www.army.gov.au/~/_media/Files/Our%20future/Publications/FLWR_Web_B5_Final.pdf)

- ACS. 2011. Australian Computer Society, *Australian ICT Statistical Compendium 2011*.  
Available at: [http://www.acs.org.au/\\_data/assets/pdf\\_file/0019/9307/Australian-ICT-Statistical-Compendium-2011.pdf](http://www.acs.org.au/_data/assets/pdf_file/0019/9307/Australian-ICT-Statistical-Compendium-2011.pdf)
- ACS. 2013. Australian Computer Society, *Australian ICT Statistical Compendium 2013*.  
Available at: [https://acs.org.au/\\_data/assets/pdf\\_file/0004/28570/Australian-ICT-Statistical-Compendium-2013.pdf](https://acs.org.au/_data/assets/pdf_file/0004/28570/Australian-ICT-Statistical-Compendium-2013.pdf)
- Austin, Greg. 2014. *Cyber Policy in China*. Cambridge: Polity Press
- Chief Scientist. 2014a. “Professor Chubb Releases ‘Science, Technology, Engineering and Mathematics: Australia’s Future’”, Press Release, Office of the Chief Scientist, Canberra, 2 September 2014. Available at: <http://www.chiefscientist.gov.au/2014/09/professor-chubb-releases-science-technology-engineering-and-mathematics-australias-future/>
- Chief Scientist. 2014b. *Science, Technology, Engineering and Mathematics: Australia’s Future*, Office of the Chief Scientist 2014, Australian Government, Canberra. Available at: [http://www.chiefscientist.gov.au/wp-content/uploads/STEM\\_AustraliasFuture\\_Sept2014\\_Web.pdf](http://www.chiefscientist.gov.au/wp-content/uploads/STEM_AustraliasFuture_Sept2014_Web.pdf)
- Coalition. 2013. “The Coalition’s Policy for E-Government and the Digital Economy”. Brian Loughnane, Canberra ACT, August 2013
- Dept. of Communications. 2013. *Advancing Australia as a Digital Economy*,. Available at: <http://apo.org.au/files/Resource/Advancing-Australia-as-a-Digital-Economy-BOOK-WEB.pdf>.
- Dept. of Defence. 2013. *Defence White Paper 2013*. Available at: [http://www.defence.gov.au/whitepaper2013/docs/WP\\_2013\\_web.pdf](http://www.defence.gov.au/whitepaper2013/docs/WP_2013_web.pdf)
- Dept. of Education. 2014a. 2013 Award Course Completions, 14 July 2014. Available at: <http://docs.education.gov.au/node/35987>
- Dept. of Education. 2104b. Completion Rates of Domestic Bachelor Students: A Cohort Analysis, 2014, p. 15. Available at: [http://docs.education.gov.au/system/files/doc/other/completion\\_rates\\_of\\_domestic\\_bachelor\\_students\\_-\\_a\\_cohort\\_analysis\\_1.pdf](http://docs.education.gov.au/system/files/doc/other/completion_rates_of_domestic_bachelor_students_-_a_cohort_analysis_1.pdf)

- Haaretz. 2014. "U.S. unveils new cyber coalition aimed at combating ISIS", 28 October 2014. Available at: [haaretz.com](http://www.haaretz.com), <http://www.haaretz.com/news/middle-east/1.623096>
- Japan. 2013. "Cybersecurity Strategy: Towards a World-leading, Resilient and Vigorous Cyberspace", Tokyo: Information Security Policy Council. Available at: [http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/JAP\\_NCSS2.pdf](http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/JAP_NCSS2.pdf)
- Japan Times. 2103. "Japan, U.S. agree to beef up cybersecurity", *Japan Times*, 3 October 2013. Available at: <http://www.japantimes.co.jp/news/2013/10/03/national/politics-diplomacy/japan-u-s-defense-chiefs-meet-on-cybersecurity/#.VFQKzxbgU71>
- Karunaratne, Neil Dias 1989. "A Rapid Informatisation Strategy for Australia: An Impact Analysis", *Economic Systems Research*, Vol. 1 (4), 465-79.
- Keating, Paul L. 1997. "Cyberpolities - Australia, Asia and the Information Revolution", SUGA '97 Conference, Hilton Hotel, Sydney, 5 August 1997. Available at: <http://www.keating.org.au/shop/item/cyberpolities-the-information-revolution---5-august-1997>
- PWC. 2014. *Deciding with data: How data-driven innovation is fuelling Australia's economic growth*, Price Waterhouse Coopers on behalf of Google. Available at: <http://www.pwc.com.au/consulting/assets/publications/Data-drive-innovation-Sep14.pdf>
- Reuters. 2104a. "China's Xi urges army to create strategy for information warfare", 30 August 2014. Available at: <http://www.reuters.com/article/2014/08/30/us-china-xi-defence-idUSKBN0GU0H020140830>
- Reuters. 2104b. Doina Chiachu, "U.S. NSA chief says monitoring tech-savvy Islamic State", 16 September 2014. Available at: <http://www.reuters.com/article/2014/09/16/us-cybersecurity-usa-islamic-state-idUSKBN0HB22A20140916>
- United States. 2011. "Department of Defense Strategy for Operating in Cyberspace", Washington DC. Available at: <http://www.defense.gov/news/d20110714cyber.pdf>
- United States. 2012a. "Presidential Policy Directive 20: U.S. Cyber Operations Policy", The White House, 2012, Available at: <http://fas.org/irp/offdocs/ppd/ppd-20.pdf>

- United States. 2012b. "Information Operations", Washington DC: The Joint Chiefs of Staff, November 2012, Joint Publication 3-13, Available at:  
[http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_13.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf)
- Waters, Gary; Ball, Desmond; Dudgeon, Ian. 2008. *Australia and Cyber-Warfare*, Canberra Papers in Strategy and Defence, Australian National University ePress. Available at:  
[http://press.anu.edu.au/wp-content/uploads/2011/08/whole\\_book5.pdf](http://press.anu.edu.au/wp-content/uploads/2011/08/whole_book5.pdf)
- Watson, Chris. 2007. "Joint Information Operations: The Way Ahead", *Australian Army Journal*, Vol. 4 (1), 77-98. Available at: <http://www.army.gov.au/Our-future/Publications/Australian-Army-Journal/Past-editions/~media/Files/Our%20future/LWSC%20Publications/AAJ/2007Autumn/07-JointInformationOperati.pdf>
- WEF. 2004. *Global Information Technology Report 2003-2004*, New York: Oxford University Press, for the World Economic Forum and others, 2004. Available at: [http://www-wds.worldbank.org/servlet/WDSContentServer/IW3P/IB/2005/11/17/000090341\\_20051117162002/Rendered/PDF/343090GITR2003.pdf](http://www-wds.worldbank.org/servlet/WDSContentServer/IW3P/IB/2005/11/17/000090341_20051117162002/Rendered/PDF/343090GITR2003.pdf)
- WEF. 2011. *Global Information Technology Report 2010-2011*, New York: Oxford University Press, for the World Economic Forum and others, 2011. Available at:  
[http://www3.weforum.org/docs/WEF\\_GITR\\_Report\\_2011.pdf](http://www3.weforum.org/docs/WEF_GITR_Report_2011.pdf)
- WEF. 2013. *Global Information Technology Report 2013*, New York: Oxford University Press, for the World Economic Forum and others. Available at:  
<http://www.weforum.org/reports/global-information-technology-report-2013>
- WEF. 2014. *Global Information Technology Report 2014*, New York: Oxford University Press, for the World Economic Forum and others. Available at:  
<http://www.weforum.org/reports/global-information-technology-report-2014>

## Critique of the new NBN policy

### Lower cost, faster roll-out, access competition, technology independence, future proof?

---

Graham Shepherd

Netfluency

---

**Summary:** In December 2014 the Australian Minister for Communications released a policy destined to transform the NBN as conceived by the previous government. Its primary stated aims are to lower costs and introduce competition. The cost reductions are driven by significantly compromising the access speed and substantially but not entirely eliminating the lead-in cost. The policy also anticipates a competitive model, which risks creating islands of monopoly based upon the footprints of the proposed FTTN and HFC networks – although the fixed wireless and satellite technologies should be able to operate competitively, if not profitably. This paper addresses the limitations of the policy as currently stated and proposes some changes in approach which share the objectives of the policy but without compromising speed. The changes will eliminate the lead-in cost entirely and will introduce infrastructure competition in the long-term interests of end-users. They will accelerate the NBN roll-out and ensure that the national infrastructure is responsive to future technologies, market demands and business opportunities.

## Introduction

On 11 December 2014 the Minister for Communications, Malcolm Turnbull, published a new government policy paper, 'Telecommunications Regulatory and Structural Reform' (Policy, 2014).

The policy requires, through carrier licence conditions destined to come into effect on the 1st of January 2015, that "providers of superfast broadband networks providing services to residential customers to be functionally separated (that is, operate their networks and retail operations at arm's length) and offer a 25/5 Mbit/s wholesale bitstream service at no more than \$27 per month."

Crucial aspects of this policy are that it establishes a relatively low speed access network compared with other countries and sets the scene for competition in the wholesale of broadband access. It leaves unaddressed some significant uncertainties in the costs of the

NBN project, such as the lead-in cost; and it imposes some additional costs in preparing for future infrastructure competition.

This policy is based on a series of studies commissioned by the Minister, most importantly the Vertigan Panel Report ([Vertigan, 2014](#)) whose terms were announced in December 2013 ([MoC Terms, 2013](#)).

The headline terms of reference for the Panel to address were:

- What is the direct and indirect value, in economic and social terms, of increased broadband speeds, and to what extent should broadband be supported by the government?
- What are the optimal long-term ownership and regulatory arrangements for NBN Co?
- How should the activities of NBN Co be constrained given its mandate to efficiently build, operate and maintain a wholesale-only access network?
- How should NBN Co's capital investment, products and pricing be reviewed and regulated?

## Vertigan Panel Report

The Vertigan Panel Report ([Vertigan, 2014](#)) in addressing these questions cites the Council of Australian Government's Competition Principles Agreement ([COAG, 1995](#)), supporting competition and promoting the "long-term interests of end-users" – a key criterion for this critique. The Cost Benefit Analysis ([Vertigan Vol. II, 2014](#)) addressed the long term and set out to project outcomes to 2040.

The Panel concluded that "a fully commercial rollout, to areas where demand covers costs, would yield net economic benefits of \$24 billion" (NPV). And that the multi-technology mix (MTM) approach, basically FTTN, HFC and FTTP, would yield \$16 billion greater benefits than relying solely on FTTP. It claimed that MTM can be upgraded and is "robust to variation in the growth in demand." This "robustness" depends significantly on effective wholesale infrastructure competition to drive continuing investment.

The framework for the Cost Benefit Analysis and future projections was set by an economic analysis of today's products, technologies, usages and business opportunities ([Robson, 2014](#)). This framework and the resulting cost benefit analysis were based on a peak download speed requirement of 25 Mbit/s possibly stretching to 50 Mbit/s.

The speed estimates factored into the model were from the Communications Chambers report of 26 May 2014 ([Kenny, 2014](#)).

The Panel observed that “the growth rate of willingness to pay for higher speeds is a major source of uncertainty, as the nature of and willingness to pay for future applications are not readily predictable.” This observation is based on the assumption that higher speeds actually cost significantly more.

Whilst the published Cost Benefit Analysis has much of its information redacted, it is not clear that the Panel separated out all of the various components of cost, tested all of the sensitivities nor consider other designs and methodologies. In particular the lead-in cost from the street to the home is one of the largest costs to FTTP and the greatest cost and time uncertainty (apart from politics). FTTN does avoid this problem because the lead-in exists, but it does so by significantly compromising the access speed. HFC also avoids the lead-in problem but only for premises actually connected. FTTdp, a technology covered briefly below and elsewhere in this Journal, avoids the lead-in problem altogether and eliminates the access speed constraint ([Watkins, Mar 2014](#) and [Watkins, Dec 2014](#)).

Based effectively on the two assumptions that the maximum speed requirement is only 50 Mbit/s and that the lead-in cost can be avoided (to a certain extent), the Panel concluded that the MTM is significantly cheaper than FTTP alone.

Vertigan then went on to recommend “that the Government move to disaggregate NBN Co along the lines of its underlying networks where each of the satellite, fixed wireless, HFC and FTTx networks would serve as the basis for a competing entity.”

## Government policy paper

As a result of this substantial preparatory work, the Government’s new policy, “Telecommunications Regulatory and Structural Reform” was published on 11 December 2014 ([Policy, 2014](#)).

Whilst maintaining that “the Government does not support near-term disaggregation of NBN Co into business units based on access technologies” it retained the option “for future restructuring or disaggregation ... to provide future governments with greater policy and financial flexibility.” It also expresses a preference for OSS/BSS IT systems to be readily separable, acknowledging that “this may involve higher costs.”

## NBN Co, Telstra and Optus: definitive agreements

On 14 December 2014 the Minister of Communications, NBN Co, Telstra and Optus announced new definitive agreements regarding the access and transfer of copper and HFC assets to NBN Co ([Definitive Agreements Announced, 2014](#)). The main changes to the definitive agreements were published in Telstra’s announcement to the ASX on 14 December

2014. ([Telstra ASX Announcement, 2014](#)). The agreements are confidential but certain information can be gleaned from the main changes described.

The headline \$11 billion post-tax NPV price paid to Telstra remains unchanged. The ownership of the copper-pair and HFC assets will progressively transfer to NBN Co. Telstra will retain ownership of the ducts – a major physical asset for which NBN Co will continue to pay substantial amounts annually, which leaves Telstra in a commanding competitive position with regard to duct usage. NBN Co will take over the remediation and maintenance costs of the ducts, pits and copper (and consequently the public liability). Telstra will also continue to deliver Foxtel services over the HFC. Telstra's remediation obligations within FTTP regions have been capped.

Collectively these changes are significantly beneficial to Telstra although NBN Co obtains greater flexibility in the usage of assets. It might seem that the transfer of ownership of ducts and pits to NBN Co would have been a sensible move but Telstra has held all the cards in the negotiations and it remains politically too hard for governments to force the issue given the wide ownership of Telstra shares and the long history of share price problems.

## Summary of issues

The Vertigan Panel Report and the Government Policy Paper present a range of issues all of which, if properly addressed, could result in a different set of conclusions and a different policy. The issues are summarised here and two in particular are addressed under the main headings of Access Speed and Deep Fibre FTTdp below.

The issues are:

- The access speed capability is the major determining factor, as assessed by the Vertigan Panel, in NBN cost. The forecast speed requirement was set by the Communications Chambers report at 25 Mbit/s possibly stretching to 50 Mbit/s ([Kenny, 2014](#)). This extraordinarily low forecast is in dramatic contrast with the massive investments being made by technology companies and carriers in driving access speeds for all types of fixed and wireless networks world-wide towards and beyond 1 Gbit/s per user or household. Admittedly, the Communications Chambers report openly acknowledges that it provides just one view in a subject open to debate. Unfortunately the debate appears not to have been given a full hearing by Vertigan or the Minister's advisors.
- The lead-in cost and uncertainty are not addressed explicitly by Vertigan nor in any further policy considerations. Nevertheless the avoidance of the lead-in cost is clearly the major advantage of FTTN over FTTP but with serious penalties in access speed

and operational costs. HFC also avoids the lead-in cost where a connection already exists.

- The potential for HFC and FTTN to provide infrastructure competition is explicit but it is not clear how this will be effective for the benefit of end-users. The HFC networks have some particular characteristics. The two networks (Telstra and Optus) substantially overlap. And, of course, they also overlap the copper-pair network. Many premises (approximately 900,000) are passed by HFC but not connected. HFC coverage is also selective and would require fill-in in both commercial and residential areas if it were to become the only high-speed broadband access technology available in an area. The HFC infrastructure is 20 years old now and has had limited investment except for upgrading DOCSIS and digital TV. Telstra and Optus both stopped rolling out and promoting new consumer connections when confronted with low net growth, high roll-out costs, and increasingly high lead-in costs. John Goddard has written an excellent review of HFC and its potential as an alternative broadband technology demonstrating its capabilities to achieve high access speeds in the long term ([Goddard, 2014](#)). CCAP and Remote PHY are two technologies which extend the capability of HFC networks to offer 100+ Gbit/s access speeds ([Brockett, 2013](#)). But the existing Australian networks need serious and on going investment. In an HFC area without an FTTx competitor, there may be little incentive for such investments.
- NBN Co has announced a policy which effectively suspends FTTN deployment in HFC coverage areas ([NBN Co, 2014](#)). This is in conflict with the concept of effective infrastructure competition in the long-term interests of end-users – a conflict which needs to be resolved.
- One transforming technology which was not explicitly discussed in the Vertigan Panel Report is fibre to the distribution point (FTTdp) ([Watkins, Mar 2014](#) and [Watkins, Dec 2014](#)). It avoids the major lead-in cost, offers 1 Gbit/s speeds and opens up effective competition options for the customer connection.
- By disaggregating NBN Co into business units based on the footprints of today's technologies and eventually selling them off, the government will face the risk of setting up islands of monopoly with little incentive for investment in the future and no effective choice for customers. This was obviously not the intention of the Vertigan Panel, and it needs to be prevented. The government's approach has been to defer disaggregation but to set up the conditions for it within NBN Co. Either way NBN Co will be distracted by the complexities and costs of multiple competing technologies.. The selling price obtainable by the government for a perceived monopoly would be higher than for a business facing real competition, but the former would not be in the

long-term interests of end-users nor of Australia's capability to engage in the global digital economy. It would give the unfortunate appearance of giving lip service to competition while paving the way for prospective monopolists as the new owners.

- Vertigan and the government policy both acknowledge that disaggregating the business units and their respective OSS/BSS IT systems will add additional costs, which could well be significant.

## Access Speed

One of the critical (and startling) assumptions of the Vertigan report and the government's response is that a peak requirement of 25 Mbit/s is enough per household, with 50 Mbit/s being an upper limit looking ten years out. This assumption drives the calculations of estimated cost and national economic benefit. The assumption is based on the Communications Chambers report ([Kenny, 2014](#)) but the debate surrounding it has not had an adequate hearing. The debate (or argument) has been raging within industry circles, but beyond the hearing of government and, it seems, without influence.

To the credit of the authors of the Communications Chambers report, they acknowledge that their findings are "open to debate", are "limited in scope", are subject to "alternative assumptions" and are a "contribution to a meaningful discussion rather than its conclusion". Nevertheless one gets the strong impression that the report tries to talk down future data speed requirements to match the client's expectations. The report also focuses heavily on current Internet usage, namely browsing and video downloads, giving much less attention to (and sometimes discounting) other uses or the potential for completely new applications which wide-spread download speeds of 1 Gbit/s overseas will undoubtedly spawn.

Clearly the rest of the world does not agree with the Communications Chambers findings. Scores of countries are rolling out FTTP networks to tens, possibly hundreds of millions of customers. Admittedly very few are on the geographical scale of the NBN as originally conceived, nor are as equitable, but the high average bit rates achieved by so many countries ahead of Australia indicate that FTTP penetration is very high and growing.

As at 13 December 2014, measurements in 41 countries indicate a "rolling mean download speed" of 25 Mbit/s or more: Australia ranks 58<sup>th</sup>, at under 16Mbit/s ([OOKLA, 2014](#)). Australia is substantially behind the G8 (27.9), the EU (27.0), the OECD (26.7) and APEC (24.3). Akamai is another source of similar rankings, and its numbers are even less flattering to Australia ([Akamai, 2014](#)).

A number of arguments are presented by Communications Chambers that the demand for speed will slow. They start from the premise that video download is the major driver, that it

is related to the number of users, not devices, and that users watch videos serially and therefore growth is limited. There is some validity in this but there is a long way to go before we reach a demand plateau, particularly as video over IP (for main stream movies or television) shows all the signs of becoming a dominant delivery mechanism – and it has barely started.

The arguments include that data compression will continue to reduce bandwidth requirements. In fact improved compression techniques have taken place in steps several years apart but not progressively. H.265 or HEVC (2013) is the latest technique, which is said to double the efficiency of H.264 or MPEG-4 (2003). All these standards have complex intellectual property and royalty issues, which inevitably delay and restrict deployment. The additional compression offered is more than offset by increasing demand for higher resolutions. Communications Chambers acknowledges this offset but gives an overly strong weight to increasing compression.

Screen resolutions now exceed standard printing resolutions, HD TV is now the de facto standard (2K pixels on the long dimension). 50 inch (127 cm) 4K 3D TVs are available in Australia for under \$2,000. 8K resolutions are also in development. Low cost 4K video cameras are also readily available, placing an increasing demand on upload speeds. Communications Chambers acknowledges this but projects a slow take up of 4K despite the low costs and ready availability even today.

Media compression techniques are usually but not always “lossy”, compromising those parameters which are deemed to be least discernible to the eye or ear. (Those that are not lossy generally produce much larger files.) However, these kinds of compromises are becoming less acceptable for both consumers and for commercial reasons. Commercial advantages of higher accuracy of reproduction include improving the shopping experience. Colour fidelity and matching is one example (colour being the first parameter sacrificed in compression), and texture matching is likely in the future using 3D imaging. Another example is that higher resolution of sporting videos significantly improves the impact of fixed advertising even while cameras closely follow the action rather than the background. A number of companies are focused on significant improvements in colour fidelity for 4K video including Dolby Vision and Technicolor.

It is argued that videos are watched serially and are limited by the number of users. However, the increase in imaging (multiple devices) in homes and offices for security, education, health, management and control would suggest that there is no end in sight (yet) to growth in demand for speed and capacity. Not every image or video taken and uploaded has to be watched.

The world-wide deployment of access networks capable of delivering 1 Gbit/s, together with globally distributed data centres, are removing the bottle necks for high speed downloads and are also removing the incentive for higher compression in favour of better reproduction accuracy.

Similar objections apply to the growth in number, range and capability of applications. Once certain bottlenecks are removed, the growth in traffic can increase very rapidly. Phone apps grew quickly once APIs were standardised, user interfaces simplified and app stores became available. Revolutionary improvements in download and upload access speeds will combine with these other revolutions to accelerate applications across the board. The revolution is not increasing the download speed to 25 or 50 Mbit/s but to 1 Gbit/s or 10Gbit/s, as it has in the commercial world. Big Data and the Internet of Things are upon us now. Australia has to be able to participate in the global scene.

One further consideration is that the growth in cloud storage and computing is at least as strong in the consumer market as in the business market. Images and videos are now being automatically backed up at full-resolution, often with unlimited bandwidth and sometimes to multiple cloud services. For example, Sony PlayMemories offers unlimited free photo storage at full resolution, regardless of whether you own a Sony camera or not. Entry level (paid) consumer cloud storage capacity jumped in one step in 2014 from 100 GB to 1TB for the same price ([Dropbox, 2014](#)). Apple, Microsoft and Google have followed suit.

All of these factors drive growth in economic activity and Australia should not be held back by a misalignment with the global directions on access speed, especially if its impact on cost is imagined rather than real.

## Deep Fibre FTTdp

Fibre to the distribution point (FTTdp) is covered very comprehensively elsewhere in this Journal ([Watkins, Mar 2014](#), and [Watkins, Dec 2014](#)). It passes unmentioned by the Vertigan Panel and the new policy, even though it may be considered to be an end-game of fibre to the node (FTTN).

In summary FTTdp involves replacing all the copper pair cable in the access network (up to the property boundary) with optic fibre cable, and providing a pit mounted VDSL2 or G.fast node to connect one or more dwellings at up to 1 Gbit/s, using the existing copper pair lead-ins. The significant advantages of this technique are firstly that the lead-in replacement cost is avoided, and secondly that a choice of retailers can provide the customer connection rather than the wholesaler. This results in massive savings in construction, operations (compared with FTTN) and BSS/OSS costs to NBN Co, as well as creating a form of competition which is meaningful for the consumer. Nor does it preclude wireless as a competitive access

methodology along the lines of Telstra's Wi-Fi initiative ([Telstra Wi-Fi, 2014](#)) or a 4G or 5G mobile equivalent. Customers who want a direct fibre connection can also obtain it from competitive retailers.

A cost comparison between FTTN and FTTdp would entail the costs of the street-side cabinets, their power and maintenance plus the maintenance of the copper-pair cables versus the extension of more fibre (a significant proportion of premises would already be passed by fibre to reach the FTTN cabinets) and the relative costs of the FTTdp mini-nodes versus the FTTN nodes. Over a 25 year cost benefit comparison, the inevitable need to upgrade the FTTN periodically must be factored in.

The management advantage of an FTTdp roll-out versus an FTTN is that it becomes essentially a civil engineering project with a single wholesale BSS/OSS. By giving a singular focus to the NBN Co project team together with an aggressive and progressive improvement programme, costs can be driven down and the rate of deployment increased. Objectives can be set and incentives provided towards that end.

The greatest national economic benefit of FTTdp is that Australian businesses and entrepreneurs can then participate in the global digital economy on an equal basis to the rest of the world instead of being artificially and unnecessarily constrained in access speed to something 40 times less than that which the best of the rest of world is deploying.

FTTdp offers both a potential cost advantage plus the potential economic benefits flowing to Australia where 1 Gbit/s access speeds are available rather than 25 Mbit/s.

## Recommendations

By making the following amendments, the NBN policy could be significantly improved:

1. Declare the property boundary as the network boundary.

This will eliminate the lead-in cost from the NBN Co project and enable a much tighter focus on what is the best delivery technology.

2. Declare the customer lead-in as open to competition.

This will provide effective competition for the benefit of end-users, not just in initial cost but for long-term ongoing support. It should be open for copper-pair, coaxial cable, wireless or fibre solutions depending only upon the customer and the retailer. Retailers should be licensed and meet certain basic requirements including APIs and service levels.

3. Consider selling the HFC networks sooner rather than later.

Minimum service requirements would have to be placed on the purchaser(s) but this would improve the immediate cash flow position for the government, and for NBN Co it would remove a significant management and engineering overhead, thus significantly tightening the focus of the project, with associated cost and delivery benefits.

4. Require NBN Co to pass all premises in the original FTTP footprint with optic fibre.

This will establish effective wholesale competition in the access network between FTTdp and HFC. The priorities should be determined by NBN Co on the basis of maximising the speed of the roll-out, without regard to existing HFC coverage.

5. Establish KPIs and incentives for NBN Co.

The KPIs should include cutting its fibre deployment cost by X% per annum, increasing its rate of deployment by Y% per annum and increasing its maximum available speed by Z% per annum.

There must be a process whereby the objectives set for NBN Co are comprehensive, are genuinely challenging but are achievable.

Collectively this amended policy would:

- Provide effective competition and real choices for customers.
- Drive the capital and operating costs of NBN down dramatically.
- Lift the entirely unrealistic speed and performance caps in the proposed access network to world standards in a relatively short time frame.
- Establish a simple low-cost NBN wholesale infrastructure company which is open to competition in the short term, and in the longer term is saleable.
- Enable and energise Australia to participate profitably in the global digital economy.

## Conclusions

With the recent run of government reports, policies and agreements, it might appear that the deal is done and that it is too politically difficult to make the necessary changes to such an improved policy. But this might not be the case.

The MTM is not actually incompatible with FTTdp and the proposed more competitive model advanced in this paper. FTTN and HFC both need to push fibre deeper into the access network to achieve world standard performance. NBN Co could make the transition over

months with minimal further direction and the Minister could revise the policy accordingly after due consideration of costs and benefits.

The competitive model as described should be very attractive to the competitive carriers, large and small, and it should open up many opportunities for innovative solutions.

Most of all, great opportunities would be opened up for Australian businesses and entrepreneurs to participate in the global digital economy, unconstrained by ultimately irrelevant technical arguments about whether users should be limited in speed to 50 Mbit/s or 25 Mbit/s, when 1 Gbit/s is necessary and becomes entirely feasible at a reasonable cost.

## Acknowledgements

This paper has benefitted greatly from the contributions of many people, not the least being the anonymous reviewers, all of whom have been studious and expert in their contributions and appraisals at both the strategic and tactical levels as well as in the fine detail. Nevertheless, all the flaws and weaknesses in the paper are entirely the responsibility of the author.

## Glossary

COAG	Council of Australian Governments
LTIE	Long-term interests of end-users – an objective of the COAG Competition Principles Agreement.
Copper-pair cable	Cable of bundled twisted pairs of copper wires which have provided the telephone connection for many decades. New technologies have made it capable of carrying high speed data.
Lead-in cable	The final connection between the external network and the internal premises network. It may be a twisted pair cable or a coaxial cable or an optical fibre. It may be short but because all premises are different the cost of provision is unpredictable and potentially very high.
FTTP	Fibre to the premises – comprises an end to end optical fibre connection.
FTTH	Synonymous with FTTP except that it implies a residential connection.

FTTN	Fibre to the Node – comprises optical fibre to a street-side cabinet with a dedicated copper-pair cable to the premises. Powered locally and contains battery backup power.
HFC	Hybrid Fibre Coax – comprises optical fibre from the operators “headend” to a “node” with a shared RF modulated coaxial cable to the premises.
CCAP	Converged Cable Access Platform – a fully digital HFC technology which facilitates high speed and a range of services.
Remote PHY	Remote PHY is an HFC node technology which dynamically manages the upstream and downstream bandwidths on shared HFC.
FTTdp	Fibre to the distribution point – comprises optical fibre to a node very close to the premises with copper-pair distribution of broadband to individual premises. Very small nodes are often back-powered from the premises over the copper pair.
FTTx	A generalised term for any of the fibre and/or copper-pair technologies. Does not encompass HFC.
VDSL2	Very high bit rate Distributed Subscriber Line – modulation technique used on copper-pair cable for the final connection to the premises. It is useable up to about 800 metres after which the speed falls off quickly.
G.fast	An evolution of VDSL2 intended for shorter lengths of copper-pair cable up to 250 metres. The access speed can potentially reach 1 Gbit/s.
MTM	Multi-Technology Mix – comprises all of the broadband access technologies including FTTN, HFC, FTTdp, fixed wireless and satellite.
Deep fibre	Fibre almost to the premises – may be applied to FTTN, FTTdp or HFC.
CPE	Customer premises equipment – in this case a modem to covert the broadband signal to one or more Ethernet ports.

OSS/BSS	Operational Support Systems/Business Support Systems – comprises both the processes and the IT systems which enable them.
---------	---

## References

- Akamai. 2014, *State of the Internet*, <http://www.akamai.com/stateoftheinternet/index.html>, accessed 15 Dec 2014.
- Brockett, Rei, 2013. *The evolution of CCAP*, <http://www.lightwaveonline.com/articles/2013/09/the-evolution-of-ccap.html>, accessed 18 Dec 2014
- Comparison of international download speeds, OOKLA Net Index, <http://www.netindex.com/download/allcountries/>, accessed 13 Dec 2014.
- Council of Australian Governments, 1995. Competition Principles Agreement, <https://www.coag.gov.au/node/52>, accessed 13 Dec 2014.
- Dropbox cloud storage plans. 2014. <https://www.dropbox.com/plans>, accessed 13 Dec 2014.
- Goddard, John. 2014. *The Untapped Potential of Hybrid Fibre Coaxial Networks*, <http://telsoc.org/ajtde/2014-06-v2-n2/a40>, accessed 18 Dec 2014.
- Kenny, Robert; Broughton, Tom. 2014. *Domestic bandwidth requirements in Australia - A forecast for the period 2013-2023*, [http://www.communications.gov.au/\\_data/assets/pdf\\_file/0013/243040/Forecasting-Australian-Per-Household-Bandwidth-Demand-Commun.pdf](http://www.communications.gov.au/_data/assets/pdf_file/0013/243040/Forecasting-Australian-Per-Household-Bandwidth-Demand-Commun.pdf), accessed 13 Dec 2014.
- Minister for Communications. 2013. *Panel of Experts to conduct cost-benefit analysis of broadband & review NBN regulation*, [http://www.minister.communications.gov.au/malcolm\\_turnbull/news/Panel\\_of\\_experts\\_to\\_conduct\\_cost-benefit\\_analysis\\_of\\_broadband\\_and\\_review\\_nbn\\_regulation](http://www.minister.communications.gov.au/malcolm_turnbull/news/Panel_of_experts_to_conduct_cost-benefit_analysis_of_broadband_and_review_nbn_regulation), accessed 13 Dec 2014.
- Minister for Communications Policy Paper. 2014. *Telecommunications Regulatory and Structural Reform*, [http://www.communications.gov.au/\\_data/assets/pdf\\_file/0020/243902/Telecommunications\\_Regulatory\\_and\\_Structural\\_Reform\\_Paper\\_-\\_11\\_December\\_....pdf](http://www.communications.gov.au/_data/assets/pdf_file/0020/243902/Telecommunications_Regulatory_and_Structural_Reform_Paper_-_11_December_....pdf), accessed 13 Dec 2014.
- Minister for Communications NBN Co definitive agreements. 2014. *NBN Co and Telstra sign revised Definitive Agreements*, [http://www.minister.communications.gov.au/malcolm\\_turnbull/news/nbn\\_co\\_and\\_telstra\\_sign\\_revised\\_definitive\\_agreements](http://www.minister.communications.gov.au/malcolm_turnbull/news/nbn_co_and_telstra_sign_revised_definitive_agreements), accessed 15 Dec 2014.
- NBN Co media release. 2014. *NBN Co outlines principles for Multi-Technology rollout*, [http://www.nbnco.com.au/corporate-information/media-centre/media-releases/nbn\\_co\\_outlines\\_principles\\_for\\_multi\\_technology\\_rollout.html](http://www.nbnco.com.au/corporate-information/media-centre/media-releases/nbn_co_outlines_principles_for_multi_technology_rollout.html), accessed 18 Dec 2014.
- Robson, Alex. 2014. *Cost-Benefit Analysis of Public Investment in High Speed Broadband Network Infrastructure: An Analytical Framework*, [http://www.communications.gov.au/\\_data/assets/pdf\\_file/0007/240766/5\\_NBN\\_CB\\_A\\_Analytical\\_Framework\\_Final\\_16\\_May\\_2014.pdf](http://www.communications.gov.au/_data/assets/pdf_file/0007/240766/5_NBN_CB_A_Analytical_Framework_Final_16_May_2014.pdf), accessed 13 Dec 2014.

- Telstra ASX Announcement. 2014. *Key changes to the original definitive agreements*, <http://www.telstra.com.au/abouttelstra/download/document/asx-announcement.pdf>, accessed 15 Dec 2014.
- Telstra National Wi-Fi Network, <https://www.telstra.com.au/broadband/wifi>, accessed 15 Dec 2014.
- Vertigan Panel Report to the Minister for Communications. 2014. *Independent cost-benefit analysis of broadband and review of regulation*, [http://www.communications.gov.au/\\_\\_\\_data/assets/pdf\\_file/0009/243387/NBN-Market-and-Regulatory-Report.pdf](http://www.communications.gov.au/___data/assets/pdf_file/0009/243387/NBN-Market-and-Regulatory-Report.pdf), accessed 13 Dec 2014.
- Vertigan Panel Report Volume II. 2014. *Cost Benefit Analysis*, [http://www.communications.gov.au/\\_\\_\\_data/assets/pdf\\_file/0003/243039/Cost-Benefit-Analysis-FINAL-For-Publication.pdf](http://www.communications.gov.au/___data/assets/pdf_file/0003/243039/Cost-Benefit-Analysis-FINAL-For-Publication.pdf), accessed 13 Dec 2014. (Useful cost information has been redacted)
- Watkins, Craig; Lillingstone-Hall, Kelvin. 2014. *The FTTdp technology option for the Australian National Broadband Network*, <http://telsoc.org/ajtde/2014-03-v2-n1/a26>, accessed 13 Dec 2014.
- Watkins, Craig; Lillingstone-Hall, Kelvin. 2014. *A closer look at Deep-fibre FTTdp*, <http://telsoc.org/ajtde/2014-12-v2-n4/a67>, accessed 13 Dec 2014.

## A closer look at Deep-fibre FTTdp

**Craig Watkins**

Informative Technology Innovations

**Kelvin Lillingstone-Hall**

OAK Telecom

**Summary:** In this paper we outline a number of matters that have been raised in relation to Deep-fibre Fibre-to-the-Distribution-Point (FTTdp), and address practical ways that FTTdp can be expected to deliver a maximum overall cost-benefit outcome for the Australian NBN. We present brief discussions of some HFC (Hybrid Fibre Coax) and FTTN (Fibre-to-the-Node) issues considered of concern, to place FTTdp in perspective. We touch briefly on the threat from wireless communications to the fixed line technologies. We discuss the FTTdp equipment ecosystem, migration from legacy services to FTTN or FTTdp, in-building copper concerns, and LFN architecture savings emerging from the FTTdp approach. As previously, we conclude that FTTdp must be honestly evaluated if the nation is to achieve a maximal NBN capability outcome.

### Introduction

The vision of the NBN is to supply access network capacity to economically meet demands of today and those of the future. Deep-fibre Fibre-to-the-Distribution-Point (FTTdp) in the form of fibre to the street lead-in pit at the front fence, with an average copper lead-in of 30m, promises a level of overall network capability very close to that of full FTTP (Fibre to the Premises). Improvements in fibre-related technologies continue to promise increasing levels of connectivity (Ovum 2014). Simultaneously, while improvements in fibre technologies and construction practices continue to reduce fibre deployment costs, deployment of customer lead-in connections is more resistant to the potential for cost savings. Following our earlier paper (Watkins and Lillingstone-Hall 2014), we believe that deep-fibre FTTdp is a strong candidate for delivering the maximum cost-benefit access network outcome to the nation.

Communications technology determinations are highly contingent upon access network bandwidth demand projections, and these are observed to vary immensely. A sensible analysis exploiting valid assumptions and rational logic can eliminate the most offensive demand projection outliers, but there is no obvious way to obtain significant consensus perspective on future demand requirements of the NBN. We can, however, expect to obtain strong consensus on the fact that demand variability from user to user is high. We can also

be quite certain that bandwidth demands will continue to rise for the foreseeable future. Translation of these facts to NBN deployment determinations implies the need for high network flexibility.

Fibre to the Node (FTTN) is a well-known path to incremental improvements in access network capability. With augmentation by a small number of micro-node devices, FTTN is capable of delivering significant connectivity improvements over exchange-based ADSL services. The best improvement can be expected for those users closest to nodes or micro-nodes. It is, however, problematic to provide any certainty in connectivity outcomes for premises more distant from node locations. Copper-related factors are an important consideration for all non-fibre connection solutions, and in-building or in-premises copper configuration issues may cause a need for expensive rectification work. The long-term prospects for FTTN are also poor in the sense that demand growth may quickly outstrip the capability of long copper pairs from the node, with the only prospect being eventual deployment of fibre beyond the node.

Advanced technologies such as G.fast (ITU 2013) offer little benefit in a FTTN setting (although vectored G.fast may prove useful with the related FTTB (Fibre-to-the-Building/Basement) approach in some MDU environments). The recently announced Vplus technology from Alcatel-Lucent (Russell et al 2014) appears to maximise the capability of DSL-based technologies in a node setting. It is important to note that even with Vplus, only premises close to the node receive significant benefit. The geometry of Telstra Distribution Areas may limit meaningful Vplus potential gains from the node to less than 30% of premises. Vplus allows a distribution area to be subdivided by strategic positioning of smaller node devices to reduce overall copper loop lengths, but the deployment expense of such an option must be compared with the relative merits of a deep-fibre FTTdp solution.

Deep-fibre FTTdp, bringing fibre to street distribution pits, eliminates around 90% of the copper network compared to FTTN, and importantly eliminates practically all copper network joints. The considerably shorter copper lengths of deep-fibre FTTdp maximise the prospects for technologies such as G.fast, although extremely good connectivity outcomes are also readily achieved through VDSL2, where 200 Mbps download and 50 Mbps upload are likely to be achievable for a vast majority of premises. We note that VDSL2 offers an aggregate (download plus upload) of 300 Mbps for short copper lengths (Lantiq 2014, Hirscher 2014).

FTTdp provides three significant advantages in overcoming in-building or in-premises copper configuration issues compared to FTTN:

(1) a large reduction in overall copper length maximises connection throughput capabilities even with undesirable copper configuration conditions (bridge taps);

(2) significant reduction in bundled copper usage reduces the prospect that undesirable signals such as impulse noises collected in one premises will impact connectivity in other premises; and

(3) highly problematic premises are provided with an economic option to upgrade to a fibre drop connection, effectively capping in-premises copper rectification expenses.

The core advantages of the deep-fibre FTTdp approach are that it facilitates user demand flexibility and accommodates large potential future bandwidth demand growth. The deep-fibre FTTdp approach provides a base-level of connectivity to all users that is substantially higher than the average connectivity level provided via FTTN. This has significant value in relation to the capacity of the network to meet future demand scenarios. It is crucial to note that lower demand growth projections may not value such capability appropriately, and the precise terms of any Statement of Expectations given to NBN Co becomes a critical issue for the future of the nation's communications infrastructure.

FTTdp economically provides for the high connectivity demands of a small proportion of key consumers. It does this in a way that does not stifle creativity and growth at the start-up enterprise level where there may be limited ability to pay for more expensive connectivity outcomes. Limits on the ability to pay may come from cash-flow restrictions, or the expectation of future growth-demanded business premises relocation.

Deep-fibre FTTdp provides an overall level of network capability similar to that of FTTP, yet with cost and time equations comparable with FTTN, due to elimination of the extreme expense and labour resource requirements associated with FTTP premises connections in the Australian NBN context. It promises long-term communications infrastructure for the nation, at a substantial cost and time reduction to FTTP, making a superior national communications outcome possible.

This paper extends the presentation of deep-fibre FTTdp introduced by the authors in a March 2014 paper published in the same journal. We cover a collection of concerns and issues that have been raised through the ensuing six months discussing the rationality of FTTdp within wide circles. Our primary resolve that FTTdp must be considered seriously as a mainstream option for NBN deployment is significantly stronger today than in March. We believe a highly capable NBN outcome is achievable for the nation within appropriate cost and time constraints through deep-fibre FTTdp.

## A definition of deep-fibre FTTdp

There is no single definition of a copper network “distribution point”. As a consequence, FTTdp can have a variety of meanings. FTTdp is associated with larger “micro”-node devices of from 16 to 48 ports, as adopted in some deployment scenarios overseas. We are primarily

interested in the deep-fibre FTTdp concept, where fibre is deployed to the street lead-in pit. Small micro-node devices of 4 or 8 ports supply premises over existing copper lead-in twisted pairs from the pits. The average copper length is thus perhaps as little as 30m.

Deep-fibre FTTdp in this sense can be directly compared to the NBN Co FTTP architecture, with multi-port units being replaced by small reverse-powered (powered from premises over the lead-in copper) 4 or 8 port weather-protected (including immersion protection) micro-node devices mounted inside the lead-in pit. The associated reduction in fibre counts (a single fibre connects each micro-node device to the Fibre Distribution Hub instead of a multiple-fibre ribbon in the NBN Co FTTP architecture) provides flexibilities that minimise the need for pit and pipe rectification work. The avoidance of fibre premises lead-in deployment (by FTTdp exploitation of existing twisted pair copper lead-ins) allows substantial deployment cost and time savings. From the NBN Co Strategic Review (NBN Co 2013), a brownfields per-premises cost of \$3260 can be derived for the “Radically Redesigned FTTP” scenario. The per-premises fibre connection cost of \$2100 is largely avoided by FTTdp. (Connection costs remain, related to micro-node devices, customer premises equipment, and pit installation of FTTdp micro-node equipment, although these likely total a small percentage only of the \$2100 savings.)

The deep-fibre FTTdp approach results in a significant reduction in fibre count at the FDH (Fibre Distribution Hub). Ultimately this allows for a FDH enclosure that is greatly reduced in size, minimising street impact, and potentially allowing for pit-retractable designs.

For practical reasons related to efficient deployment, single port VDSL or G.fast devices may also be part of the deep-fibre FTTdp solution set. It should be clear that the lack of shared lead-ins from many pits implies that there is little need for vectoring implementation because there will be negligible cross-talk present. Consequently, serving multiple customers from a pit via single port devices is feasible, as is the adoption of 4 or 8 port micro-node equipment that may not implement vectoring functionality (where significant crosstalk and high line utilisation factors exist, vectoring becomes instrumental in delivering a superior overall outcome).

The deep-fibre FTTdp approach is a Passive Optical Network architecture up to the premises lead-in. As such, it is trivially upgradable on an individual premises basis to a FTTP connection. An NBN construction program based on FTTdp remains a “single build” solution to supplying the long-term communications demands of the nation. The cost and time savings in comparison to FTTP are extremely positive, and may translate favourably to a direct positive comparison between FTTdp and FTTN. VDSL2-based FTTdp, at circa 250 Mbps down and 50 Mbps up (or similar) provides a much higher level of baseline

connectivity than FTTN, and crucially provides economic means of connectivity upgrade for those premises requiring more.

This deep-fibre FTTdp approach, taking fibre to street lead-in pits, potentially aligns with the naturally emergent “fibre edge” of the network. An all-fibre network (FTTP) represents a particular vision of the future that many suggest is an inescapable reality on a long-term basis. However, there is no guarantee that the economics of fibre premises connections will compete with DSL approaches for connectivity demand levels that we can be confident of seeing from the vast majority of premises. We can, however, be certain that the fibre edge of the network will be significantly beyond the node (Telstra Distribution Area). Fibre running down local streets may thus be the natural edge of the fibre network, although another five years of progress might be necessary to provide any conclusiveness to such a prediction.

Deep-fibre FTTdp provides robust and flexible connectivity capabilities, economically meeting demands of all users, serving long-term network requirements, and avoiding the considerable cost of tailored civil works to deploy new fibre lead-ins to every premises. Heritage buildings are one example where concerns about the physical infrastructure associated with fibre lead-in deployment is a very 'sensitive' topic. In a more general view, the need for involved civil works through individual premises is a deployment situation that quickly leads to high cost and time delay. Existing, suitably short copper lead-ins, enable high connectivity outcomes with relatively minimal expense via VDSL2 or other related DSL technologies.

## Deep-fibre FTTdp compared to HFC

The NBN Co Strategic Review (NBN Co 2013) strongly suggested that the economics of exploiting existing Hybrid-Fibre-Coax (HFC) networks was sound. Almost 12 months later, little information has emerged from NBN Co to support the assertions of very low incremental costs to supply NBN services over extant HFC infrastructure. However, we must assume that there is merit to careful consideration of how the existing HFC assets might best be exploited.

John Goddard (Goddard 2014) outlines many of the elemental concerns related to incorporation of HFC assets in the NBN product mix. However, a concrete engineering road-map for HFC assets is yet to emerge from NBN Co. Large node sizes are a primary challenge for existing HFC assets to supply high connectivity levels across a wide customer base in the NBN application. The node size issue is seen as particularly relevant in conjunction with the likely addition of many new premises connecting to the HFC network within existing physical node boundaries. (As affordable and capable NBN services are provided over the HFC networks it is sensible to imagine a significant proportion of ADSL users will switch to

cable-modem NBN service in these areas.) The overlap of two distinct HFC network architectures is likely to present additional challenges.

More pragmatic matters are expected to relate to the difficulties in simultaneous operation of multiple networks over the HFC infrastructure (for example Foxtel and NBN) and the related issue of which entity retains update control of relevant CPE (Customer Premises Equipment). The installed capability of the HFC backbone fibre network, and the ready extensibility of the downstream fibre infrastructure (ease of node splitting and driving fibre deeper into the network) are key details that only a few select individuals are likely to properly appreciate. The difficulty is not that a path forward does not exist. CableLabs standards and global cable industry best practice provide the necessary capability augmentation route. A lack of complete appreciation of the current state of the HFC networks, and the associated uncertainty of upgrade cost estimates is the key concern. Ultimately the difficulty and costs associated with NBN Co exploitation of the HFC infrastructure may be dramatically in excess of those suggested by the 2013 NBN Strategic Review.

As HFC infrastructure was initially deployed, the goal of supplying as many as 2000 premises on a node would have been seen as an impressive engineering achievement. We don't claim that the average number of premises per HFC node is as high as this, and note that Goddard suggests 200 is a more sensible figure. A percentage of HFC nodes may of course contain significantly more than the average number of premises. A high number of premises connected to a node is a present and future engineering challenge for data service delivery. GPON architectures typically settle on maximum sharing of the access network across 32 premises (the NBN Co approach doesn't even fully populate to this level initially). This small number of premises per node represents an efficient engineering trade-off between anticipated demand growth, expected active component upgrade cycles, and the cost of deployment of even higher fibre counts throughout the LNDN (Local Network/Distribution Network). While HFC networks may never require node sizes as small as this, a massive reduction in node size is likely to be necessary on a relatively short time-frame. High levels of sharing have a very real impact on overall Quality of Service. The quantum of work required to deliver sensible node sizes to HFC networks must ideally be contrasted with the alternatives involving new LFN (Local Fibre Network) deployments (one such option being the deep fibre FTTdp approach).

Allowing that use of HFC assets may have a valuable role to play in the NBN, HFC coverage infill areas might also present prospects for FTTdp. We should note that aerial cabling deployment options would most likely favour HFC infrastructure or FTTP. NBN Co CEO Bill Morrow, when discussing HFC recently (Dobbie 2014), appears to suggest that the cost of aerial customer connection is so low that we must rightfully ask whether aerial FTTP must

once again be more widely considered for the NBN. However, Bill Morrow's comments might also ultimately be found to be overly optimistic in this regard.

Even a 20% proportion of premises lacking a lead-in may translate to favourable economics for alternative approaches in HFC coverage areas. Clearly detailed costing analysis is required prior to making any solid conclusions in this regard. However, we note that history of the Australian cable TV and cable modem market sectors, combined with competing ADSL offerings, implies that many premises lead-ins would need to be constructed in the NBN HFC scenario. As lead-ins are added there is risk of DOCSIS (Data Over Cable Service Interface Specification) node overloading, contributing to declining service levels without additional HFC network investment. We must be realistic in admitting that while some premises report good cable modem service today, there are many reports of unsatisfactory service, especially in relation to peak usage time periods.

This paper focuses on deep-fibre FTTdp in contrast to FTTN. For similar investments of cost and time, FTTdp provides significant capability increase over FTTN. Importantly, FTTdp avoids the relative lack of an upgrade path from FTTN to higher capability outcomes. Any comparison between HFC and FTTdp is expected to be less conclusive than a comparison between FTTN and FTTdp. Some of the primary flexibility advantages of FTTdp compared to FTTN are loosely paralleled by abilities to incrementally upgrade HFC outcomes. This does not imply that detailed analysis won't determine FTTdp to be an economic option in HFC areas, but that our focus at present is a comparison between FTTN and deep-fibre FTTdp. We assume that, a priori, exploitation of HFC assets by the NBN is economically rational, but note that determinations in this regard must weigh long-term considerations in addition to more immediate concerns, and consider network flexibility in meeting the needs of high-demand customers. Without input to the contrary, FTTdp is perhaps best considered as a baseline alternative option in HFC areas.

## The upgrade path from FTTN

FTTN is reported as being capable of delivering 100 Mbps (downstream, and perhaps 40 Mbps upstream) at copper distances of up to 300 to 400 metres from the node. For larger distances the data rate decreases, but it is suggested that 50 Mbps may be possible at a distance of up to 800m from the node (VanHastel & Verlinden 2012). Of course, the reality of what is achievable depends on both the specific condition of the copper network from the node to the premises, and any in-building or in-premises copper configuration issues. We discuss the latter concern in more detail in a subsequent section.

The recent Alcatel-Lucent Vplus announcement (Russell et al 2014) promises improvement in capability over the first few hundred metres of copper loop length through exploitation of

a 30 MHz VDSL2 bandwidth from the node. However, as mentioned in the introduction above, obtaining advantage from Vplus, for more than a moderate percentage of premises within a node area, is likely to require deployment of smaller satellite nodes. The marginal cost versus benefit analysis for deployment of such nodes appears relatively unappealing compared to other options such as deep-fibre FTTdp, although the option clearly deserves closer analysis if only as a deployment reference case. How quickly Vplus can be adopted by the broader VDSL modem manufacturer ecosystem also remains to be seen. Even a requirement for a future flash upgrade of CPE will severely limit the ease of future FTTN augmentation via Vplus deployment.

For the 17 MHz VDSL2 deployment likely to be provided as part of the NBN, a minimum 50 Mbps download connection, coupled with an appropriate upload allowance of perhaps 20 Mbps, (note NBN Co is still focussed on a lower minimum of 25 Mbps download) offers a dramatic improvement in capability compared to average ADSL experience of around 6 Mbps. Most users would be happy with 50 Mbps (down) today, and there is good reason (Department of Communications 2014a) to suggest that there is limited overall willingness to pay for more (using analyses rooted in our current experience).

The NBN must, however, look to the future. The minimum horizon of interest is the several years to deploy the NBN, but a 10 to 30 year outlook is also necessary for such a national infrastructure project. While it is obvious that projections of bandwidth demand growth vary tremendously, there is only a need to look forward a few short years before we start to appreciate that the risk of being locked in to a 50 Mbps connectivity outcome is substantial. We can be certain, globally, that 4K video streaming to multiple concurrent devices per premises will become a reality for a significant number of premises within a very small number of years. While available CPU and memory capabilities allow some continuation of advances in video compression technology, we must conservatively assume a 4K video data rate of between 20 and 30 Mbps. The NBN is not simply a video entertainment system; however it would be an extreme mistake to underestimate the risk of locking the nation into a 50 Mbps outcome. We must ask what economic pathways exist to provide significant improvements in connectivity, assuming the nation has already deployed FTTN.

Within the FTTN model, there is a real prospect of exploitation of pair bonding to provide higher connectivity outcomes for a small proportion of premises that require improved bandwidth. This option might be expected to be of first interest to premises most distant from the node. There is a risk of spare pairs being exhausted quickly, even allowing for a reasonable percentage of premises disconnecting from the wired network (some Telstra Distribution Areas will fare better in regard to spare pairs than others). It is also not clear whether extant FTTN equipment is fully capable of seamless pair bonding on a significant scale. Assuming node equipment supports bonding and NBN Co software systems are up to

the task, we must also ask whether the additional copper management and maintenance requirements make this option economic. Any need to re-patch pairs at the node to ensure they are served by the same line card for bonding purposes (if we assume this might be a requirement), would rapidly detract from the economics of provisioning incremental bandwidth improvements from the node by pair bonding. Note that vectoring is readily able to occur across line cards, facilitated by exchange of a modest amount of vectoring data. It is difficult, but not impossible, to imagine a related data exchange process that would facilitate bonding of pairs served by different line cards.

There is also a prospect within the FTTN approach to gradually migrate to deeper fibre deployment by installation of micro-nodes of from 16 to 48 ports (as suggested by, but not limited to, the Vplus concept mentioned above), directly replacing ports serviced from the node. However, we might quickly imagine that such an approach has limited practical appeal. To reach any worthwhile number of such mid-size 'nodes', enough fibres would be radiating from the node to pass the street pits of a significant number of premises within the Distribution Area. The alternative approach of a GPON-based deep-fibre FTTdp solution has quite obvious appeal where this is the case, delivering a markedly improved overall network connectivity result.

The inescapable conclusion is that any significant upgrade to connection outcomes beyond what is possible today with vectored VDSL2 from the node, must necessarily involve a substantial deployment of fibre past the node. The prime candidate to achieve this is the deep-fibre FTTdp model where the twisted-pair copper lead-in network is exploited for the final few metres from the street pit to the premises.

FTTN provides a very poor economic outlook for any fibre-on-demand product offering from NBN Co. Demand variability, coupled with the low (or modest) level of capability supplied by FTTN, suggests latent demand for fibre-on-demand will be significant. However, the cost of provisioning such a service is likely to suppress such demand, potentially to the point of extinguishing it (the economics of fibre-on-demand within the FTTN model look spectacularly poor once limitations of the total pool of skilled staff are considered along with the need for NBN Co to undertake a special project for the benefit of just a few customers).

The failure to deliver a practical fibre-on-demand solution translates to a significant reduction in the time frame to when it becomes necessary to drive fibre past the node. The substantial sunk investments at the node provide no benefit to driving fibre past the node other than the fact that CPE at the customers' premises should provide an almost seamless transition to VDSL-based FTTdp. The only additional CPE requirement should be the provision of reverse power feed from premises to the micro-node devices in the lead-in street pit. Expensive FTTN cabinets with sophisticated cooling systems, mains powering, battery

back-up, and time-consuming copper patching work to existing node pillars, have an extremely short potential service life based on most (if not all) sensible demand-growth projections. At risk of repetition, while uncertainty about copper condition exists in determining what level of capability is provided by FTTN, the Shannon-Hartley theorem provides clear guidance on the maximum level of connectivity able to be achieved. We are unable to be as certain on the topic of future demand projection, but reasonable growth projections suggest there is little safety margin associated with FTTN delivery capability.

The considerable cost of provision and installation of FTTN cabinets, including the deployment time factor due to the high-level of technician skill required on the copper network, would translate to an appreciable amount of fibre deployment past the node in a lean FTTdp LFN (Local Fibre Network) model. Furthermore, exhausting the nation's available equity funding to deploy fibre only to the node level, risks the prospect of additional funding being absent should an upgrade from FTTN be required to meet growing demand in the near future. Clearly we are not able to determine what real appetite for equity funding the nation possesses, and the \$29.5 billion indicated in the April 2014 NBN Co Statement of Expectations (Department of Communications 2014b) does not necessarily reflect the nation's equity limit. The key point is the rationality of careful determination on expenditure that provides a limited future benefit. Such expenditure may be justifiable, but without systematic due diligence the nation can not necessarily claim it is justified expenditure.

## The migration challenge

Migration of users and services from the existing copper network to any NBN network presents a number of challenges that must be considered carefully from an overall systems engineering perspective. The issue of how to optimally allow cut-over for a large number of independent end-users, operating via a broad collection of RSPs (Retail Service Providers), and making NBN connection decisions at varying times, is a major concern. It is not difficult to imagine that options relating to systems flexibility in regard to migration approaches, are likely to translate to enormous overall systems deployment cost differentials. A primary consideration is the cost of a truck roll and minimising the total number of necessary truck rolls within practical constraints of workable (and available) support software (OSS – Operations Support Systems, and BSS – Business Support Systems).

It is important that a holistic systems engineering perspective is taken with regard to the cost of truck rolls. The use of NBN Co marketing power to negotiate favourable contracts may translate to an NBN Co book cost of truck rolls that is below a sustainable level to the independent contractors working at the installer level. Pushing systemic inefficiencies of truck movements between widely varying locations onto the independent contractors may cause a false valuation of key engineering options that might otherwise provide an overall

benefit to the NBN. Implemented cost structures that prove unsustainable are ultimately likely to be identified and rectified. The most substantial risk is where costing errors are instrumental in deployment decisions, and the crucial point is that a holistic engineering perspective should aim to avoid such errors. The complexity of the migration challenge ensures this remains a non-trivial task.

Legacy services operating over the copper network also present significant migration challenges. The NBN Co approach to solving both this and the basic migration problem has centred on allowing an 18 month window where the new NBN FTTP network is operated in parallel with the existing copper infrastructure. A similar parallel network scenario is possible with both FTTN and FTTdp. In both cases copper connectivity is readily provided to the exchange for legacy telephony services including ISDN by the use of small line filter/splitter devices. Maintaining legacy ADSL services presents somewhat more challenge.

The VDSL standard has been designed to be interoperable with ADSL, with effectively identical modulation format over the ADSL band. Consequently VDSL implementations readily provide ADSL connectivity. However, migration of individual RSP ADSL services supplied from the exchange to the node or micro-node would most certainly be a non-trivial undertaking. Fortunately the impact of the ADSL bandwidth on VDSL vectoring is comparably minor, allowing legacy ADSL services to be supplied from the exchange as vectored VDSL is provided from the node. A disadvantage of this approach is that new VDSL service connections require attendance at the node for copper connection. Fortunately it is possible to pre-deliver a customer VDSL modem that will default to the customer's ADSL configuration until such time that the new VDSL connection is established, minimising the service disruption experienced by the end user. Of course this requires access to legacy ADSL username and password settings that most end users do not have at their fingertips, but presumably competitive RSPs will seize the opportunity to deliver superior customer service.

Further improvements in the migration approach that reduce the overall level of truck rolls may be possible through judicious use of splitter devices that allow ADSL services to be served from the exchange initially. Even non-ideal or partial solutions to the migration challenge that allow greater batching of work at the nodes, are likely to make a major contribution to the NBN bottom line. We note that G.fast is designed to interoperate with legacy ADSL and VDSL services through optional notching out the lower portion of the transmission bandwidth as required. The greater modulation bandwidth of VDSL2, at 17 MHz for FTTN and 30 MHz for FTTdp, compared to the 2 MHz bandwidth of ADSL, enables similar operation, even if the original VDSL standard appears to have not anticipated such a deployment scenario (the authors have not been able to identify specific VDSL2 bandwidth profiles designed to support this use).

## LFN architecture for FTTdp

Consideration of FTTdp quickly reveals prospects for major LFN architecture change compared to that already considered by NBN Co for FTTP (NBN Co 2012). Deep-fibre FTTdp is most obviously closely aligned with a multi-stage split LFN architecture. Compared to the base case of the NBN Co FTTP architecture, a significant reduction in fibre counts is obtained.

NBN Co Type 2.1 architecture runs 12-fibre ribbon cables from the FDH (Fibre Distribution Hub) in what is effectively a star configuration. The “radically redesigned FTTP” scenario introduced in the NBN Co Strategic Review reduces the overall fibre count, and we can easily speculate that this architecture might entail use of 6-fibre ribbon cables, but we ignore this as the base comparison case due to lack of specific published detail.

Cables of size varying from 72 to 288 fibres are used in the Type 2.1 architecture for the LFN. The 72-fibre cable has six ribbons of 12 fibres each, and is thus capable of supplying six multiport devices, presumably in six different pits. The 288-fibre cable likewise serves up to 24 street pits. Directly translating this to the FTTdp situation, we would presume the need for LFN cables of between 6 and 24 fibres. Such smaller and lighter fibres present a greatly improved outlook for ease of physical deployment. There is no primary difference in the optical budget or physical reach of the GPON (Gigabit Passive Optical Network) system in the two LFN architectures of FTTP or FTTdp.

Without an individual fibre from each premises back to a centralised FDH cabinet, there is a minor loss in capability with regard to balancing the load across individual GPON circuits. In the scenario where FTTdp micro-node devices remain the dominant connectivity medium for a significant duration, the concern of loss in such 'perfect' flexibility is moot. With a centralised primary stage split architecture we still retain the ability to balance GPON circuits to the level of the micro-node device. In reality the benefit arising from balancing GPON circuits beyond this level is only likely to be applicable to very high usage customers. Such customers would presumably be prepared to pay modest additional fees to have priority access to select reduced fan-out or otherwise low use GPON circuits, facilitated by spare fibre capacity in the LFN cables. We also need to appreciate the fact that the level of future need for GPON circuit balancing may be offset by other fibre-optic technologies such as the use of additional wavelengths over the existing PON (Ovum 2014).

A small amount of additional fibre capacity in LFN cables enables an extremely low-cost option where balancing GPON circuits above the level of the micro-node devices becomes desired. Such might be envisaged where neighbouring high-demand small business enterprises share FTTdp service from the same pit. Noting that the FTTdp GPON link is able

to support an average of 100/40 Mbps service for 25 simultaneous users, it is only where an individual premises upgrades to a fibre (or G.fast link) and utilises this at high capacity for a large fraction of time that statistical GPON limitations are likely to be experienced. Two such high-demand premises served from neighbouring pits presents no difficulty in the centralised splitter model for balancing the GPON circuits. When such high demand users are served from a single pit, a spare fibre can be used to allow the premises to be served on separate GPON circuits.

Perhaps more radically, a non-centralised primary splitter architecture is able to reduce LFN fibre counts even further. In the more extreme case, a primary 8-way split, with micro-nodes serving on average 4 premises, 6 fibres can maximally serve 24 pits. Being this lean on the fibre count does potentially impact our ability to easily balance GPON circuits, and such a fully distributed primary split architecture perhaps has little overall value. On the other hand, some element of non-centralised primary splitter architecture may be of interest, and we attempt to elucidate this in the following paragraphs.

A fully connectorised splitter array in a central location under the FTTdp model is reduced in size by at least a factor of 4 compared to the NBN Co FDH approach (splitter unit size is effectively determined by number of connectors). Design attention focussed on minimal physical size is likely to provide further benefit, and the prospect of a primary splitter array that is fully retractable into a pit becomes entirely feasible. The elimination of street furniture impact and the avoidance of damage from errant vehicles, etc., is a positive result that merits serious consideration. However, a splitter architecture fully mounted in existing pit infrastructure (thus providing substantial deployment cost and time savings) becomes possible once a very small distribution of splitter components is allowed.

The physical fan-out of fibre bundles from a FDH location provides for locations where a small number of splitter units might be readily mounted in a semi-distributed fashion. Excess fibres linking the distributed splitter locations can supply the ability to balance GPON loads to the limited extent that this might be deemed an important capability. While it may seem anathema to those heavily indoctrinated in the NBN architecture as seen to date, the use of fully spliced splitters is also worth consideration. Technologies such as spider-web ribbon (Takeda 2014) make it possible to tease out a single fibre in the situation where it becomes desirable to migrate users from one splitter to another. A departure from Nielsen's Law exponential demand growth (Nielsen 1998), to more conservative bandwidth demand growth projections, suggests that the need for shuffling users between splitters might be rare enough that the overheads of a fully connectorised solution are entirely unjustified.

The advantages of having a single small, flexible fibre cable option for deployment in the LFN are obvious. A 24-fibre spider-web ribbon solution (in say six groups of 4 fibres)

provides ample convenience and flexibility to meet the demands of any particular LFN layout. The supply logistics side of the deployment is greatly simplified by such an approach. Some fibre network nodes in the LFN may naturally suggest multiple fibre cables deviating at the node, while others may be optimally suited to insertion of splitters. Whether ultimately using field-installable connectors, fusion-spliced connectors, or direct-splice connections, tapping into a single fibre cable variant is a skill quickly mastered by the NBN Co installer army. A clear division of labour is possible between teams laying fibre, those connecting passive network devices, and those connecting the active micro-node devices.

For low take-up areas there is unlikely to be any advantage to pre-installation of micro-node devices in pits prior to service orders being received. In the case of a single-port FTTdp device being deployed, there is obviously no reason to pre-install the active equipment. (The use of single port active components presumably requires a second-stage splitter installed at the pit with at least the second service delivered from the pit, or requires additional LFN fibre capacity and a reversion to the larger centralised split approach of the existing NBN Co FDH architecture.)

In summary, there are many reasons to expect significant LFN fibre deployment gains to be achieved with the deep-fibre FTTdp paradigm. The gains are importantly both in terms of cost and deployment time, compounding the cost and time gains made by avoiding fibre premises drops.

## The FTTdp equipment ecosystem

FTTN equipment is of sufficient overall complexity to provide a largely prohibitive barrier to market entry for many otherwise capable suppliers. While no single element of a node device provides inordinate difficulty for a new market entrant, to be able to provide sales of volume to offset engineering development costs, a high level of customer confidence must be created in all elements. The established market players thus have a considerable advantage in FTTN node equipment.

An associated issue is the reduced prospect of a mixed vendor model for FTTN node equipment. Different vendors are likely to provide units that are functionally equivalent at a primary level, but from an installation and operational perspective, any collection of subtle differences translates to a potentially large cost overhead in dealing with multiple equipment configurations. Ultimately this reduces the number of suppliers actively exploited by NBN Co, and has an impact on the ability of NBN Co to negotiate favourable equipment pricing from any major vendor. However such issues are not without precedent in telecommunications networks, and ways to (at least partially) mitigate such effects are possible.

In contrast, the small micro-node devices of deep-fibre FTTdp present a far-simplified set of possible specifications. The prospects for exploiting functionally identical equipment from a large range of suppliers is very real. The overall simplicity of micro-node devices ensure that the production of a superior product is within reach of many companies, and there is relatively little advantage gained by the more traditional equipment suppliers in this space. Examples to illustrate the level of activity in this sector of the industry are the young start-up Sckipio (Sckipio 2014), and the partnership announced at the October 2014 Broadband World Forum between TE Connectivity and Technicolor (Technicolor 2014). Ultimately the intense activity in this sector of the market translates to likely availability of equipment at reasonable prices and high functionality, today or in the very near future, with a steady improvement in the supply equation expected over the coming years.

The passive-cooling requirement for small micro-node devices ensures that minimisation of power consumption is a primary design requirement. Lantiq (Lantiq 2014) indicates a single-port device may consume 6 Watts. A reasonable expectation is that multi-port devices would have an improved consumption figure on a per-user basis, but even at 6 Watts it is clear that the “green credentials” of the deep-fibre FTTdp option are positive.

We must note that NBN Co might benefit from leading market specifications for FTTdp micro-node product solutions. There is little risk from doing so for such a comparatively simple component, and the upside benefit could be significant. Alternatively, the global industry is likely to supply highly capable devices that closely match the needs of the Australian NBN, even though application of deep-fibre FTTdp may differ slightly in overseas deployment settings.

The high cost of labour in the Australian context produces an inordinately high cost of fibre connections to premises. In turn this suggests that the prospects for deep-fibre FTTdp are very positive in the NBN setting. A reduced deployment cost of fibre premises drops in overseas settings may suggest that the economics of FTTdp are less positive. However, in environments where duplicate or competing local connectivity infrastructure exists, competitive forces from the end-user perspective, or the reduced possibility of sufficiently long-term end-user commitments, are likely to also drive deployment of deep-fibre FTTdp options. Such overseas deployments provide a healthy FTTdp industry ecosystem, and is thus good news for the Australian NBN.

The recent October 2014 Broadband World Forum in Amsterdam, revealed significant FTTdp announcements from Alcatel-Lucent (Alcatel-Lucent 2014), TE Connectivity/Technicolor (Technicolor 2014), and Sckipio (Sckipio 2014). Other well-known suppliers such as Huawei (Techweek 2013) and Adtran (Adtran 2014) are also active in the FTTdp

product space. It is clear that there are positive global movements towards deep-fibre FTTdp, with strong reasons to expect rapid developments in this market over the next two years.

## The in-building copper configuration issue

In-Building or in-premises copper configuration can be a significant issue for DSL-based technologies. The prospect of bridge tap configurations is high in some building and premises settings. The detrimental impact bridge taps have on the overall spectral response of the DSL channel can be enormous. In-building copper wiring can also pick up large amounts of impulse noise, with this being repetitive impulse events in many cases. Cross-talk in shared copper bundles can translate impacts from impulse noise from one premises to other premises in a small percentage of cases.

Many modern premises operate with a single Telstra socket outlet employed for DSL modem/router and cordless phone. The ideal DSL outcome would be achieved in the situation where the Telstra socket employed for such purpose was the first Telstra entry point in the premises, with the remainder of the in-building copper wiring disconnected. Any alteration of in-building wiring work is a licensed cabling activity and thus requires professional attendance inside premises or to common building areas in the MDU (Multiple Dwelling Unit) setting. While the cost of such copper rectification work may be readily passed to premises owners or bodies corporate, it still represents a real cost component of the NBN. Additionally, any skilled staffing requirement needed for such network-edge deployment tasks is likely to extract suitable staff from the core NBN network deployment pool, ultimately raising costs and slowing the deployment.

It is important to appreciate that access to in-building wiring may be a simple task in some situations. Perhaps the most simplistic case is where the first Telstra socket (Telstra copper entry point) is opened to simply disconnect any additional household twisted pair wiring. Some percentage of cases can be expected to have wiring junctions more deeply buried within the building structure, whether that is within walls, above ceilings, or under floors. Tragedies related to the recent home insulation scheme should remind us that the cost of professional rectification works can rise sharply due to Occupational Health and Safety/ Work Health and Safety precautions in many situations.

In the MDU setting an additional difficulty is that cooperation may be required between premises owners and the body corporate. While it is likely that the desires of many premises owners would be similar, and hence the bodies corporate should be agreeable, there will be some cases where this ideal is not readily obtained. In the situation where access to all building risers is necessary to fix systemic building copper issues, the prospect of installing new building cabling of some variety (CAT6, Coax, or Fibre) needs consideration. It would be

a massive undertaking for NBN Co to expect to deliver a single optimised service to all MDUs in this regard. However, the scope for specialised industry providers targeting such services in a competitive industry fashion, directed by bodies corporate, is exciting.

As FTTN and FTTdp are both reliant on DSL, it is natural to expect that they both involve similar costs associated with in-building copper rectification works. However, there are reasons to expect that the FTTdp scenario obtains a significant reduction in the overall costs of such rectification work. Firstly, the ability to economically route a new fibre service from the street pit effectively caps the in-building copper rectification cost. Secondly, the very short FTTdp copper length provides maximisation of the DSL connection capability even in the presence of in-building bridge taps or poor copper joints. Thirdly, the reduced use of shared copper bundles inherent in FTTdp translates to a marked reduction in the potential for adverse impacts on other premises to be generated by undesirable wiring configuration in any single premises (such as where significant impulse noise is collected).

Importantly, any reduction or delay in the call on licensed cabling professionals to perform in-building copper rectification works, allows such skilled staff to be employed in the core NBN build.

An additional prospect with FTTdp is the potential for a significant reduction in the need for licensed cabling activities, assuming appropriate changes to regulations. While a need for regulation and licensing of cable installers will continue with FTTdp, it is reasonable to expect that this may be at an appreciably reduced level. In-building cabling has a smaller association with the broader communications network under FTTdp, and the associated risk of detrimental impact is considerably reduced (albeit non-zero). Ultimately any efficiency-based simplification of cabling regulation and licensing can help to widen the overall pool of skilled resources, improving the cost and time outlook for the national NBN build. The weighting to any benefit that might be obtained in this area is low due to the fact that regulation changes are assumed to be necessary, and an optimal migration strategy may involve a long-term connection of the in-premises copper network to the existing exchange network, thus negating any potential for significant regulation and license simplification.

## The threat from wireless networks

There is little disagreement that wireless and wire-based (predominantly fibre) networks provide complementary services. The promise of improved wireless connectivity continues to lure a selection of media commentators into thinking that wireless is a panacea. The reality is that many premises will retain a need for a fixed-network connection. A growing number of premises may be able to satisfy their demands (usually where these demands are

significantly lower than average) solely and economically by wireless access provided by non-NBN Co commercial entities. This presents a threat to all NBN Co access technologies.

The large capital investment (and time investment) in FTTP implies that the technology evolution risk from wireless development is significant. Any reduction in revenue as users migrate away from the NBN is particularly problematic in the FTTP model where premises may connect (incurring the hefty connection costs for NBN Co) and yet within as little as two years determine that they are better served by commercial (non NBN Co) wireless services. The elevated ARPU (Average Revenue per User) required by NBN Co limits its ability to minimise such losses through competitive pricing.

The lower overall deployment cost and time for FTTN and FTTdp network options presents an improved picture. However, the proportion of premises abandoning the NBN in favour of commercial mobile wireless services can be expected to be higher in the situation where the NBN is seen to provide limited additional value. The quantum of risk is greatest in the FTTN case, where although monthly NBN data quotas are likely to be higher than commercial mobile services for the foreseeable future, peak download rate is likely to be a more meaningful determinant of service quality for many users.

The argument as to the relative importance of peak download rate versus streaming throughput capability is a very complex one, on which we are unlikely to be able to obtain significant consensus at present. The recently completed NBN Cost Benefit Analysis (Department of Communications 2014a) can certainly be excused for largely neglecting the consideration. The graphics shown on page 107 and 167 of the CBA report can be interpreted as accommodating the issue of peak download rate via translation by 'expert' opinion to an equivalent streaming rate. The 15 Mbps shown for software updates illuminates the point. In many cases software update download occurs in the background and a download rate as low as a fraction of percent of the stated 15 Mbps would suffice. However, there are other situations where a software update prevents work from commencing or continuing, and in this case update responsiveness is a crucial usability factor. For the purposes of the CBA Choice modelling, 15 Mbps appears to be sensible compromise figure, but it clearly risks oversimplifying the analysis.

Of more material impact on the outcomes of the CBA choice analysis is clearly the figure shown for 4K TV streaming. This is shown on page 107 as 30 Mbps, yet is modified on page 167 (as used in the choice study) to 20 Mbps. The present point is that it is clearly a difficult task to obtain reliable input on streaming throughput requirements. It is probably prudent to remain open to the prospect that high peak data rates may provide benefits that are even more difficult to attempt to quantify. The threat from wireless networks is that by providing high peak data rates (5G Wireless, etc.), there may be a significant associated usability

improvement experienced by some users. The 25 Mbps minimum suggested in the NBN Co Statement of Expectations is low enough that it may cause concern in this way.

Optimal NBN Co deployment decisions must weigh the likely threat from wireless advances. It is suggested that a proper analysis will lean toward the higher capabilities of the deep-fibre FTTdp option as part of considering the future wireless threat.

## Conclusion

For brownfield underground distribution areas, the deep-fibre FTTdp approach supplies overall network capability effectively identical to that provided by FTTP at a substantially reduced cost. In greenfield areas and in overhead distribution areas, reduced benefits (in the sense of limited cost improvements compared to FTTP) are provided by deep-fibre FTTdp, leading to the probable preference for full FTTP in these areas.

It is less clear that FTTdp has a significant role to play in HFC areas. However, while the basic promise of exploiting existing HFC infrastructure is sound, practical realities may ultimately dictate that FTTdp has a role, even if in niche areas within the overall HFC footprint. Certainly FTTdp, and FTTP in aerial deployment areas, should be considered as baseline cases against which any HFC investment is compared. HFC investment based solely on immediate returns may incur a risk of inferior long-term outcomes. Short term priorities must be weighed appropriately with an understanding of network flexibility and broader life-cycle costs and benefits.

Outside of HFC deployment areas at least, the deep-fibre FTTdp approach fosters a substantial re-think of the LFN architecture. The prospect for dramatic cost and time savings in this part of the deployment is enormous and exciting in terms of the overall NBN outcome. The LFN architecture ideas introduced within this paper are not intended to be suggestive of an optimal approach, as there are many factors to consider in determining an ideal architecture. However, the ideas proposed should help to delineate some of the many considerations that require more careful analysis by NBN Co or a related entity charged with maximising deployment outcomes. A field trial by NBN Co of FTTdp installations would also help to focus on the optimal approach to detailed deep-fibre FTTdp architecture.

The Deep-fibre FTTdp approach has validity well beyond that of the Australian context. However, some peculiarities of the Australian deployment environment (primarily high labour costs, relative lack of competing infrastructure, and large Telstra distribution areas) suggest that this form of FTTdp is likely to have particular applicability to our nation's NBN. By fully embracing FTTdp, the nation may achieve an optimised NBN outcome of which we can be justifiably proud.

## References

- Adtran, 2014. 'Accelerating Gigabit Broadband: A FTTdp White Paper', Adtran, 2014, available at: <https://www.adtran.com/web/fileDownload/doc/32246>, retrieved October 24, 2014
- Alcatel-Lucent, 2014. 'Alcatel-Lucent's new G.fast solution to help operators provide more subscribers with ultra-broadband access', Alcatel-Lucent Press Release, October 21, 2014, available at: <http://www.alcatel-lucent.com/press/2014/alcatel-lucent-s-new-gfast-solution-help-operators-provide-more-subscribers-ultra-broadband-access>, accessed October 24, 2014
- Russell, K; Spruyt, P; VanHastel, S. 2014. 'Vplus gets more out of VDSL2 vectoring', *Alcatel-Lucent TECHzine*, October 16, 2014, available at: <http://www2.alcatel-lucent.com/techzine/vplus-gets-vdsl2-vectoring>, accessed November 22, 2014
- Department of Communications. 2014a. 'Independent cost-benefit analysis of broadband and review of regulation: Volume II – the costs and benefits of high speed broadband', available at: [http://www.communications.gov.au/\\_data/assets/pdf\\_file/0003/243039/Cost-Benefit-Analysis-FINAL-For-Publication.pdf](http://www.communications.gov.au/_data/assets/pdf_file/0003/243039/Cost-Benefit-Analysis-FINAL-For-Publication.pdf), August 27, 2014, retrieved September 3, 2014.
- Department of Communications. 2014b. 'Statement of Expectations', April 8, 2014, available at: [http://www.communications.gov.au/\\_data/assets/pdf\\_file/0014/221162/SOE\\_Shareholder\\_Minister\\_letter.pdf](http://www.communications.gov.au/_data/assets/pdf_file/0014/221162/SOE_Shareholder_Minister_letter.pdf), retrieved April 14, 2014.
- Dobbie, Phil. 2014. 'Bill Morrow with NBN Co's reality check', Crosstalk, October 23, 2014, available at: <http://phildobbie.com/main/podcasts/crosstalk/item/1343-bill-morrow-with-nbn-s-reality-check>, accessed October 24, 2014
- Goddard, John. 2014. 'The Untapped Potential of Hybrid Fibre Coaxial Networks', *Australian Journal of Telecommunications and the Digital Economy* 2(2) pp. 17.1-17.7, DOI: 10.7790/ajtde.v2n2.40. Available at: <http://telsoc.org.au/journal>, accessed October 24, 2014
- Hirscher, Stefan. 2014. '300 Mbps over Copper: VDSL2 FTTdp Delivers the Future, Today', available at: [http://www.lantiq.com/fileadmin/products/201404\\_Lantiq\\_VDSL\\_FTTdp\\_with\\_VINA\\_X\\_TM\\_dp.pdf](http://www.lantiq.com/fileadmin/products/201404_Lantiq_VDSL_FTTdp_with_VINA_X_TM_dp.pdf), retrieved October 24, 2014
- ITU. 2013. 'New ITU broadband standard fast-tracks route to 1Gbit/s: G.fast capitalises on existing copper to deliver fibre speeds at lower costs', ITU Press Release, December 11, 2013, available at: [http://www.itu.int/net/pressoffice/press\\_releases/2013/74.aspx#.VHAU9IWUfCI](http://www.itu.int/net/pressoffice/press_releases/2013/74.aspx#.VHAU9IWUfCI), accessed November 22, 2014
- Lantiq. 2014. '300 Mbps VDSL Right Now – Lantiq Introduces New Fiber-to-the-Distribution-Point Solution', available at: <http://www.connectionsplus.ca/press-releases/300-mbps-vdsl-right-now-lantiq-introduces-new-fiber-to-the-distribution-point-solution/>, accessed October 24, 2014
- NBN Co. 2013. *Strategic Review, Final Report* (with redactions). Available at: <http://www.nbnco.com.au/content/dam/nbnco/documents/NBN-Co-Strategic-Review-Report.pdf>, retrieved December 12, 2013
- NBN Co. 2012. *Network Design Rules*. Available at: <http://www.nbnco.com.au/content/dam/nbnco/documents/network-design-rules-2012.pdf>, retrieved November 22, 2014

- Nielsen, Jakob. 1998. 'Nielsen's Law of Internet Bandwidth', available at <http://www.nngroup.com/articles/law-of-bandwidth/>, accessed January 12, 2014
- Ovum. 2014. 'TWDM PON Is on the Horizon: Facilitating fast FTTx network monetization' Ovum, 2014, available at: [http://info.ovum.com/uploads/files/TWDM\\_PON\\_white\\_paper.pdf](http://info.ovum.com/uploads/files/TWDM_PON_white_paper.pdf), retrieved October 24, 2014.
- Sckipio. 2014. 'World's First 16-Port G.fast Demonstration Shown by Sckipio at Broadband World Forum', Sckipio Press Release, October 21, 2014, available at: <http://www.sckipio.com/worlds-first-16-port-g-fast-demo>, accessed November 24, 2014
- Takeda D; Isaji, M; Tomikawa, K; Osato, K; Yamanaka, M; Okada, N. 2014. 'Ultra-High-Density Optical Fiber Cable', Fujikura Technical Review, 2014, available at: [http://www.fujikura.co.jp/eng/rd/gihou/backnumber/pages/\\_icsFiles/afieldfile/2014/07/04/43e\\_02.pdf](http://www.fujikura.co.jp/eng/rd/gihou/backnumber/pages/_icsFiles/afieldfile/2014/07/04/43e_02.pdf), retrieved November 22, 2014
- Technicolor. 2014. 'Technicolor: Frontrunner in next-gen ultra broadband technologies that boost the speed of your network'. Available at: <http://newsletterstack.technicolor.com/workspace/uploads/images/next-gen-ubb-technologies-final.pdf>, accessed November 22, 2014
- TechWeek Europe. 2013. 'BT To Trial Huawei G.fast FTTdp Copper Broadband Technology'. available at: <http://www.techweekeurope.co.uk/news/huawei-gfast-fttdp-copper-bt-129855>, accessed January 8, 2014
- VanHastel, S; Verlinden, J. 2012. 'VDSL2 Vectoring Delivers on its Promise'. Alcatel-Lucent TECHzine, September 17, 2012, available at: <http://www2.alcatel-lucent.com/techzine/vdsl2-vectoring-delivers-on-its-promise>, accessed November 22, 2014
- Watkins, C; Lillingstone-Hall, K. 2014. 'The FTTdp technology option for the Australian National Broadband Network', *Australian Journal of Telecommunications and the Digital Economy* 2(1), March 2014, available at: <http://doi.org/10.7790/ajtde.v2n1.26> Available at: <http://telsoc.org.au/journal>, accessed October 24, 2014

## Australia's fixed broadband deficit

# Indecision around industry structure could entrench Australia's laggard broadband position

---

Gary McLaren

Principal at McLaren Williams Consulting

---

### Summary:

Australia's fixed broadband services performance and takeup is continuing to fall behind other comparable countries in international benchmarks. This is despite broadband being a hot topic of debate at three Federal Elections and the creation of a new broadband utility company by the Australian Government. The recent change of government, in 2013, prompted reviews into the structure of Australia's fixed telecommunications market. A move away from utility style broadband to infrastructure competition has been recommended but the Australian Government has not embraced such a move, preferring instead to keep the utility structure for fixed broadband. While the new Coalition Government is investing in more fibre infrastructure as part of its Multi Technology Mix, there is no commitment to build a 'deep fibre' network that would have 'natural monopoly' characteristics. Competition from new technologies, wireless and fixed, may limit the financial viability of the utility broadband provider. Indecision about the structure of Australia's broadband market is likely to continue to retard medium to long term investment in the fibre infrastructure needed to improve Australia's broadband rankings against its international peers.

### Introduction

Broadband is a key political issue in Australia. The last three Federal Elections, in 2007, 2010 and 2013, have seen Australian broadband policy as one of the key debating issues between the Labor and Coalition parties. At the core of this development is the awareness amongst the Australian public that we are lagging the rest of the world when it comes to broadband performance and quality. As in any vibrant democracy the political process has recognised this and sought to respond.

This article will look at how Australia has struggled to define a sustainable model for the fixed access sector of its telecommunications industry since the de-regulation and privatisation of Telstra in the 1990s. Australia, like many other countries, moved away from the public utility model for telecommunications as technology opened up opportunities for competition in the fixed telecommunication sector. However, the infrastructure competition

model failed to develop sufficient scale and momentum to create an environment where the private sector would invest in modern fibre based broadband fixed networks.

Instead, a Labor Government in 2009 decided that government should re-enter the market and fill the investment gap by creating its own new utility company to upgrade the nation's fixed telecommunications infrastructure. However, the tension between competition and utility frameworks for telecommunications continues to grow as the new Coalition Government grapples with upgrading the infrastructure at less cost within the same utility company structure.

## Australia's fixed broadband deficit

Australia has a proud history in telecommunications (Moyal 1984). The difficulty of providing basic telecommunications to all citizens in a country with huge geographical challenges and extremely low population densities was overcome by pioneering engineers and technicians by the mid 1970s. More recently, Australia has become a world leader in the takeup and rollout of mobile phone (OECD 2013) and, more recently, mobile broadband networks (Akamai 2014).

However now, some significant way into the 21<sup>st</sup> century, Australia is well behind the rest of the world in the delivery of modern fixed broadband telecommunications services. Australia's fixed broadband penetration is low compared to other OECD countries, ranking just 21 out of 34 countries and below the OECD average.

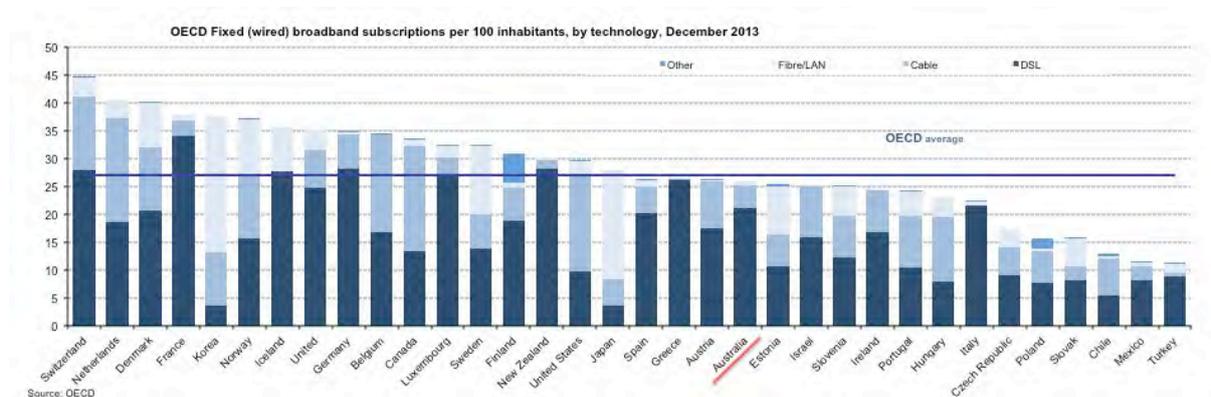


Figure 1 – Fixed Broadband Penetration in OECD countries (Dec 2013)

Average download speeds are also low, ranking 23 out of the 29 OECD countries reported on by Akamai.

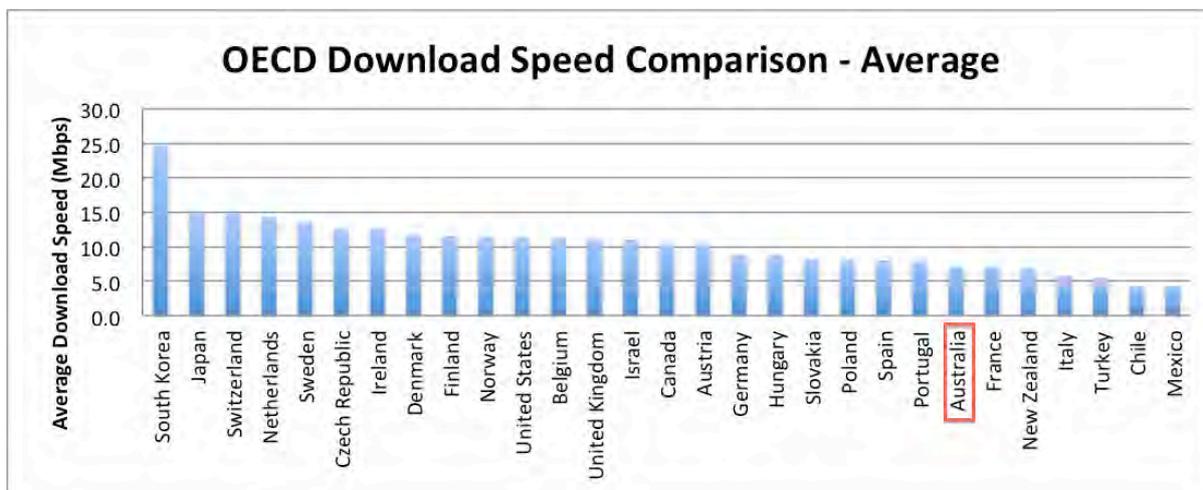


Figure 2– Average Download Speeds in OECD countries (2Q2014)

Peak download speeds are also low, with Australia ranking 21 out of the 29 OECD countries reported on by Akamai.

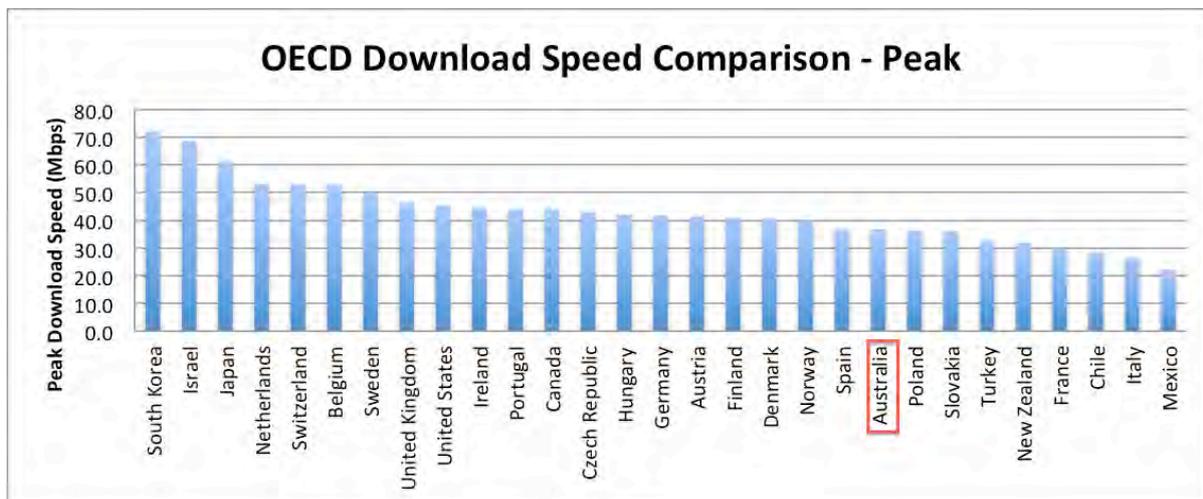


Figure 3– Peak Download Speeds in OECD countries (2Q2014)

This is not a recent phenomenon. Back in 2002, at the start of this digital century, the then Minister of Communications, Richard Alston was interviewed by Alan Kohler on the ABC's "Inside Business" program. When asked about the then recent reports showing Australia's broadband penetration was falling behind other leading countries by a significant margin, the Minister responded with "The fact is we're at the beginning of a very long race" (Australian Broadcasting Corporation 2002). Well, that race is still going now in late 2014 and Australia is probably further behind than ever.

Australia has since seen three Federal Elections, in 2007, 2010 and 2014, where broadband was a significant policy area differentiating the two major political parties. Broadband has become fertile political ground because the Australian public have become keenly aware of the country's broadband "deficit". Now, some 15 years into the 21<sup>st</sup> century, Australians are aware they are trailing in the "long race" towards a digital economy supported by access to high quality broadband.

## More fibre deployment necessary

Australia's fixed telecommunications network, built over many decades from the early 1900s, is predominantly a twisted-pair copper network purpose built to provide basic telephony services. In the 1990s and 2000s a range of technologies (initially ISDN and more recently DSL) were introduced to allow digital transmission of data over this copper network. Today's ADSL2+ services can achieve maximum peak download speeds of 24Mbps and upload speeds of 1.4Mbps. Speeds experienced by end users depend primarily on the length of the copper run from the telephone exchange to the end user. In its most recent report on broadband availability and quality in Australia, the Department of Communications reported that 4.62 million premises (or 47% of ADSL served premises) receive a median peak download speed of less than 9Mbps ([Department of Communications, Australia 2014](#)).<sup>1</sup>

More recently, Telstra and Optus have rolled out Hybrid Fibre Coaxial (HFC) cable networks, predominantly for subscription pay TV services. These networks are also broadband capable and with the latest DOCSIS3 technologies they can support download speeds of 100Mbps and upload speeds of 5 to 8Mbps. The major limiting factor for increased speed in HFC networks is contention on the cable segments that are shared by many users simultaneously.

Although the limiting factors in both copper and HFC networks are different, one being distance and the other being user contention, the solution to both is ultimately to install more optical fibre closer to the end user to reduce the copper distance or the number of users contending on a cable segment. In copper networks there are various FTTx acronyms describing the depth of fibre deployed to various points closer to the customer where various DSL technologies can be deployed. For HFC networks we are seeing the implementation of digital transmission techniques that enable a transition to Ethernet distribution technologies (rather than radio frequency channels), thereby lowering the upgrade and operational costs of deeper fibre HFC networks ([Salinger 2014](#)).

In fact this need for more fibre is common for all networks, even those using wireless spectrum such as mobile broadband or public WiFi networks. Ultimately, broadband quality

and performance is directly related to the degree or 'depth' to which fibre is deployed in any network.

So, Australia's problem with broadband quality and performance can only be solved by deployment of more fibre, 'deeper' into the network and closer to the end user.

But installing more fibre is a costly and time-consuming task. The job of designing, constructing and installing this fibre to run through the hundreds of thousands of kilometres of Australian suburbs and towns is daunting. It is similar in many ways to the building of the initial copper telephone network. In reality it is more difficult, as the suburbs and towns are now well established and it is costly to disturb these neighbourhoods in this day and age. The original copper network grew, more or less organically, with Australia's suburbs over many decades.

But this problem is common in most countries, especially the OECD group of countries that Australia is best compared with. How is the telecommunications industry approaching this challenge of the 21<sup>st</sup> century and more particularly what 'models' exist for the structure of the industry to create incentives to undertake this large, but important task?

## Utility Model

The first option to be discussed is the 'Utility Model'. Today's modern cities and towns owe their existence to three basic utilities that are provided to almost 100% of residences, namely electricity, water and sewerage. An optional fourth utility of natural gas is also available in many areas but not universally. These utilities were installed over decades, if not centuries, as the cities and towns grew. A mixture of government departments, government owned companies or heavily regulated private companies provide these utilities. Economists like to refer to these utilities as natural monopolies.

In many respects the original copper telephone network was built and managed as a utility service. In Australia, this was firstly done through the Postmaster General's Department (PMG), then by a wholly government-owned company (Telecom Australia) and more recently by the privatised Telstra. However, unlike the electricity<sup>2</sup>, water and sewage utilities mentioned above, the copper telephone network has come under challenge from newer competing technologies such as mobile and HFC networks. This development has been obvious since the 1980s and was part of the reason policy makers have moved towards privatisation and de-regulation of the telecommunications industry – that is, a departure from the public utility model for telecommunication infrastructure – as technical advances opened up possibilities for competition. The transition of telephony from being a utility service to an "application" provided over a broadband network has accelerated this trend.

But as we now move firmly into the broadband era, some are calling for a return to the utility model in telecommunications. Interestingly, much of this discussion is coming from the USA as part of the 'net neutrality' debate. The dominance of the cable companies in particular has caused concerns that their growing monopoly power requires utility-style regulation (Crawford 2013). President Obama has weighed in, arguing that the industry's regulator, the Federal Communications Commission (FCC), should seriously consider re-introducing the regulatory structures created for telephony into the broadband arena (Australian Broadcasting Corporation 2014).

Australia's 2009 National Broadband Network (NBN) policy predates some of this debate in the USA, but its wholesale only Layer 2 access model and anti-cherry-picking legislation is a definite 'utility' style framework. The goal was the creation of a monopoly broadband infrastructure network that would underpin a competitive retail or value added services market. In addition to creating a broadband utility company, the 2009 fibre to the premises (FTTP) version of the NBN was aimed at solving two fundamental problems in the Australian market. Firstly, it would remove Telstra's dominance of the fixed telecommunications market; and secondly it would provide the ultimate 'end-game' investment in fibre necessary to jump to the front of the broadband race internationally. Australia is not alone in following this approach – others countries such as Singapore and New Zealand are following a similar model.

An important aspect of this broadband utility model approach must, in the author's opinion, be a commitment to invest in a 'deep' fibre network that can satisfy the majority, if not all, the application needs for the next 30 to 50 years. Operators of competing technologies (such as mobile or public WiFi) would be permitted, encouraged and incentivised to use this 'deep' fibre network rather than build their own duplicate networks. Only a 'deep' fibre network can establish a true long-lasting natural monopoly by making the fibre network the most efficient (ie. lowest long-run average cost) for delivery of future broadband services. A broadband network that has limited deployment of fibre will suffer from the effect of 'cherry picking', where alternative technologies will be deployed to compete 'surgically' with the utility. This will have the effect of undermining the utility's economics by eroding its natural monopoly position.

The commitment to invest in a 'deep' fibre network need not require that such an investment be made immediately, but may instead involve the network rollout or implementation being made over a long period of time. The optimum timeframe should be determined by economic considerations. What is important is that the fibre investment should be done ahead of, or in line with the demand for broadband performance and not trail the demand. This will dissuade investment from cherry pickers who will be deterred by the risk of having their

early investment stranded as the utility broadband provider quickly deploys fibre networks ahead of demand.

Funding for the utility may come from the public or private sector, but in either case the investment rate of return will need to be regulated and monitored to ensure monopoly rents are not extracted. Furthermore, in most cases, especially in geographically challenged countries like Australia, government will have to provide or manage cross-subsidies or outright subsidies where the cost of such broadband deployments becomes intolerable on social equity of access grounds.

Australia's public telephony network was developed along such utility model lines by the PMG and then Telecom Australia. Much of the high-cost regional network was built during the Coalition's long post-war reign from 1949 to 1972. As Doyle recounts, "Country Party MPs excelled at channelling telecoms equipment and funds to rural areas and burying the ever-spiralling costs within the PMG's impenetrable network of cross-subsidies" (Doyle 2014). The Labor NBN model unashamedly borrowed this technique in its plans for NBN Co to build the fibre utility network to over 90% of Australian households and provide wireless and satellite services to the remainder. The "impenetrable network of cross-subsidies" would now be inside NBN Co rather than the PMG or Telecom Australia.

However, now in the early 21<sup>st</sup> century the utility model is out of favour amongst economists and most right-leaning politicians. Transparency and good governance demands that taxpayer funding of utility style infrastructure costs should occur only after extensive cost benefit analysis. Subsidies should be transparent and judged on the extra societal benefits they provide that are not captured by the pure economics. Both of these hurdles make a utility style telecommunications model very difficult to justify. Firstly, it is difficult to predict today what consumers and businesses will need in the future in terms of broadband performance. It requires a "leap of faith" to believe that high-performance broadband networks will stimulate more innovation in applications that will then make use of the higher performance that justifies the extra investment. The symbiotic-like growth in computing power, data storage and bandwidth over the last 20 to 30 years would seem to support such an argument. Technologists can see the opportunities for new applications – "if you build it they will come". But many economists will argue if you can't "see" the application – don't build the network.

Politically, the divide between left and right (or government intervention in markets on the one hand and free market policies on the other) will mean that the use of taxpayers' money to build and/or subsidise the cost of the network will be hotly debated. Arguments highlighting the high cost and risk of the rollout will be more tangible and easier to make compared to the (largely future-orientated) benefits of the applications made possible by

such a network. Extra societal benefits in such areas of education, health and transport are difficult to analyse and weigh up against the high costs.

Australia's most recent Federal Election in 2013 saw the defeat of the 'leap of faith' vision. However, the utility model is not dead and buried. As described further below, the new Coalition Government is continuing to pursue a utility model approach, primarily using existing network assets and technologies rather than committing to build a 'deep fibre' network.

## The Vertigan infrastructure competition model

As part of its reviews into the NBN after gaining power in the 2013 Federal Election, the Coalition Government created a panel of experts, the Vertigan Panel, to provide advice on the future structure of Australia's telecommunications market and in particular NBN Co.

In its last report, released in October 2014, the Vertigan Panel recommended that NBN Co's technology assets (FTTx, HFC, Satellite and Fixed Wireless) be disaggregated and eventually divested to different private sector owners. In essence, the Vertigan Panel has recommended that the Utility Model be disbanded and competition at the infrastructure level (in addition to the retail level) be pursued in Australia (Vertigan 2014). This would be a dramatic change in Australia's current telecommunications landscape, but not necessarily a new one for the country.

Firstly, Australia's mobile phone networks have essentially followed this model since the 1990s. Telstra, Optus, Vodafone (and for a time Hutchinson before merging with Vodafone) have built and operated separate competing mobile networks. Competition between these providers has stimulated both the marketing of services and new technology rollouts. Australia has some of the highest penetrations of mobile phones and mobile broadband in the world and has been a leader in the adoption of 3G and 4G/LTE technologies (OECD 2013).

Secondly, infrastructure competition has been a policy goal for the fixed telecommunications market since the de-regulation commenced in the 1980s. Some early infrastructure builds were attempted by Optus, Transact and Neighbourhood Cable but with limited success. Telstra through its domination of the retail market, its aggression in defending its control of access network infrastructure (particularly through its competing rollout of HFC in Optus HFC areas) and its alliance with content holders through its Foxtel partnership with News Ltd, has continued to hold significant, arguably dominant, market power in the Australian fixed telecommunications network.

Other comparable markets have seen their once dominant telecommunication incumbents become significantly less powerful than Telstra. Most face competition in significant areas of their network footprint from HFC networks. The effect of infrastructure competition in fixed broadband markets has been a clear increase in investment in more fibre networks in these markets. Incumbent telcos have rolled out FTTN and FTTP networks to avoid losing market share to other network technologies. The development of DOCSIS3.0 on HFC networks and delivery of 100Mbps download speeds has been the biggest spur for this investment. The opportunity for telcos to become media players and distribute content has also been a significant driver.

Economists favour such an infrastructure competition model. By letting the market decide the appetite for broadband and the necessary investment in fibre, economists will argue, such investments are more efficient and timely than via a utility model. Competition also spurs innovation and increases operating efficiencies between competing companies and technologies. There is no need to perform cost benefit analyses, as each competitor is in effect doing its own business cases based on a wide degree of factors and responding as they see fit in their best interests. Politically, the conservative right favours the infrastructure competition model. Taxpayers are not burdened with the cost and risk of the investment in fibre and the private sector investment is encouraged.

However, such a model needs to be actively managed to ensure that over time competition does not wane through mergers, acquisitions, agreements or market oligopolies. Government policy and regulators need to actively push against any tendencies towards market concentration given the high barriers to entry in telecommunication networks.

But what of the need for high-performing broadband infrastructure in regional areas that is clearly uneconomic due to the high costs associated with Australia's challenging geography? Absent any subsidy mechanism for the private sector, it is clear that a large proportion of Australia's households would not be able to afford the high costs of the services necessary to fund such investments. Economists will argue that subsidy schemes can be created to incentivise the private sector to build such infrastructure if this is required for social or political reasons. However, politicians on both sides of the political divide balk at the manner in which such schemes highlight the high costs of such subsidies, which inevitably must be borne by taxpayers generally or by the metropolitan households via higher telecommunication prices. The concept of such an explicit 'broadband tax' used to fund investment in regional telecommunication infrastructure appears to be a non-starter for any political party.

It would appear that it is this difficult policy and political question that it at the core of why Australia cannot embrace a move away from the old 'utility model'.

## The risks of a Multi Technology Monopoly

The Coalition Government has not yet embraced the Vertigan Panel recommendations to pursue infrastructure competition. It has in fact been actively seeking to discourage it via proposed licence conditions on superfast broadband networks ([Australian Government 2014](#)).

The current policy, described as the NBN Multi Technology Model, is essentially the old NBN Utility Model with the minimal fibre investment required to achieve minimum download speeds of 25Mbps for all and 50Mbps for 90% of the population. While this model may provide a quicker initial upgrade to Australia's broadband performance it leaves in doubt the longer term model for continuing investment in fibre infrastructure.

Of particular concern is the continuing monopoly characteristic of NBN Co under this policy. What incentive will NBN Co have to continue to invest in fibre infrastructure after achieving its broadband download speeds goals? NBN Co, although wholly government-owned, is run on commercial business principles and in particular is tasked with making a modest return on its investment. In this situation, the cost of more fibre investment will only be justified if it will mean less operational cost. But such an analysis depends entirely on the timeframe used. Over a long timeframe, say 20 to 30 years, the discounted operational cost of the increasing maintenance costs of copper and HFC networks, may be greater than the initial capital expenditure required to install more fibre infrastructure. But funding restrictions and technology risks will more than likely mean the timeframe is dramatically less, probably under 10 years. As a result the commercial business case will be hard to make.

NBN Co is likely to come under threat from small-cell wireless networks and cherry picking rollouts of fibre-based networks. In areas where this is a risk, NBN Co may respond by investing in more fibre itself. Or it may exit these markets, especially if it can access subsidies to cover shortfalls needed to fund obligations in other loss making geographies. The former scenario would stimulate investment in more fibre and would create some semblance of the infrastructure competition recommended by the Vertigan Panel, but at the same undermining the natural monopoly principles of the utility broadband provider. The latter scenario would leave the new entrants as the monopoly broadband provider with minimal incentive to invest in more fibre infrastructure when it is required.

However, absent such competing networks, NBN Co is likely to sit and wait after its initial MTM investment until higher speed benchmarks are mandated and additional government funding is provided. Such higher speed policy objectives will likely only come as a result of cost benefit analyses showing tangible benefits from applications that require such speeds that outweigh the costs. The applications with increased benefits will come from

international markets where higher speed networks will become the norm – not from Australia. Once Australians become aware of such applications they will demand the government do something about it and hence the cost benefit analysis ‘proof’ that further fibre investment is justified will only come well after Australia’s international competitors have the benefit of these higher performing broadband applications. Hence, after a process which will probably take many years after the new applications appear internationally, NBN Co will be given instructions and funding to increase its investment in fibre. The end result is Australia will continue to lag the rest of the world in its broadband network performance.

If NBN Co is privatised under the Multi Technology Model approach we can probably expect this process to take longer and maybe even stall. On reflection this is actually what happened in Australia in the 2000s. Telstra, privatised and the dominant player of all fixed network technologies, would not invest in the FTTN unless the government provided the funding and certain guarantees around investment returns. The general public became aware of Australia’s falling broadband performance as the new broadband era applications (such as Facebook, YouTube and Skype) grew in popularity internationally but suffered on Australia’s slow broadband networks. This low grade broadband performance became a political issue that has carried through until the most recent Federal Election in 2013.

The reluctance of the Coalition to embrace the recommendations of the Vertigan Panel appears to be inextricably linked to question of subsidies for improving broadband in the non-economic regional areas of Australia. As with the PMG and Telecom Australia before it, NBN Co is being used as the vehicle to hide the cross-subsidies necessary to provide a uniform price of broadband across Australia. The ‘broadband tax’ is hidden within NBN Co, rather than being exposed through the federal budget or industry levies. But in order for NBN Co to make a return on its investment it must be protected from competition or cherry picking in the metropolitan areas.

The Utility Model provides a convenient mechanism to maintain this political goal of hiding the ‘broadband tax’ necessary to keep the price of an upgraded broadband experience uniform across Australia. However, the compromise is that the monopoly so created will have little incentive to continue to invest in ‘deep fibre’ over the medium to long term.

## Conclusion

Australia has ranked poorly in comparison with other similar countries in terms of its broadband takeup and performance since the early 2000s. While the “long race” towards a broadband enabled digital economy may be still under way, Australia is in a difficult position at the back of the OECD pack.

The NBN policy debate of the last seven years is testament to the awareness of the Australian public to this state of affairs. The Labor 'deep fibre' NBN policy did seek to address this by building a network that would return Australia's telecommunications infrastructure to a natural monopoly structure. However, the recent Coalition NBN model based on the use of existing networks puts in jeopardy the path to investment in the necessary fibre infrastructure over the medium to long term. Any temporary uplift in broadband performance will most likely give only temporary relief to the Australian voting public – better, more data intensive applications in the fields of entertainment, education, health and business generally will eventually demand a raising of the bar on broadband speeds. And then the debate will start again on how to pay for the fibre investment needed to achieve these higher speeds.

The retention of the utility model and protection of the natural monopoly appear to be motivated by political concerns regarding the exposure of the high ongoing cost to subsidise uniform pricing of broadband services in regional areas. Any introduction of private sector infrastructure competition would appear to be blocked by the inability to devise a subsidy scheme that can be justified to the Australian electorate. But the only alternative to private sector investment is public funding through either government owned companies such as NBN Co or direct government subsidies to private sector monopolies.

The consequences are significant. Australia's position in the global digital economy is at stake. Without high quality, high performance broadband no economy can expect to hold its own, let alone strive for success in the new digital world.

Australians can expect to see broadband remain a key part of the political discourse for many years to come.

## References

- Akamai. 2014. *State of the Internet Q2 2014 Report*. Available at: [http://www.akamai.com/dl/whitepapers/akamai-soti-q214.pdf?campaign\\_id=F-MC-22494&curl=/dl/whitepapers/akamai-soti-q214.pdf&solcheck=1&WT.mc\\_id=soti\\_Q214&](http://www.akamai.com/dl/whitepapers/akamai-soti-q214.pdf?campaign_id=F-MC-22494&curl=/dl/whitepapers/akamai-soti-q214.pdf&solcheck=1&WT.mc_id=soti_Q214&), retrieved November 14, 2014.
- Australian Broadcasting Corporation. 2002. *Inside Business 25<sup>th</sup> August 2002 edition*. Transcript at <http://www.abc.net.au/insidebusiness/content/2002/s658096.htm> retrieved 14th November 2014.
- Australian Broadcasting Corporation. 2014. *Net Neutrality: Barack Obama says broadband internet should be treated like public utility*, November 11, 2014, Available at: <http://www.abc.net.au/news/2014-11-11/barack-obama-says-broadband-internet-should-be-treated-like-a-u/5881058> retrieved November 17, 2014.
- Australian Government, 2014. *Carrier Licence Conditions (Networks supplying Superfast Carriage Services to Residential Customers) Declaration 2014 (Draft)*. Available at: [http://www.communications.gov.au/\\_\\_data/assets/pdf\\_file/0016/243520/Draft-Carrier-Licence-Condition.pdf](http://www.communications.gov.au/__data/assets/pdf_file/0016/243520/Draft-Carrier-Licence-Condition.pdf) retrieved November 17, 2014.

- Crawford, S. 2013. *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age*, Yale University Press, New Haven.
- Department of Communications, Australian Government. 2014. *Broadband Availability and Quality Report*, 3-8.
- Doyle, J. 2014. *The long, covert history of rural telecoms policy*, Inside Story, Available at: <http://insidestory.org.au/the-long-covert-history-of-rural-telecoms-policy/> retrieved November 17, 2014.
- Moyal, A. 1984. *Clear Across Australia*, Nelson, Melbourne.
- Organisation for Economic Development. Dec 2013. Available at: <http://www.oecd.org/sti/broadband/oecdbroadbandportal.htm> retrieved October 20, 2014.
- Salinger, J. 2014. *Remote PHY: Why and How*, National Cable and Telecommunications Technical Papers, Available at: <http://www.nctatechnicalpapers.com/Paper/2014/2014-remote-phy-why-and-how>, retrieved November 17, 2014.
- Vertigan, M. 2014. *Independent Cost-Benefit Analysis of Broadband and Review of Regulation*. Available at: [http://www.communications.gov.au/\\_\\_\\_data/assets/pdf\\_file/0009/243387/NBN-Market-and-Regulatory-Report.pdf](http://www.communications.gov.au/___data/assets/pdf_file/0009/243387/NBN-Market-and-Regulatory-Report.pdf) retrieved November 17, 2014.

## Endnotes

---

<sup>1</sup> According to the Broadband Availability and Quality report, Australia has 10.9 million premises [p8] of which 91% or 9.9 million have access to ADSL technology [p3]. 3.7 million or 37% of ADSL served premises have estimated median peak download speeds of less than 9Mbps and 920,000 or 9.2% of ADSL served premises have estimated median peak download speeds of less than 4.8Mbps.

<sup>2</sup> In recent times the electricity distribution utility model is coming under threat from the viability of co-generation or self-generation of electricity on both commercial and residential premises. New, cheaper technologies for generation and storage of electricity on site, using renewable energies in particular, may in the medium to long term provide viable competition to an industry long thought to exhibit natural monopoly characteristics.

# Telecommunications and disaster management: Participatory approaches and climate change adaptation

---

**Marta Poblet**

RMIT University

**Hartmut Fünfgeld**

RMIT University

**Ian McShane**

RMIT University

---

**Summary:** This paper offers an overview of participatory approaches to disaster management and climate change adaptation as an introductory framework for the following five papers on the special theme of telecommunications and disaster management. While climate change is considered a societal challenge of global proportions, its impacts on human population and ecosystems take place at the local and regional levels. The geographic coordinates of disasters and emergencies, therefore, call for different location-based strategies that are embedded in their social and ecological context. Affordable, bottom-up, networked telecommunications meeting these conditions can be part of these strategies. The following papers in this issue offer a number of concepts, cases, and potential solutions.

## Introduction

By the end of 2014, the number of active mobile phones will have reached 6.9 billion, approaching the number of people living on our planet (ITU 2014). By 2018, there could be 1.4 mobile phones per capita, in addition to a rapidly growing number of tablets, navigation systems and other mobile telecommunications devices (CISCO 2013). In the Australian context, recent research has highlighted that, following a global trend, communication services delivered over the top of the telecommunications network (OTT)—VoIP and mobile messaging applications such as Whatsapp, Snapchat, Viber, Line, and Facebook Messenger,—are increasingly used as alternative sources to carriage services (ACMA 2014). This trend enables consumers to “build their own communication links” by choosing “a different option if one service is not working, effectively building additional redundancy and robustness through self-management of their communications network and service access” (ACMA 2014: 1).

While being “online and mobile” at the same time has become a commonplace experience in developing and developed countries alike, much of the marketing of mobile devices is focused on their entertainment and social networking capabilities. The increasingly ubiquitous nature of mobile connectivity, however, has the potential to change the way we interact with, and participate in, a range of political and institutional processes. This includes how we communicate with each other, with authorities and with non-governmental organisations during times of disaster and extreme events. This special theme of the *Journal* seeks to explore the role and potential of affordable telecommunications in providing more inclusive, bottom-up mechanisms for planning for, and responding to, natural disasters and extreme climatic events. The contributing authors explore this theme through a range of different technological and social lenses that highlight the rapidly changing nature of disaster-related communication and information provision, induced by technological innovation.

## Global environmental change, local communication strategies

Climate change is a societal challenge of global proportions, and for over two decades, governments have discussed the importance of a global agreement to reduce greenhouse gas emissions and address the negative consequences of climate change arising from existing greenhouse gas emissions into the atmosphere ([IPCC 2014](#)). Despite the need for global solutions to fight the causes of climate change, it is important to acknowledge that, by and large, the impacts of climate change on humans, crops, or livestock take place at local and regional scales – they are experienced by people in their respective natural and social environments. The majority of disaster events – whether they are climatic, geophysical or technological in nature – are confined to local or regional geographic areas or landscapes, and consequently, emergency management and climate change adaptation planning efforts are focused on local-level action. Bushfires in south-east Australia, for example, are localised events that, in extreme cases, can expand to cover entire forested regions, such as during the 2009 Black Saturday fires in Victoria, in which 173 people died and 414 were injured ([Climate Commission 2011](#)). Heatwaves can persist across significant parts of the continent, yet they usually cause their greatest impact in urban areas where concentrated assemblages of people, the built environment, and an urbanised ‘natural’ environment result in the urban heat island effect, with sometimes severe consequences to human lives ([Kovats & Ebi 2006](#)).

These localised characteristics of disasters call for rapid, effective responses that are specific to location and embedded in social and ecological context. Local communities are typically the first responders, supported by locally or regionally based emergency management and community support organisations, many of which rely on volunteers and are poorly resourced.

Developing localised networks and mechanisms for early warning, response and recovery from disasters is a critical aspect of increasing social resilience and the capacity of communities to adapt to climate change and other dimensions of global environmental change (Davoudi *et al.* 2012; Sherrieb *et al.* 2010).

During and after disasters, communication technologies and networks become vital components of the response effort that can decide over life and death. However, all too often, communication infrastructure is itself affected by the disaster. Systems less prone to failure are required that are effective, easy to operate and use, and readily accessible. In the medium and longer term, developing more affordable, accessible, participatory and distributed telecommunications systems can become an integral part of resilience building and systemic adaptation to climate change. The characteristics of localisation, infrastructure-lite, flexibility and peer-to-peer topology featuring DIY telecommunications perfectly apply to this context. Effective disaster management and climate adaptation design should include these principles, to support participatory planning and responsive approaches that can make a difference to human lives during crises, as well as assisting in developing an adaptive capability in the face of climate change.

## The makers movement and DIY telecommunications

Internationally, telecommunications provision has been predominantly organised through public monopolies or regulated markets, although the formation of telecommunication cooperatives – particularly in rural areas – points to bottom-up organisation in some cases (Fischer 1992).

With the exception of amateur radio, early telecommunications technologies – regardless of the provisioning model – channelled information flows up and down hierarchies, rather than directly across networks. The co-development of interactive digital technologies, peer-to-peer networking and DIY tinkering has reoriented communication flows and fostered participatory cultures.

For some years now, the “makers movement” has gained world-wide popularity as an emerging techno-culture. The maker movement has been defined in different ways, such as a “growing culture of hands-on making, creating, designing, and innovating” (Peppler & Bender 2013), or a culture that includes practices “from crafting to high-tech electronics” (Anderson 2012: 20; Manzini 2013: 2). Others have emphasised the participatory component of the movement by referring to it as a “democratised technological practice” (Tannenbaum *et al.* 2013: 2604).

Yet, the makers movement is not a new phenomenon, for it is connected to Do-It-Yourself (DIY) cultures of the previous decades (Hertz 2011; Doherty 2012; Powell 2012). Fox has

recently referred to a “Third Wave DIY” that “draws upon the read/write functionality of the Internet, and digitally-driven design/manufacture, to enable ordinary people to invent, design, make, and/or sell goods” (Fox 2014:19). The Web 2.0 ecosystem of social media, platforms, tools, etc. is currently enabling new forms of networked, real-time collective intelligence to solve issues when it comes to building any type of mechanical artefact, electronic device, software or hardware. To Dougherty, founder of the *Make* magazine in 2005, the Internet enables “today’s makers [to] enjoy a level of interconnectedness that has helped to build a movement out of what in the past would have been simply a series of microcommunities defined by a particular hobby or activity” (Dougherty 2012:2).

Another distinctive sign of the movement is “the combination of new economic funding models, physical spaces, new platforms, tools and publications” (Lindter *et al.* 2014: 440). More specifically, makers have leveraged crowdfunding platforms and social media to enlarge the community base of donors and developers, who may even overlap in some cases. Maker fairs, ‘fab labs’ and hacker spaces have blossomed in the USA and Europe, and are growing fast in Africa (Fox 2014: 20). In this new ecosystem, the boundaries between producers and users, hobbyists and professionals, are constantly redrawn. The paper by Antunes in this issue, discussing the design of affordable sensor networks where “the target user is not assumed to be skilled in communications” is a clear example of this intention to open up practices (i.e. environmental data collection) which were previously restricted to public agencies and/or professional researchers (Antunes 2014: 9).

Telecommunications has not remained unaffected by the DIY and makers’ movements (Poblet 2013). At present, the early ham radio communities coexist with wireless community networks across the globe. In festivals, campuses, or remote areas with either poor or unaffordable GSM coverage, DIY and open-source cell networks are introduced as either a proof of concept, a temporary solution, or as alternative telecommunications services (Ruiz 2013; Gallagher 2014; Patterson 2014). The exploration of these grassroots capacities extends to the production of DIY cell phones and routers (Mellis & Buechley 2014).

In parallel to these developments, the use of Unmanned Aerial Vehicles (UAVs), more popularly known as drones, has burst across the globe with the most varied applications. While Unmanned Aerial Systems (comprising UAVs, their control ground stations and communications systems) “constitute the most dynamic section of the aerospace industry” (Odido & Madara 2013: 108), communities of DIY UAVs are flourishing on the Web (the popular DIYDrones.com, started in 2007, has more than 60,000 members sharing experiences, instructions, and open source software). Equipped with cameras and other advanced sensors, civilian and personal drones enable observation, monitoring, mapping, and/or real-time broadcasting of environmental conditions, humanitarian crises, emergencies

and other events. Likewise, DIY satellites, which have been used by amateur radio satellite communities for decades, are now becoming accessible to large communities. Open hardware, open standards, and inexpensive sensors are enabling projects that aim at a “democratisation” of the space for earth observation ([Marshall 2014](#)). PlanetLab, a start-up that has recently put into space a constellation of 28 earth-imaging satellites (10x10x30 cm.), or SatNogs, providing open source ground stations, are new entrepreneurial initiatives in this line. Yet, the democratisation of outer space will need to address multi-level regulations and, in some countries, contested “government export controls on satellite hardware and software” ([Reyes 2014](#)).

Despite the variety in scope, objectives and resources, these new generation DIY telecommunications initiatives and projects tend to share some distinctive features. In a nutshell, DIY telecommunications usually are:

- Local: DIY telecommunications emerge to satisfy a necessity inefficiently covered at the local level (poor infrastructure, lack of coverage, unaffordable costs, etc.)
- Ad-hoc: DIY telecommunications serve, at least initially, a particular purpose (e.g. access to a cell network, access to the Internet, provide an alternative to existing services, etc.)
- Infrastructure-lite: DIY telecommunications tend to keep infrastructure costs to a minimum so that the user base can expand.
- Flexible: DIY initiatives and projects are in perpetual beta trials and tend to evolve and adapt to different configurations depending on the contextual needs of the users.
- Peer-to-peer: DIY telecommunications have a preference for different decentralised topologies based on nodes and links rather than hierarchical structures.

Some of these features – notably minimal infrastructure, flexibility, and decentralisation – are typical of mesh networks as designed in the domain of information systems. In a similar vein, they also echo the SLOC model (small, local, open, connected) developed by Manzini as “a design guideline for creating resilient systems and sustainable qualities” ([Manzini 2013](#)). In our review of affordable telecommunications for disaster management and climate change adaptation, local strategies leveraging local capacities and shared, distributed knowledge across the Internet have a place in addressing these global challenges. The papers in this issue are also walking along this path.

## Participatory approaches and institutional settings

While DIY telecommunications activists have frequently positioned themselves in opposition to markets and the State, the complex and evolving relationship between the sectors influences the capacity for bottom-up mechanisms to organise around disaster management.

Limitations have been placed on community activism through the State regulation of spectrum and telecommunications services, and aggressive litigation by commercial telcos seeking to protect their investment and market share. Community provision, sometimes supported by local governments, has in the past been viewed as a threat to competitive markets, seen as the preferred model for global mobile telecommunications. Other objections to community activism turn on claims of exclusiveness and unreliability.

The merits of these claims have been significantly challenged by civic and activist responses to disasters, including Hurricane Katrina (New Orleans 2006) and Hurricane Sandy (New York 2011). In both instances, public or community-run Wi-Fi networks proved the most robust form of telecommunications, providing vital information links for residents, first responders and city workers alike. In New Orleans' case, while commercial mobile services were knocked out, telcos and rival ISPs were sufficiently influential to have the free city Wi-Fi network throttled to a miserly 512Kbps in the immediate post-hurricane period. When the emergency period ended, network speed was further reduced to 128Kbps, to comply with Louisiana's broadband laws ([Bangeman 2006](#)). In New York, a Wi-Fi network launched by a not-for-profit in 2011 at New York City Housing Authority's largest public housing development, Brooklyn's Red Hook Houses, stayed on-line during Sandy and its aftermath, providing a lifeline for residents stranded in the complex without power or water ([Kazansky 2012](#)).

The aggressive stance of higher governments and telcos towards community and municipal activism, observed most in North America and Europe, has begun to soften, though. Smartphone penetration has driven demand for data beyond the capacity of some 3G and 4G networks, leading to commercial subsidy of public wireless networks to offload data traffic. An increasing array of cross-sector partnerships utilises the communication, data and geo-locative capabilities of mobiles in predictive, emergency and recovery situations. Major humanitarian agencies, such as the American Red Cross, have built capacities to gather and disseminate information through social media into core operating structures. However, this institutionalisation of digital humanitarianism has in turn led to new concerns over data privacy and security, and the targeting of communications infrastructure by State and non-State actors in parts of Africa, Asia and the Middle East.

These developments are framed by a rights-based stance on information access, articulated with renewed vigour by humanitarian and disaster relief agencies. As the UN Office for the Coordination of Humanitarian Affairs (2013:13) reminds us, the freedom to seek, receive and impart information in any media features in Article 19 of the 1949 UN Declaration of Human Rights. While acknowledging this universalism, the articles in this special edition show, also challenge us to understand mobile communications within their particular communication ecologies, and political and cultural settings.

## The papers on this special theme

The articles on this special theme aim at exploring the role of affordable telecommunications in designing participatory approaches to disaster management and climate change adaptation. The projects, initiatives and technologies discussed target different issues and geographic areas, but they are all based on approaches that combine the use of inexpensive devices (e.g. mobile phones, two-way radios, or sensors) with local infrastructure capacities to produce contextualised, granular, and real-time information on climate and weather conditions, alerts, and disaster response. The “bring-your-own-device” approach adopted in most of these papers seeks to lower the learning curve for the participation of individuals and groups while diminishing the infrastructure requirements for an effective communication. In each case, nevertheless, a number of market constraints and regulatory issues are to be considered, such as compliance with spectrum licensing and usage policies at the national and international level.

The first paper by Alex Antunes (“Cheap deployable networked sensors for environmental use”) proposes the deployment of inexpensive networked sensors for environmental monitoring. He argues that different affordable technologies are already in place to enable steady state data collection at the local, private and amateur levels. Antunes presents a model for inexpensive sensors, known in some maker communities as Dirt Cheap Dumb Wireless (DCDW) to enable new segments of non-professional users to monitor environmental conditions. The main limiting factors, according to Antunes, are not technical but regulatory. Thus regulations may impose either absolute or relative restrictions to different types of communications (e.g. FCC regulations on Low Power Radio Station (LPRS) that allow transmission of data but not for sensor purposes).

The next three papers on this special theme, while relying on different approaches, consider the present ubiquity of mobile phones across the globe to be a fundamental component of participatory disaster management.

In their paper (“Acoustic coupled disaster and remote communications systems”) Müller-Baumgart *et al.* explore how to provide cost-effective communications in disaster-affected

areas where infrastructure has been severely damaged. With the aim of leveraging existing locally available hardware, the paper describes a possible solution based on acoustic coupling of mobile telephones with the two-way radios that are often carried in remote areas of Australia. The combination of these two devices has yet to address two types of challenges:

- i) technical (e.g. how to interface digital communications systems to analogue devices, how to maximise the limited bandwidth available for data transmission) and
- ii) regulatory (namely, how to make digital communications compatible with licences for citizen band radio that, in principle, do not cover digital transmission).

While further exploration needs to be done in both areas, the acoustic coupling would allow the broadcasting of weather information, local news and limited private messaging in disaster zones or remote areas where there is currently no such possibility.

The next paper, by Noske-Turner *et al.* (“Locating disaster communication in changing communicative ecologies across the Pacific”), provides a comparative overview of disaster communication systems and infrastructures, practices and challenges in the Pacific Island region, a very diverse geographical and cultural area. The authors argue that access to, and affordability of technologies, are just two of the variables to consider in disaster communication. Consequently, to achieve an effective communication strategy other qualitative aspects come into play, such as appropriate technologies, systems for the ownership and maintenance of infrastructures, or local knowledge and belief systems. The paper adopts the approach of “communicative ecologies”, which prioritises local knowledge, to identify nuances in access, use, and practices. In this perspective both offline (traditional and face-to-face) and online modes become relevant when designing appropriate disaster communication strategies. The authors conclude that the accurate assessment of the “communicative ecology” of each particular area is vital for providing a better integration of mobile phones and other ICTs into disaster plans and policies across the Pacific.

The fourth paper is “Updating warning systems for climate hazards: can navigation satellites help?” by Handmer, Choy and Kohtake. The paper discusses the current disjunction between mainstream models of warning systems, the expectations of the public for personalised warnings, and the potential of social media and mobile technologies to improve both reach and effectiveness. It then makes the case for the integration of satellite navigation by proposing the use of the next generation of Japanese positioning satellites (QZSS, or Quasi-Zenith Satellite System). Satellite warning systems would be able to simultaneously deliver millions of individual warnings to personal devices while providing a backup system when local communications infrastructure fails.

The last paper on this special theme (“Warrnambool Exchange Fire: Resilience and Emergency Management”) by Gregory *et al.* covers a very significant event in Victoria: a fire occurred on November 22, 2012 in the vicinity of Telstra’s Exchange building in Warrnambool, Victoria, which severely impacted regional telecommunication services for more than two weeks. The paper does not strictly deal with the topic of participatory approaches as its aim is to provide lessons learnt from the incident in order to enhance increased resilience. However, the paper has the great value of illustrating the disruptive effects of a single point of failure disaster on telecommunications for individuals (especially the most vulnerable), communities, business, and local providers. As the authors put it, the “no one-size-fits-all solution” principle, (or location-based approach) needs to guide increased resilience strategies in the future.

We expect that this special theme will provide new insights on how global societal challenges such as climate change, disasters, and emergencies can be addressed with a new generation of telecommunications and technologies that leverage local capacities to provide ad-hoc, infrastructure-lite, flexible, and decentralised services and, ultimately, to enhance participatory approaches to tackle these major challenges.

## Acknowledgements

We thank the authors of the papers for contributing to this special theme with their dedicated work. We are also grateful for the contributions of several people who have greatly helped us in its completion: Dr Peter Gerrand, Managing Editor of the *Journal*, for inviting us to edit this special theme and for his ongoing support; and Dr Andrew Glover, for his efficient assistance in coordinating tasks and communications. We are also thankful to all the referees who provided very valuable and timely reviews.

This special theme has also benefited from the support of the RMIT Friendship Research Grant offered by the School of Global, Urban and Social Studies (GUSS) and the Graduate School of Business and Law (GSBL). It has also partially benefited from research within the framework of two previous research projects funded by the Spanish Ministry of Economy and Competitiveness: CrowdCrisisControl (IPT-2012-0968-390000) and “Crowdsourcing: instrumentos semánticos para el desarrollo de la participación y la mediación online” (DER 2012- 39492 -CO2 -01).

## References

- Antunes, A. 2014. 'Cheap deployable networked sensors for environmental use'. *Australian Journal of Telecommunications and the Digital Economy*, Vol. 2(4)
- ACMA. 2014. 'Six emerging trends in media and communications'. Research report, available at: <http://www.acma.gov.au/theACMA/Library/researchacma/Research-reports/six-emerging-trends-in-media-and-communications>, retrieved November 24, 2014.
- Anderson, C. 2012. *Makers: The New Industrial Revolution*. London: Random House.
- Apvrille, L; Tanzi, T; Dugelay, J. L. 2014. 'Autonomous drones for assisting rescue services within the context of natural disasters'. In General Assembly and Scientific Symposium (URSI GASS), 2014 XXXIth URSI, 1-4.
- Bangeman, E. 2006. 'New Orleans to take city-wide WiFi network offline', *Ars Technica*, October 24, available at: <http://arstechnica.com/gadgets/2006/10/8052/>, retrieved November 24, 2014.
- CISCO. 2013. Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018, available at: [http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white\\_paper\\_c11-520862.html](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html), retrieved November 24, 2014.
- Climate Commission. 2011. *The critical decade: Victorian climate impacts and opportunities*, Canberra, available at: [http://climatecommission.gov.au/wp-content/uploads/120719\\_VIC-report-web-version\\_final.pdf](http://climatecommission.gov.au/wp-content/uploads/120719_VIC-report-web-version_final.pdf).
- Davoudi, S; Shaw, K; Haider, L J; Quinlan, A E; Peterson, G D; Wilkinson, C; Fünfgeld, H; McEvoy, D; Porter, L. 2012. 'Resilience: A Bridging Concept or a Dead End?; "Reframing" Resilience: Challenges for Planning Theory and Practice; Interacting Traps: Resilience Assessment of a Pasture Management System in Northern Afghanistan; Urban Resilience: What Does it Mean in Planning Practice'. *Planning Theory & Practice*, 13(2), pp.299–333, <http://dx.doi.org/10.1080/14649357.2012.677124>.
- Dougherty, D. 2012. 'The maker movement'. *Innovations*, 7(3), 11-14.
- Fischer, C. 1992. *America Calling: A Social History of the Telephone*, Berkeley & London: University of California Press.
- Fox, S. 2014. 'Third Wave Do-It-Yourself (DIY): Potential for prosumption, innovation, and entrepreneurship by local populations in regions without industrial manufacturing infrastructure'. *Technology in Society*, 39, 18-30.

- Gallagher, S. 2014. 'Cellular's open source future is latched to tallest tree in the village. *Ars Technica*', available at: <http://arstechnica.com/information-technology/2014/02/cellulars-open-source-future-is-latched-to-tallest-tree-in-the-village/>, retrieved November 24, 2014.
- IPCC. 2014. *Climate change 2014: Synthesis report - Approved summary for policymakers, Geneva*, available at: <http://www.ipcc.ch/report/ar5/syr/>, retrieved November 24, 2014.
- Hertz, G. 2011. 'Arduino Microcontrollers and the Queen's Hamlet: Utilitarian and Hedonized DIY Practices in Contemporary Electronic Culture' (ACADIA 2011).
- ITU. 2014. *Facts and Figures*, available at: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf>, retrieved November 24, 2014.
- Kazansky, B. 2012. 'In Red Hook, mesh network connects Sandy survivors still without power', 12 November, available at: <http://techpresident.com/news/23127/red-hook-mesh-network-connects-sandy-survivors-still-without-power>, retrieved November 24, 2014.
- Kovats, R.S; Ebi, K.L. 2006. 'Heatwaves and public health in Europe', *European Journal Of Public Health*, 16(6), 592–599, available at: <http://www.ncbi.nlm.nih.gov/pubmed/16644927>, retrieved November 24, 2014.
- Lindtner, S; Hertz, G. D; Dourish, P. 2014. 'Emerging sites of HCI innovation: hackerspaces, hardware startups & incubators'. In Proceedings of the 32nd annual ACM conference on Human Factors in Computing Systems, 439-448.
- Manzini, E. 2013. "Resilient systems and sustainable qualities". *Current: Design Research Journal*, 4, 11-14.
- Marshall, W. 2014. 'Tiny satellites show us the Earth as it changes in near-real-time', available at: [http://www.ted.com/talks/will\\_marshall\\_teeny\\_tiny\\_satellites\\_that\\_photograph\\_the\\_entire\\_planet\\_every\\_day](http://www.ted.com/talks/will_marshall_teeny_tiny_satellites_that_photograph_the_entire_planet_every_day), retrieved November 24, 2014.
- Mellis, D. A; Buechley, L. 2014. 'Do-it-yourself cellphones: an investigation into the possibilities and limits of high-tech diy'. In Proceedings of the 32nd annual ACM conference on Human factors in computing systems, 1723-1732.
- Odido, M. D; Madara, D. 2013. 'Emerging Technologies: Use of Unmanned Aerial Systems in the Realisation of Vision 2030 Goals in the Counties'. *International Journal of Applied Science and Technology*, Vol. 3(8): 107-127, available at: [http://ijastnet.com/journals/Vol\\_3\\_No\\_8\\_December\\_2013/15.pdf](http://ijastnet.com/journals/Vol_3_No_8_December_2013/15.pdf), retrieved November 24, 2014.

- Patterson, S.M. 2014. 'Open source project builds mobile networks without big carriers', available at: <http://www.networkworld.com/article/2226543/wireless/open-source-project-builds-mobile-networks-without-big-carriers.html>, retrieved November 24, 2014.
- Peppler, K; Bender, S. 2013. 'Maker movement spreads innovation one project at a time' *Phi Delta Kappan*, 95(3), 22-27, available at: <http://pdk.sagepub.com/content/95/3/22.full.pdf+html>, retrieved November 24, 2014.
- Poblet, M. 2013. Affordable telecommunications: A new digital economy is calling. *Australian Journal of Telecommunications and the Digital Economy*, Vol.1(1), 12, available at: <http://doi.org/10.7790/ajtde.v1n1.12>
- Powell, A. 2012. Democratizing production through open source knowledge: from open software to open hardware. *Media, Culture, and Society*, 34 (6): 691-708. <http://dx.doi.org/10.1177/0163443712449497>
- Reyes, M.F. 2014. DIY Satellites: Now and near future. *Makezine*, available at: <http://makezine.com/2014/04/07/diy-satellites-now-and-near-future/>, retrieved November 24, 2014.
- Ruiz, V. 2013. 'Forgotten by telecoms, Mexico town runs cell service'. *Phys.org* [Internet]. Accessed 25 September 2013. available at: <http://phys.org/news/2013-08-forgotten-telecoms-mexico-town-cell.html>, retrieved November 24, 2014.
- Sherrieb, K; Norris, F.H; Galea, S., 2010. "Measuring Capacities for Community Resilience". *Social Indicators Research*, 99(2), 227–247 LA – English. available at: <http://dx.doi.org/10.1007/s11205-010-9576-9>.
- Tanenbaum, J. G; Williams, A. M; Desjardins, A; Tanenbaum, K. 2013. 'Democratizing technology: pleasure, utility and expressiveness in DIY and maker practice'. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2603-2612.
- UN Office for the Coordination of Humanitarian Affairs. 2013. 'Humanitarianism in the Network Age', available at: <https://docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf> , retrieved November 24, 2014.

## Cheap Deployable Networked Sensors for Environmental Use

Alex Antunes

Capitol Technology University

**Summary:** We profile the utility and limits in deployment of inexpensive disposable sensor networks by amateurs to achieve environmental monitoring goals. Four current technology movements – PC-on-a-chip processors such as Arduino, prebuilt sensors, 3-D printing, and Wi-Fi and mesh networking – enable rapid sensor platform creation and make it easy for non-specialists to create general sensor-bearing platforms. Deployment of a cluster of multiple sensor-bearing platforms is, however, communications-limited in terms of both range and number of devices supported, and generally requires a base station with internet access. We examine how inexpensive technology supports scenarios for short-term environmental modelling by average citizens.

### Introduction

When an environmental crisis or disaster occurs, there is a need to deploy a large number of sensors quickly over a large area to provide data for a short period of time to a local controller. Scenarios include mapping the spread of a wildfire, tracking the rise of a flood, and one-time data measurement of a potential contamination source. While most crises currently rely on state-supported agencies (first responders and authorised scientific agencies) to provide data to the public, we assert that the technology is already in place to enable appropriate crisis, ad hoc, and steady state data collection at the local, private, and amateur level. The primary limitation is not hardware or skill, but effective implementation of communications to minimise the cost-per-sensor and ensure effective data collection from a dispersed set of sensors.

Key for these sensors is the engineering limits requiring low cost, minimal technical skills, and ability to rapidly deploy with or without permission from state agencies. Internet access combined with smart devices can enable use of telecomm networks to create ad hoc sensor data collection networks over the channels currently used for voice, email and web browsing. By using conventional internet, this allows creation of smart sensor networks at either an official or activist level.

Smart devices and 'the internet of things' suggest ordinary appliances be made net-accessible, 3-D printing enables rapid construction of simple prototypes, and Arduino- and Pi-based kits let teams build inexpensive sensor rigs. The combination of these technologies enables creation of customised inexpensive one-use sensors that can be deployed or scattered over a target area. Like buoys on the ocean, data can be sampled in-situ at many places to provide a

detailed geographic picture of wildfire advances, pollution or toxin levels over a disputed site, rainfall in flood country, and other simple measurables.

The downside is the 'landmine' problem; tracking and disposing of your sensors to avoid adding to environmental woes. We discuss how proliferation of easy-to-deploy 'land buoys' can advance scientific and activist goals by combining inexpensive off-the-shelf technology with internet access to advance environmental causes and disaster assessment. However, citizen monitoring must also be aware of social concerns in the pursuit of data.

This paper lists situation drivers for short-term environmental data collection, followed by the operational limits. Several existing sensor deployments are presented, followed by possible future scenarios. The paper lists a prototype generic build, then discusses communications issues and communications topologies. After survivability and recover concerns are discussed, the paper concludes with a review of the frequency limitations and potential abuse likely in pursuit of these data gathering goals.

## Situation drivers

The conventional image of a scientific sensor package, remote sensing robot, or surveillance drone assumes two-way communication that allows the device to be modified during use by a skilled remote operator. Such 'smart' sensors can be manipulated and reconfigured in real time to optimise the data return. Deployable pre-configured non-adjustable 'dumb' sensors – lacking two-way communication and with no movement or positioning capability – are not yet a commercial segment and require custom building. Such sensors do not require advanced degrees or large funding to create. By analogy, a weather satellite can obtain temperature data for a hemisphere of the entire Earth from space over broad areas of the sea, but we require inexpensive temperature sensors on cheap buoys to provide more detailed mile-by-mile measurements of ocean temperature variance. For situations requiring sampling of a small spatial area with many data points, deployment of multiple ground-based sensors is required.

A low time sampling rate and simple low-resolution detector images are acceptable in favour of being able to sample a local geographic region with high spatial sampling, especially for transient events or items not available by satellite due to being in economically minor areas. On-site small-scale data collection is a sub-range in terms of area (small) and resolution (high) combined with high time resolution (24 hours, 7 days at week at minutes or hours sampling).

This produces a level of detail that satellites can't see from Geosynchronous orbit (GEO) using Earth-observing missions, which have spatial resolution no smaller than 1km in area. Monitoring often requires data taken more frequently than with satellites such as the Afternoon Constellation of international earth-observing satellites (dubbed the 'A-train') that pass overhead over 90 minutes.

For in-situ sensors, conventional military, commercial and scientific work tends towards robust multi-capability sensor platforms with extensive software support, dedicated

communications, and a correspondingly high price. However, disposable inexpensive sensors exist and are proliferating. The primary bottleneck is access to communications from the environmental site to the data collection centre. We look at cases that need sensors, evaluate cost and design issues for sensor design and deployment, calculate coverage areas, and discuss deployment and communications issues that, if resolved, leads to good science.

Communications becomes the limiting factor. [Middleton \(2014\)](#) discusses the geographic limits in availability of mobile broadband and wireless access in Australia, noting "there are no comprehensive statistics that track WiFi users" and that "service is available on a patchwork basis, with many different providers offering WiFi coverage in specific geographic locations, sometimes for free, sometimes not". Middleton suggests future user access can be geographically broadened, in part, by allowing access over both licensed (commercial) and licence-exempt (non-commercial) spectrum.

This follows the model of the 'Internet of Things' (IoT), a scenario where ordinary devices such as toasters are Internet-enabled to allow data collection and remote operations. The limitation is no longer cheap hardware availability or short-range data transmission, but the need to network a hub or base controller to get the collected sensor net data from the work site via the larger internet to the lab.

## Potential scenarios

Potential implementation of citizen- and amateur-deployed sensors requires an assessment of cost per sensor, expected coverage area desired, and communications and network support required to deliver the data to the user. To maintain the low cost per sensor, we continue with the model of using non-mobile wireless sensors that transmit repeated data points for the desired measurable, require no real time commanding, and only gather data for a brief time (hours to days).

Tasks can include monitoring of natural disaster events such as fires, volcanos, ice, and flood. Industrial monitoring includes tracking industrial and chemical activity, noise levels, or radiation levels. Farm and environmental assessment of small regions are a third category. Purely scientific studies of dry and wet regions are also a category favouring small inexpensive deployable sensors. Urban situations also can be monitored. In all cases, the data is transmitted away from the target site to a remote user, necessitating a long-distance communication pathway via internet, amateur radio, or GSM.

Sample crises include fire rehabilitation, fuel maps to predict fire spread, volcano eruption assessment, flood assessment, and ice breakup change detection. Chemical pollution tracking includes on land or in bodies of water, either to detect whether contamination exists or to monitor changes in concentrations. Agricultural uses include monitoring rain and water levels, and is particularly documented in the previous examples, as this is a commercially viable area. Marine biology uses in littoral zones, watersheds, and wetlands, as well as arid environments including desert, mountain and ice climates. In addition to the previous examples

of urban heating, sensors can be deployed to track noise levels, building vibration due to traffic, light levels for trees in city environments, CO<sub>2</sub> or pollutant mapping, and even utilisation rates of roads or parks as determined by noise levels.

The operational limits for these scenarios require that

- (a) the sensor data is gathered from a distance of at least 1km from the sensor deployment and
- (b) that multiple sensors are able to return a position via GPS data, a timestamp, and the sensor value gathered.

Communication via internet requires network access, as does GSM use. Communications via radio use must follow national codes, such as the Federal Communications Commission (FCC) in the US and the Australian Communications and Media Authority (ACMA) in Australia.

Licence compliance is one of the communications bottlenecks. Because spectrum is regulated, citizens are not allowed to arbitrarily boost the signal from low-power off-the-shelf devices, install repeaters across public land, or access the radio spectrum except in narrowly permitted bands such as the channels allocated to amateur ham radio, that have their own licensing requirements for use.

Off-the-shelf radio transmitters include the XBee and other short-range devices, conventional Wi-Fi devices intended to be received by a Wi-Fi hub, and licensed radio transmitters at multiple frequencies. Our communications model is simplified in that we require sensor nodes to transmit only, and do not require real time commands be transmitted to the sensors. Thus we require only sensor transmitters with no receivers, and likewise any base hub need only receive, not transmit. Devices with inherent mesh capability, where each device may reroute signals from adjacent nodes as well as its own data, do require transceiver capability but are allowable in our scenarios if their price point and ease of development comply with our requirements.

## Existing hardware

The use of drones and robots for measurement is one potential solution, which is worth noting in the context of these scenarios. The marketing of items for the 'maker' and Do-It-Yourself (DIY) hobbyists and students is leading to lower price points and higher capabilities for robots, radio-control vehicles, drones, and even satellites. The current state of amateur, home-built and DIY robots, quadcopters, and camera-bearing drones is providing inexpensive commercial off-the-shelf (COTS) systems to the average consumer. The price point for an individual radio-control (r/c) drone capable of taking video images at short range for later return to the sender is under \$50, but requires a human operator. Live data delivered by a user-controlled single drone is priced in the sub-\$1000 range.

The bulk of commercially available drones for amateurs are radio-control devices cross-marketed as toys and providing short-range flight control plus some video capability. These function using standard r/c interfaces using either infrared (IR) line-of-sight control (on the sub-\$100 end), or standard FCC-licensed short range toy r/c control at 27MHz or 47MHz. Sub-\$500 r/c vehicles carry no sensors or an onboard video camera that stores data to an SD card for later recovery. For autonomous simultaneous spatial sensing in our scenarios, drones are a high-risk high-cost solution that is unlikely to support substantial environmental modelling. In contrast, networked non-mobile sensors are able to cover a large spatial area over a longer time base than drones.

A combination of 3-D printing, home-built and off-the-shelf hardware, and easy sensor integration with cheap PC-on-a-chip solutions such as Arduino and Pi enables anyone with an internet connection to quickly integrate and test a unique one-off sensor. Once they have designed a sensor, they can quickly create multiple identical ones to create a deployable swarm. Our experience has shown a single college student can, in 3 months, design and improve a specific sensor design to survive a 3-gravity impact landing and provide data on a specific single variable – temperature, or seismic, or chemical information – for six hours. The hardware is cheap and easy to design and improve. The primary bottleneck is communications for a large number of deployed sensors.

Rain and water run-off measurements for irrigation have historically been measured by subjective crew assessment ([Miller 2014](#)). The RemoteTracker \$500 hand-held sensor uses acoustic Doppler, GPS, and Bluetooth transmits standardised flow measurements via wireless wide area network (WWAN) card to a central server ([H2OTech 2014](#)). Fifteen garage-built stations built by Weather Tools LLC, deployed by an entrepreneur in California, USA ([Miller 2014](#)) are spaced 7.5 mile apart, "which allows the detection of previously unseen gradients in temperature, wind, and moisture". The company hopes to "create a service that helps growers optimise crop production and resource management".

The WallyHome, another humidity, water, and temperature sensor system, uses a tiny battery and zero connectivity infrastructure to send data to an internet-connected hub. Their sensor battery lasts 10 years, and their broadcast protocol is wireless with a typical short range under 10 metres, but extends the range by resonating the existing copper power lines in the building as an antenna. The room or building data collection hub is plugged into the power lines for both power and to receive the signal, and then serves to relay that data via internet to their data collection cloud server ([Greene 2014](#)).

Within cities, hourly tracking of apartment temperatures can be used to improve municipal heating. "Heat Seek's system [in New York City] is designed to record apartment temperatures every hour and then present the data for lawyers, advocates, and inspectors." ([Lipsky 2014](#)) Their communications network is also a mesh plus hub, where each apartment has a sensor node sending data locally over a Wi-Fi network to that building's data hub, which then sends data via internet to the company central server. The sensor nodes are off-the-shelf Xbee

modules plus temperature sensor with a price point under \$30. The central hub is a Raspberry Pi with an Xbee receiver. Including labour, they estimate \$1000 per apartment to set up monitoring (based on a Kickstarter campaign of \$10,000 to write 1,000 apartments).

A web-controlled central heating and energy monitoring system using entirely open source designs can be built for under \$US 100. Such systems send multiple sensor such as "thermistors for temperature sensing, current sensors or opto-reflective sensors for detecting motion or occupancy or even reading the dial on the gas meter. Additionally there are 4 channels of high current drivers which can be used to control relays, solenoids, dc motors etc" ([Boak 2012](#)). The power profile for remote sensors and Wi-Fi transmission to a hub is dropping to levels such that an unattended sensor can potentially last years. Ultra-low powered radios acting as internet nodes use millimetre waves to both transmit to the hub and receive power, albeit with a range of only 1-3 metres ([Marshall 2014](#)).

Additional scenarios follow this same development pathway. We do not distinguish between state agents acting in their role of disaster or environmental management, and individual organisations acting to diagnose or discover problems at a local level. The hardware is ubiquitous and available to private citizens, and requires minimal specialised knowledge. In addition, data aggregation to produce value from individual measurements is coordinated on sites such as SciStarter and Pachube, allowing individuals to contribute their local, geographically-tagged data to support larger regional or global surveys ([Gertz 2012](#)).

## Prototypical build

The two models for inexpensive sensors are called, in the Arduino community, Dirt Cheap Dumb Wireless (DCDW) and Dirt Cheap Smart Wireless (DCSW). A DCDW transmits sensor data periodically and receives no communication back from the 'base station'. DCSW is an evolving field where the sensor may optionally be triggered from a base station, only reporting when queried. DCDW has lower power consumption and is the focus of our scenarios.

Commercial off-the-shelf (COTS) products fulfil the hardware design for our 'sensor pod'. Our reference model uses the [MakerShed \(2014\)](#) 'Wireless Sensor Node' (US \$13.99) to provide four analogue or digital sensors broadcast via an internal 433MHz radio transmitter with a range of 150 yards per sensor. This hardware delivers four data pod items of 8-bit sensor data at a choice of every 10 seconds, every 10 minutes, every hour, or only when a measurable event happens. It takes 20 minutes (estimated) to set up and configure with a pre-built sensor.

The detection limits for typical (US \$7) sensors include ([futurelec.com](#)) include CO2 readings of 0-10,000 ppm of CO2 per minute, LPG readings of 200-10,000 ppm iso-butane propane, or CO sensor readings of 20-2,000ppm. Their natural gas sensor, ozone sensor, air quality sensor, methane sensor, and hydrogen sensor have performance in similar ranges.

Power needs are appropriately minimal. This sensor pod runs off a 9V battery and has typical lifetimes of 15 days or longer in operations, and sleeps in between scheduled data gathers. It

has a maximum lifetime of 76 days if read out once/hour, down to five days if read every 10 seconds ([Arduino.cc 2014](#)). Additional devices are available. Sensor data can be at resolutions from 8-bit to 14-bit, though larger sensor data packet sizes consume more power. Timing specifications, amount of user support, and survival temperature ranges for a specific system are items a designer would consider in a trade study, depending on their project's needs. Typical costs for a complete 'sensor pod' – 2 sensors, wireless transmitter, battery, case, and all supporting hardware – is US \$30 and upwards per sensor.

A sensor network requires a base station to act as a central collection 'hub' able to reroute the data via internet to a remote user. For our reference sensor pod, we configure a base station with a matching wireless receiver and Arduino microprocessor controller, which can support up to 64 of our sensor pods. Typical costs for our 'hub' are under US \$100. Power requirements remain minimal, operating from a 9V battery for 2 days ([Hanscr 2013](#)). While our reference design uses an Arduino, other COTS sources offer 32 small form factor single chip controllers ([Allan 2014](#)).

A full set of 64 2-sensor pods with batteries, plus mobile base station, will cost a team approximately \$2.1K. This provides two weeks of data taken every two minutes. The range is 150 feet, so if distributed evenly in a half-circle disk region, can cover 35,000 square feet with spacing of 500 square feet between sensors, with each sensor approximately 22 feet from each other. Coverage of a wider area requires evaluating different protocols that allow for extending the range of the sensor communications network.

## Sensor networking

Within the sensor network, using off-the-shelf transmitters sharing the same frequency requires the base station be able to distinguish each individual sensor. Solutions include always-on, call-and-respond, mesh, individual channels per sensor, multiplexing, mesh networks, and individual IP addresses.

Always-on assumes all sensors are broadcasting in such a fashion that the base station receives multiple signals and has to discriminate individual sensors. Although it is trivial to design sensors that broadcast indiscriminately, in deployment the nearer sensors overwhelm the signal of further ones. Even if each sensor is theoretically distinguishable, some form of communications multiplexing is required. Our reference design can distinguish up to a maximum of 64 sensors because each sensor has a unique ID. However, data is dropped if multiple sensors communicate simultaneously.

By analogy, amateur Ham radio allows any user to transmit, but by convention tells each user not to transmit if someone else is talking. Although any Ham can be always-on, that limits receipt to the most powerful transmitter (usually the closest), and effective use of a shared frequency therefore requires some protocol for negotiating when broadcasts occur.

Call-and-respond requires that each sensor only send a signal when queried by the base station. In this mode, a sensor is programmed to only transmit when it receives a command string from the base station. Each sensor can therefore be potentially broadcasting on the same frequency as each other sensor, since each only broadcasts when queried. This requires each sensor be equipped with a receiver as well as a transceiver, which adds to cost, power, and programming required. This mode works for r/c, ham and Wi-Fi modes. It requires minimal additional programming for the sensor modules.

Call-and-respond is particularly effective when using fixed deployment where GPS data is not needed from the sensor. If a given sensor is already tagged in the command software with a known position, the individual sensor need not include a GPS and therefore can have a lower power profile. The addition of a receiver (or transceiver) instead of just a transmitter incurs marginal overhead relative to running a GPS, and comparable power profiles are obtained in this mode.

Mesh devices not only transmit their data, but receive data from other nodes in their network and retransmit that data on further. The peer-to-peer functionality requires both sending and receiving, but allows for a larger geographical distribution of nodes from the central hub, as each node also acts as a relay.

Channel systems break up a given frequency into different coded channels, where a given sensor is sharing spectrum but expecting only one code. Toy r/c devices often come equipped with up to four channels, allowing for operation of up to four identical r/c devices within the same frequency. We neglect this method as infeasible for deploying the large number (>20) sensors required by our scenarios, which is not addressed by off-the-shelf transceivers at our price point.

The use of Wi-Fi individual IP addresses (sometimes labelled 'the internet of things') for remote sensors is an extremely easy solution to cluster deployment for amateurs who desire a pre-built communications system that requires minimal software or networking expertise. In this model, each sensor has a unique ID and the base station gathering data. It is one specific implementation of multiplexing, and has the advantage of using an existing protocol (TCP/IP) that is easily implemented in the target hardware.

One reason for using pre-existing COTS modules is that the network topology for the multiple sensor pods will already be implemented. Given our target user is not assumed to be skilled in communications, we focus less on the specific local implementation and more on the operational limits. The topology internal to the devices must support multiple (up to 64) devices relaying to a central hub, with each individual sensor tagged with a unique identifier so we can distinguish where the data came from. In addition, we are assuming low bandwidth data being broadcast infrequently (time scales of minutes) to minimise network clashes that could lead to dropped data. This still leaves the problem of what to do with the aggregate data once it is received at the local hub.

From a sensor pod point of view, any data item can be stamped with a sensor ID, and a data value, to which the controlling chip adds a GPS location and a pod ID. This completes the data set to provide the full capture needed by the base station. The final component is the data channel to get data from the hub to the remote data user.

## Hub to user communications

Once the multiple individual sensors have relayed their data to our local hub, that hub needs to rebroadcast the full data set using a different protocol and network to our remote end user, who will be kilometres away. The easiest scenario for hub-to-user is that wired or Wi-Fi internet access is feasible from within a short distance of the sensor network. Amateur radio transmissions allow for a longer range than conventional Wi-Fi. Alternately, the hub can be fitted with GSM (capability to enable remote data delivery of the aggregated sensor data. If wired or wireless internet access exists, then our model of multiple sensors → hub → user uses ordinary internet (TCP/IP) to deliver the data to the user. Because we are investigating possible disaster areas or remote regions, however, we cannot assume an existing internet infrastructure is available.

A second technique, used in our high altitude balloons, is an amateur-band handheld radio (e.g. a \$35 Baofeng UV-5R or similar radio) to rebroadcast the signal at 4 watts VHF (136-174 MHz) or 1 watt UHF (400-480MHz). This radio can be wired into the Arduino base station and requires a matching receiver station at the destination. The power lifetime for the radio is typically 10 hours, with a range of 2-5 miles or more; ranges of up to 30 miles have been achieved with a clear line of sight in outdoor tests.

Use of amateur radio frequencies requires an FCC or regional equivalent of a Technician's ham licence to operate, but if it is being used for an unmanned base station constantly transmitting, this would be already violating FCC requirements (ECFR.gov 2014). FCC Low Power Radio Station (LPRS) allow transmission of data but not for sensor use. Other wavebands have different requirements, and navigating radio licensing is often a skill set not possessed by a typical science, hobbyist, or amateur team.

One area used in amateur systems is incorporating a smartphone using G3, G4 or G5 data transmission within a standard cell phone contract. High altitude balloons (again) have used ordinary cell phones as their data transmission channel. GSM modules are available via subscription (typically US \$5-10/month) that attach to an Arduino or other microcontroller to provide transmission via GSM networks (Di Justo 2013). This model requires subscription to a GSM network. The cost for a single GSM or smartphone contract for a hub is feasible for amateur and citizen deployments, and is recommended for projects that do not have radio licensing knowledge or permission, and also lack internet access onsite.

Figure 1 illustrates the three most likely hub-to-user network models, arrayed in increasing cost as well as potential area coverable. A sensor network using our reference design, where each sensor communicates via short-range (150-foot) radio signals with a single hub, that then

Commented [R1]:

relays to a satellite or internet provider, provides the lowest cost per-sensor but requires the sensors to be in close proximity to each other, restricting the total area covered. If the sensors have mesh capability, each sensor can be placed increasingly further from the base, extending the region covered but requiring a higher cost per sensor. The third option posits that each sensor has its own direct GSM satellite capability, removing the need for a hub and substantially increasing the potential area covered, but at greater economic cost, as it requires per-sensor GSM contracts.

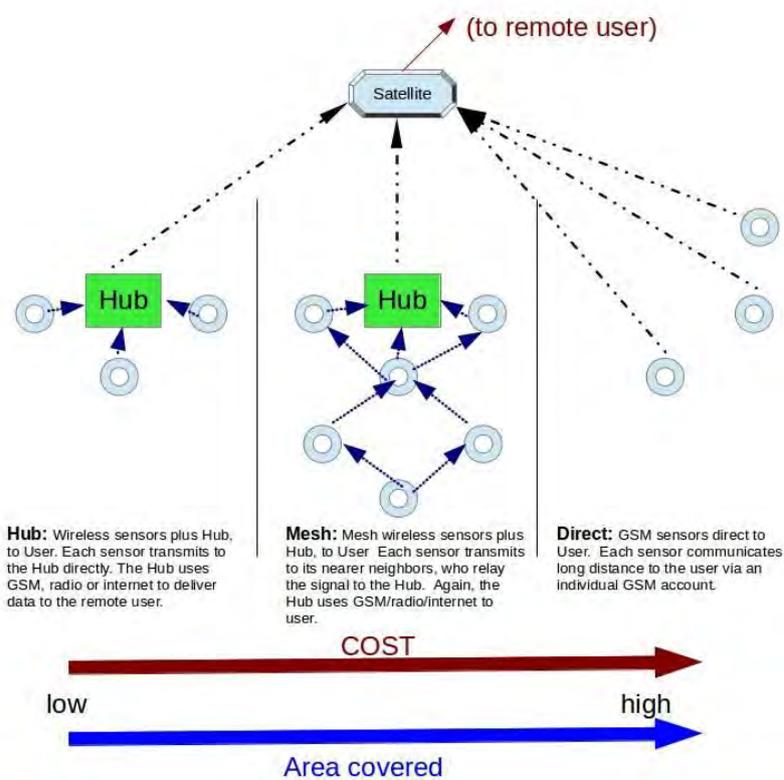


Figure 1. The three most likely hub-to-user network models

## Survivability and recoverability

Placing sensors in pre-planned locations or having sensors report GPS information also ensures better recovery after the measurement period is over. The period can be defined as

- the time needed to acquire enough data,
- the time from start to end of crisis, or
- the time until the sensor power has run out.

We prefer recovery scenarios even when there is no economic driver (when the cost in staffing to recover the sensor is higher than the sensor cost), as reducing ecological waste in a good practice for scientists and monitors to encourage. One sensor in a forest might seem minor; a network of 64 is an annoyance; three universities all deploying 2000+ sensors is an ecological mistake.

Use of an onboard GPS for a sensor pod eliminates the need for specific placement and allows for more rapid deployment, potentially by non-technicians with no finesse needed. A GPS typically adds \$30 to the cost and provides exact positions (within the US, accuracy to 3.5 metres). A robust throwable or droppable sensor pod that provides its own position information is recommended because it provides flexibility in multiple scenarios where access to the terrain or locale may be more difficult than expected. Difficulties can include regions that are flooded, have traffic blocked away, are restricted access, or are geologically precarious for humans to access.

Deployment of sensors also requires cases sufficient to survive the environment. For benign environments exposed only to ordinary weather, a plastic case suffices. Sensors designed to operate in hostile environments, including in lava, in fire, and under water, are beyond the scope of this article. We do note that a good amount of data for situations such as the growth of a forest fire can be provided with a destructible sensor that simply stops broadcasting when the fire reaches it, thus providing the necessary data point on fire line expansion.

Creating a shell for the cheap sensors can be done in small batches using existing 3-D printing technology. The casing of our device is created using a 3-D printer in order to make a form suitable for the environment expected. Pods dropped or launched will have to survive an 'egg-drop' type test to ensure the electronic contents survive. Any pod expecting water or chemical contaminate will have to be tested to survive that environment. Pods to measure fire can be presumed to only survive until the outer casing melts, at which point ceasing of transmission due to casing damage is itself the final data point. Our best guidelines are that 3-D printing enables rapid iteration of testing until a given casing is shown to survive ([Antunes et al 2013](#)).

For our lab tests our requirement was '3-D cube at 10cm x 10cm x 10cm able to withstand the static weight of a person, a dynamic drop from 1 metre, temperatures down to -60C, and pressures down to a soft vacuum', as our cubes were designed to support high altitude balloon tests. It took five iterations by a single student to create a suitable 3-D shell. We therefore suggest shell design is a straightforward engineering problem easily solved through appropriate iteration and testing.

## Implementation challenges

Social and legal concerns are a possible implementation challenge. [Di Justo and Gertz \(2013\)](#) note that one should “not deploy your gadget in public without official permission”, citing two cases where well-intentioned citizens were arrested for placing devices that police later

mistook as potential bomb threats. An unexpected box of electronics with a blinking light in public is, in their assessment, a risk. They suggest three strategies to mitigate causing alarm.

Firstly, official permission can sometimes be obtained by regional Parks Departments or by the government or private entity that owns the land. If the project is educational signed support by your institution must be obtained. Secondly, when deploying sensors in a community, discuss the project with the community before implementing the research.

Finally, in addition to communicating to the public and police prior to deploying multiple electronic devices, we also recommend clear labelling of your devices. However, also note that labelling alone may not suffice, as demonstrated by the example of students at Carnegie-Mellon University, who had to answer to police and had their equipment confiscated despite clear labelling ([Di Justo 2013](#)). Despite having solved the technical challenges, potential legal and human risks remain.

## Conclusions

Networked deployable low-fidelity environmental sensors are an active field of study as well as entrepreneurship. We assert that an individual or small group can accurately sample a moderate region, on the scale of a kilometre or so, with sensors that report every few minutes over a several day period to a base station located kilometres away. The cost per sensor is well under US\$100 and requires no special engineering talent. Covering small geographic region using simple sensors that relay data to a local hub, which then communicates that data to a remote user using GSM, is economically and technologically simple and available to general citizens. This enables citizen and activist groups as well as research entities to tackle small-scale projects for specific targeted goals.

The technology is available for amateurs and non-engineers through use of DIY resources, inexpensive pre-built hardware, 3-D printing, and conventional internet. Design of a custom project is largely an exercise in component selection, followed by integration and testing. The sample build presented is documented and freely available via internet resources. The primary limitation in deploying a large number of sensors is ensuring there is a viable communications channel from near the remote site, to the home base of the user.

For situations ranging from fires and crises through to urban monitoring, cheap deployable sensors fill a gap between existing satellite-based and large autonomous sensor deployment by government and commercial entities, and single-user sampling via individuals or drones. The ease of design and deployment should be approached with an eye towards minimising adding technological pollution to an environment, and also needs to follow existing communications licensing and use policies. Within this framework, we feel that the growth of this technology is a positive force carrying minimal risk in enabling new groups to monitor measurable situations and potentially improve local environmental conditions.

## References

- Allan A. 2014. 'Which Board is Right for Me'. *Make Magazine*. 36. Available from: <http://makezine.com/magazine/make-36-boards/which-board-is-right-for-me/>
- Antunes, A; Walters, A.; Bormanis, M.; Schrenk, R. 2014. 'Constrained Multi-Altitude Design Using 3-D Printed CubeSat Shells'. *AIAA SciTech* 2014. Available from: <https://www.aiaa.org/Secondary.aspx?id=20342>.
- Arduino.cc. 2014. <http://forum.arduino.cc/index.php?topic=63138.0:wap2>
- Boak, K. 2012. 'Building Wireless Sensing Networks- using Open Source Hardware'. Nanode LLC. Available from: <http://www.nanode.eu/news/building-wireless-sensing-networks-using-open-source-hardware/>
- Di Justo, P. and Gertz, E. 2013. *'Atmospheric Monitoring with Arduino'*. O'Reilly/Maker Press.
- ECFR. 2014. US Government Printing Office. Available from: [http://www.ecfr.gov/cgi-bin/text-idx?SID=e593ed9f147a6ee87a8803d05b9667c9&tpl=/ecfrbrowse/Title47/47cfr95\\_main\\_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?SID=e593ed9f147a6ee87a8803d05b9667c9&tpl=/ecfrbrowse/Title47/47cfr95_main_02.tpl)
- Gertz, E. and Di Justo, P. 2012. *'Environmental Monitoring with Arduino'*. O'Reilly/Maker Press.
- GPS.gov. 2014. <http://www.gps.gov/systems/gps/performance/accuracy/>
- Greene, K. 2014. 'Nest Competitor Monitors Your House's Leaks on the Cheap'. *MIT Technology Review*. Available from: <http://www.technologyreview.com/news/523741/nest-competitor-monitors-your-houses-leaks-on-the-cheap/>
- H2OTech.2014. Available from: <http://www.h2otechonline.com/innovations/remotetracker/faq/>
- Hanscr. HWStartup. 2013. 'How to run an Arduino on a 9V battery for Weeks or Months'. Available from: <http://hwstartup.wordpress.com/2013/03/11/how-to-run-an-arduino-on-a-9v-battery-for-weeks-or-months/>
- Lipsky, J. 2014. 'Sensors Build Case Against Cold'. *EE Times*. Available from: [http://www.eetimes.com/document.asp?doc\\_id=1324130](http://www.eetimes.com/document.asp?doc_id=1324130)
- Marshall, P. 2014. 'Ant-sized radios for the Internet of Things'. Government Computing News (GCN). Available from: <http://gcn.com/blogs/emerging-tech/2014/09/iot-radio-chip.aspx>
- Middleton, C. 2014. 'Building a Digital Society'. *Australian Journal of Telecommunications and the Digital Economy*, Vol 2, No 1, Article 27. Available from: <http://doi.org/10.7790/ajtde.v2n1.27>
- Miller, E. 2014. 'North State entrepreneurs innovate for efficient water use.' North Valley Correspondent. Available from: <http://www.centralvalleybusinesstimes.com/stories/001/?ID=26826>
- MakerShed. 2014. See <http://www.makershed.com/products/wireless-sensor-node>

# Locating disaster communication in changing communicative ecologies across the Pacific

Jessica Noske-Turner

RMIT University

Jo Tacchi

RMIT University

Heather Horst

RMIT University

Evangelia Papoutsaki

Unitec Institute of Technology

## Abstract:

The Pacific Island region is geographically and culturally diverse, with a significant range of communication infrastructures and challenges. Access and use of mobile phones has risen exponentially over the past five years. According to ITU statistics, around 60 percent of Pacific Islanders had access to a mobile in 2012, compared to just 10 percent in 2006. In many Pacific countries mobile phones are, therefore, emerging as a key element of the local communication systems, and are being built into disaster management and communication plans. For these plans to be effective, however, we argue that access to, and affordability of, technologies represent only one dimension of what needs to be considered in effective disaster communication plans. They also need to consider appropriate technologies, local communicative ecologies, systems for the ownership and maintenance of infrastructures, and local knowledge and belief systems. With a focus on mobile and other telecommunications technologies, this paper provides an overview of disaster communication systems and infrastructures, practices and challenges in the region.

## Introduction

Mobile phones are often the first electronic communication technology to be accessible to remote or previously unconnected populations, facilitating a 'multiplicity of relationships in areas that used to be relatively isolated' (Tenhunen 2008:516). Mobiles have become integrated into livelihood strategies and economic activity (Donner 2008; 2010; Jensen 2007; Wallis 2013), 'social logistics' (Tenhunen 2008) and the maintenance of relationships within and across national boundaries (Horst 2006). In times of natural and human-made disasters, they have also been viewed as holding potential for circulating and crowdsourcing information (Heinzelman & Waters 2010; Roche et al 2013), providing status reports (Bengtsson et al 2011),

moving money ([Mas & Moraczynski 2009](#)) and documenting and 'witnessing' violence through videos and cameraphones ([Reading 2009](#)). Yet, the ways in which these technological affordances (often viewed as technological 'solutions') and the specifics of how this happens in particular places varies according to local social and cultural conditions as well as communication practices and cultural contexts. As some of the broader literature on mobile media and communication demonstrates, we need to pay attention to the different ways in which mobiles are appropriated and used in local contexts ([Ling & Horst 2011](#); [Sey 2011](#); [de Souza e Silva et al 2011](#); [Wallis 2013](#)). Mobiles can contribute to disaster communication and other social challenges, but they also need to be understood and utilised through local cultural and meaning systems ([Horst & Miller 2006](#); [Horst & Taylor 2014](#); [Pertierra 2002](#); [Wallis 2011](#)).

In this paper we argue that local communicative ecologies need to be understood for the effective development of disaster communication plans and approaches. To make our case, we draw upon the findings from the Pacific Media Assistance Scheme (PACMAS)<sup>1</sup> baseline study, a study of the state of media and communication across 14 countries in the Pacific region ([Tacchi et al. 2013](#)). The baseline was commissioned by ABC International Development and undertaken by a team of researchers from RMIT University (Australia), Unitec (New Zealand) and University of Goroka (Papua New Guinea) over ten months in 2012 and 2013. Data was collected according to a set of themes defined by PACMAS, through desk-based research, interviews with 212 'stakeholders' from across the region, and 25 interviews with members of a Panel of Expertise. We sent researchers to all 14 countries for between 2 and 7 days to conduct the stakeholder interviews. 'Stakeholder' interviews were conducted with the following groups of people:

- TVET (Technical and Vocational Education and Training) coordinators and providers
- Broadcast/communications technicians in government, telecommunications companies and broadcast (especially radio) organisations and media/communication technicians
- Government representatives involved in the planning and management of disasters and crises
- Media managers and professionals in state, private, community, mainstream media
- Communication for Development (C4D) & ICT and development initiatives
- Climate change scientists, government ministers or representatives responsible for climate change
- NGO/CSOs that have climate change as part of their remit, NGO/CSOs that focus on youth and have climate change as part of their remit
- Health department officers/ministers; public health professionals/researchers
- National media association representatives

The Panel of Expertise was made up of 28 people from across the region. Panel members were asked to complete a short questionnaire and verification document via email or phone. The verification document focused upon legislation and the media and communication environment in each country. This provided a mechanism for checking on whether data sourced through desk based research was up to date and accurate.

The Pacific region has a rich and complex media and communication environment. Radio, and in some areas television, are important platforms for communication across vast distances and audiences, while newer information and communication technologies have entered the media and communications landscape. Populations across the 14 countries included in the baseline study range from 1,538 to over 7 million. The demographic and geographic differences are extreme; for example Nauru is one island of 21 square kilometres, while Kiribati consists of 33 low-lying coral atoll islands, across 3.5million square kilometres of ocean. The fastest growing new technology in the region is the mobile phone. According to ITU statistics, in 2012 around 60 percent of Pacific Islanders had access to a mobile, compared to just 10 percent in 2006. Mobile phones are used in a variety of ways including voice communication and SMS (text), accessing the Internet and social media ([Anderson 2013](#); [Handman 2013](#); [Lipset 2013](#); [Watson 2011](#)). In a number of Pacific countries (e.g. Fiji, Papua New Guinea, Samoa and Tonga), mobiles are increasingly being used for banking, payments and the circulation of transnational remittances ([Horst 2013](#)). Mobile phones are also 'converging' with other media by providing access to camera phones, video and Bluetooth functions that enable people to share and transfer images and other files between mobile phones. However, despite the growth in mobile phones and internet access, and the convergence of broadcast and ICTs in the region, barriers to the use of and participation in local and regional media and communication spaces still remain.

In the first section of this paper we describe the communicative ecologies approach. We then explore the range of disaster communication plans across the region. In the concluding section we illustrate the importance and relevance of a communicative ecology approach to unpack and inform responses to diverse communication environments in disaster communication planning.

## Communicative ecologies

Mobile phone networks may be the first electronic communication infrastructure to reach many populations across the world, but they are not entering into a communication vacuum. Communicative ecologies refer to the complex systems of communication, media and information flows in a community, or the communicative assemblages ([Slater 2013](#)). Taking a

communicative ecology approach means not assuming a hierarchy of ways of communicating, and being open to alternative ways of classifying communication and media platforms across different cultural locations. The approach prioritises local specificities of the ways in which information and communication flow between people and how this is understood. Here communication channels include not just electronic media channels but also through institutions (for example, kinship networks, various organisations and government departments), roads and buses, and any other communication channels, processes and practices that are significant in a particular context. Communicative ecologies are the everyday, complex networks of information and communication in individual and community lives. Our communication networks are complex and based on individual decisions and choices about how to use various media platforms, as well as broader issues of availability and access, and social and cultural barriers and opportunities. Understanding how information flows and how communication takes place is particularly important when it comes to understanding media and communication for development. All forms of communication and mediation are relevant to communicative ecologies, and this helps to ensure we consider and include new media infrastructures, platforms, devices and practices in our analysis, including broadband, social media and mobile phones as well as traditional and face to face communication protocols and practices.

For example, effective disaster planning and preparedness communication in Tuvalu requires an understanding of the cultural contexts, especially in relation to the local framing of climate change risks within Christian narratives. Although Tuvalu figures frequently in western news stories and documentaries in association with climate change, and despite the continual arrival of foreign journalists, the awareness of climate change and the increased risk of potentially devastating disasters among Tuvaluans is low and western information does not filter through to local people (Farbotko & Lazrus 2011). This is especially true for people living on the outer islands. One participant from the NGO sector in Tuvalu interviewed for the baseline study stated:

*You know, the world is more aware about Tuvalu and climate change than most people, like the local people here, you know... I mean, this sort of makes me worry too.* (Tuvalu respondent number 9, see Tacchi et al. 2013).

Christian narratives, and especially the story of Noah's Ark, are deeply embedded in local public discourses on climate change and natural disasters, and influence the circulation of information in relation to increased risks associated with climate change (Paton & Fairbairn-Dunlop 2010,

see also [Rika 2013](#)), an observation echoed by many interviewees. The respondent quoted above explained the implications of the strong faith in divine protection from natural disasters among many Tuvaluans:

*I think last two years a lot of awareness on climate change and the impact, [but] people still ignore and they, you know, the Bible when Noah's Ark, when God says, I'll give you a sign that there will be no more flood, and that is in the back of their mind today. They always refer to the Bible. (Tuvalu respondent number 9, see [Tacchi et al 2013](#)).*

At other times, the information provided by the Churches complements awareness campaigns. Some churches are taking a proactive stance on this issue and play a leading role in climate change communication, which becomes particularly relevant in the context of the Christian narratives discussed above. Church representatives regularly visit communities on outer islands to present biblical and scientific information about climate change. One such person regularly writes a sermon in a monthly newsletter on climate change. More broadly, the Pacific Conference of Churches (PCC) has been working on advocacy and awareness programs on climate change through its network of church leaders, women and youth organisations ([pacificconferenceofchurches.org](http://pacificconferenceofchurches.org)). By contrast, the local mass media does not seem to have been a key part of climate change engagement so far.

Mobile phones enter existing communicative ecologies and, in the process, alter them. They are appropriated and made meaningful by local communities within their local context, grounded in the realities of the everyday lives of individuals and groups ([Tacchi 2014](#); [Tacchi, Kitner & Crawford 2012](#)) and depending on availability, affordability and a wide range of access issues. The legislative and regulatory infrastructures, cost, as well as geography are also important. By comparing these across the 14 countries<sup>2</sup> we can see that there are complex and diverse interrelationships between deregulation, policies, processes and practices. For example, Niue, which is unique among these countries for providing free public Wi-Fi, also has a lower mobile phone penetration rate.

**Table 1: Comparative media and communication environments in Melanesia**

Country	Television	Radio	Print	Telecoms	Population and geography
<b>Fiji</b>	4 commercial companies offering 20 channels 1 church network	2 government 10 commercial 2 church 2 community (one campus)	12 commercial 3 daily, 4 weekly, 4 monthly, 1 quarterly 1 student 2 community	Telecoms competitive environment. 84% mobile penetration, 28% access the internet (in 2011), rapidly growing due to mobile phone expansion	868,400 pop 332 volcanic islands, approximately 110 inhabited, over 18,274 sq km
<b>PNG</b>	1 commercial 1 public 1 commercial (satellite)	3 government 7 commercial 2 community 5 church	3 commercial 1 church	Telecoms competitive environment. 38% mobile phone penetration 2% access the internet	7,013,829 462 sq km, a group of islands including the eastern half of New Guinea island, mountainous interior (Highlands)
<b>Solomon Islands</b>	2 commercial 1 government (international) 1 church (international)	4 government 2 commercial 1 church 1 community	4 commercial	Telecoms competitive environment. 50% mobile phone penetration, 6% access the internet	538,000 27,986 sq km, 992 islands
<b>Vanuatu</b>	1 government 2 foreign government 2 church (international)	2 government 1 commercial 1 community 1 church	3 commercial	Telecoms competitive environment. 76% mobile phone penetration, 8% internet access	245,600 pop 12,189 sq km, 83 Islands (65 inhabited)

**Table 2: Comparative media and communication environments in Polynesia**

Country	Television	Radio	Print	Telecoms	Population and geography
<b>Cook Islands</b>	2 commercial 7 community on outer islands	4 commercial, only one with almost national coverage 1 community	2 commercial newspapers 1 daily & 1 weekly	Telecoms monopoly, private company. 66% mobile penetration. Internet 'expensive and slow' <sup>3</sup>	20,000 pop 15 islands, 12 inhabited, over 236 sq km, mix of low-lying coral atoll islands, and hilly volcanic rises
<b>Niue</b>	1 government	1 government 1 hobby	1 commercial, every 3 weeks	Telecoms government monopoly, but free public wifi. 38% mobile phone penetration, 83% access the internet	1,538 pop Island of 260 sq km
<b>Samoa</b>	2 commercial 1 church 1 commercial (foreign-owned)	1 government 5 commercial 4 church 1 community	2 government 3 commercial 3 commercial (foreign-owned) 1 community	Telecoms competitive environment. 91% mobile penetration, 7% access the internet	183,900 pop 2,831 sq. km, includes 2 main islands, several smaller uninhabited islets; a narrow coastal plain with rugged volcanoes in the interior
<b>Tonga</b>	1 government 1 commercial 2 church	1 government 5 commercial 1 church	4 commercial 3 church	Telecoms competitive environment. 53% mobile penetration, 12% access the internet	104,500 pop. 260 sq. km, archipelago consisting of 176 islands, 26 of which are inhabited
<b>Tuvalu</b>	No service	1 government	None	Telecoms government monopoly. 20% mobile phone penetration, 40% access the internet	9,847 pop 9 islands, land area 26 sq km

**Table 3: Comparative media and communication environments in Micronesia**

Country	Television	Radio	Print	Telecoms	Population and geography
<b>FSM</b>	4 commercial one in each state	4 government 2 commercial 1 church 1 community	1 community bi-weekly	Telecoms monopoly, public corporation. 25% mobile penetration, 20% access the internet	107,008 pop  607 islands, combined land area of 702 sq km, spread over 2,600,000 sq km of ocean, made up of 4 federated states
<b>Kiribati</b>	1 government currently not operating	2 government 1 commercial	1 government 2 commercial 1 church all weekly or less frequent	Telecoms monopoly, government owned. 14% mobile penetration, 10% access the internet	103,000 pop 33 low-lying coral atoll islands, 21 inhabited, land area of 811 sq km, across 3,500,000 sq km of ocean
<b>Marshall Islands</b>	2 commercial with limited coverage 1 US armed forces	1 government 1 commercial 2 church 1 US armed forces	1 commercial, weekly	Telecom monopoly, private owned, government controlled. 7% mobile penetration, 3.5% access the internet	54,800 pop 29 coral atoll islands, 24 inhabited, land area 181 sq km, spread over 1,210,000 sq km of ocean
<b>Nauru</b>	1 government	1 government	1 government, monthly	Telecoms competitive environment. 65% mobile penetration, 6% access the internet	10,300 pop 21 sq km, phosphate rock island.
<b>Palau</b>	1 part government owned 2 commercial	1 government 3 commercial 2 church	1 government, irregular 3 commercial, two published irregularly and one twice weekly	Telecoms near government monopoly. 80% mobile phone penetration, 6% access the internet	26,610 pop > 300 islands, 8 inhabited. Mountainous and low, coral islands. land area 458 sq km

As the media and communication environment becomes more complex, questions remain about the appropriateness of ICTs for specific purposes, such as disaster communication. For example, there is uncertainty in some places about the ability of broadcasters and technicians to keep up-to-date with the latest equipment and software and the consequences of integrating ICTs like mobile phones into communication plans, compared with ‘tried and tested’ technologies such as broadcast radio. Studies of media in the Pacific – especially in large countries such as Papua New Guinea – from only five years ago considered access to new digital infrastructure less relevant than access to traditional media, especially radio (Duffield, Watson and Hayes 2008). More recent studies find ICTs are becoming more relevant, and indeed are under-utilised for development despite presenting significant potential (Cave 2012). In places such as PNG, where radio has been a dominant and effective platform, recent studies suggest that more households now have access to mobiles than to radio (Intermedia Europe 2012). In fact, our research, and the research of others, suggests that people are increasingly using their mobile devices to access radio programmes (Cave 2012). Intermedia Europe found that in PNG, mobiles are amongst the most common ways to access the Internet, with Facebook one of the most accessed sites (Intermedia Europe 2012).

Communicative ecologies, and the place of mobile phones within these, may differ from person to person and across generations too. For example, Marion Muliaumaseali'i, a PhD researcher in Samoa, used the communicative ecologies approach to reflect on the generational difference in seeking information, and the perceived trustworthiness of different information sources ([Muliaumaseali'i 2014](#)). She describes how she heard about a tsunami warning on Facebook from a friend who worked for the Samoan government. She 'googled' the earthquake and found that a tsunami watch warning had been issued. She then gained more information from her taxi driver who felt the quake and was listening to the state radio station, 2AP, as it was broadcasting about the warning in Samoan. She contrasts this with her grandmother and aunt's preferred communication platforms. The aunt, in her late 50s, and the grandmother, in her 90s, 'would only believe that the warning was cancelled once it was announced on the radio', even though this information was already available online.

Despite the growth in mobile phones and internet access, and the convergence of broadcast and ICTs, barriers to the use of and participation in local, national and transnational media persists. In the baseline research we found that the internet in Tuvalu (provided by the government) was often down for days at a time and, when available, had serious connection problems. The quality and availability of mobile phone signals varies across the countries, and within countries, so that in some places people have to walk to 'bush phone booths', a term to describe a location where there is reception ([Intermedia Europe 2012](#)). The geography of media access impacts on the diversity of media sources in specific locations in the Pacific. In PNG levels of accessibility are mainly associated with geography rather than demographics such as age, gender and education ([Intermedia Europe 2012](#)). Geographic regions can be described in terms of whether they are 'media-rich' or 'media dark' ([Intermedia Europe 2012](#)). In PNG, media dark areas are predominantly located in the islands. TV and newspapers are mainly accessed in urban areas, so that radio and word of mouth remain a significant source of information, especially via family members and friends who travel between provinces in PNG. This situation of differential access is repeated in different ways in other Pacific countries, such as Tuvalu, Marshall Islands, Palau, Kiribati where isolation means that outer islands receive only government radio, or sometimes no mass media at all. Face-to-face communication remains highly valued across all Pacific countries.

## Comparison of Disaster Communication Plans and Systems

A range of media and communication platforms are now being used to provide access to early warning systems before a disaster. Tables 4, 5 and 6 below compare the existence of policies and plans in each country (arranged by region), and the types of communication platforms used.

**Table 4: Role of media in disaster response and preparedness in Melanesia**

Country	Relevant legislation	Main institutions & organisations	Role of broadcast media	Role of telecom	Primary media platforms used
<b>Fiji</b>	Disaster Management Act (1998), National Disaster Management plan (1995), municipal disaster management plans.	National Disaster Management Council (DISMAC), Red Cross, Public Works Department (PWD), Ministry of Health, Ministry of Agriculture, the Military, the Police, Fiji Meteorology Service.	Government broadcasters (Radio Fiji and FM96) are formally integrated into National Disaster Plans.	Formal agreements in place for the provision of free emergency calls (Telecom Fiji, Vodafone & Digicel), and use of networks during disasters (Telecom Fiji & Digicel).	Radio Fiji & FM96 sirens (in Suva) official websites email TV social network sites SMS messages (Vodafone)
<b>PNG</b>	Disaster Management Act currently being reviewed. PNG Vision 2050, National Disaster Management Plan, National Disaster Mitigation Policy and Disaster Risk Reduction, and Disaster Management National Framework for Action 2005 – 2015.	National Disaster Centre, provincial disaster offices, military, National Weather Office, Geo Physical Observatory	Formal disaster plans involve the National Broadcasting Corporation (including its 19 provincial stations) to disseminate information.	Telecoms are formally integrated into disaster plans, however most disaster initiatives are based on informal agreements.	NBC Radio (including provincial stations), some use internet and mobile communications. HF radio (for emergency services).
<b>Solomon Islands</b>	National Disaster Risk Management Plan 2010 for Disaster Management Arrangements and Disaster and Climate change Risk Reduction, (national plan in progress)	National Disaster Management Office, National Disaster Councils (national and provincial), Police, Red Cross, NGOs and civil society, private sector, Ministry for Energy and Mines, Meteorology Service.	In the National Disaster Risk Management Plan Broadcasters are considered 'Critical Infrastructure Agencies' and are therefore formally required to work within the plan. In the event of an emergency, SIBC hands control over to the NDMO.	Telekom is included in the national Disaster Risk Management Plan. NDMO may seek assistance from Telikom in emergencies.	Radio (SIBC), church bells or conch shells. HF Radio and email among disaster responders. Telekom is exploring opportunities for warnings via mobile phones.
<b>Vanuatu</b>	Disaster Risk Reduction (DDR) and Disaster Management (DM) National Action Plan (2006-2016)	Vanuatu Meteorology and Geo-Hazards Department (VMGD), National Advisory Board (NAB) on Climate Change and Disaster Risk Reduction, National Disaster Management Office (NDMO)	Formal agreement (MOU) signed between VBTC the NDMO & VMGD outlining procedures for broadcasting of official emergency information. NDMO send emergency information updates to all radio stations, including VBTC.	Informal agreements are being developed between Meteorology and Digicel (among others). Telecom providers have internal plans.	Radio (VTBC), warning lights at Police Headquarters, satellite phones (in each village). Currently no agreement on using mass-SMS messages or other ICTs.

Table 5: Role of media in disaster response and preparedness in Polynesia

Country	Relevant legislation	Main institutions & organisations	Role of broadcast media	Role of telecom	Primary media platforms used
<b>Cook Islands</b>	National Disaster Management Act drafted in 2007 but not passed.	Emergency Management Agency, Police Commissioner, Media Office, Minister of Works, Red Cross	Currently no formal arrangement for emergency broadcasting; plan is reportedly in progress.	Currently no formal arrangement with Telecom for service provision during a disaster	Radio (especially Radio Cook Islands) Sirens (on Rarotonga only) HF radios Satellite phones Telecom has an emergency plan. Some capacity to send SMS messages.
<b>Niue</b>	National Disaster Plan (2010), Public Emergency Regulation (2004)	National Disaster Council, Chief of Police, Niue Meteorology Service	The government radio (BCN Radio) is formally integrated into the National Disaster Plan.	Niue Telecom is formally integrated into the National Disaster Plan.	Radio Sunshine (BCN), police cars travel to villages. Plans for sirens. Niue Telecom is exploring options for mass messages via mobile phones. Response stakeholders use email, phones, paper notes and HF radio communication
<b>Samoa</b>	National Disaster Management Act 2007, National Disaster Management Plan (2011-2016)	Disaster Monitoring Office, Disaster Advisory Committee, Police, Samoa Meteorology Division, Ministry of Natural Resources and Environment	Media organisations are included in the National Disaster Plan, and formal plans describe the government AM radio station, 2AP, as the primary media outlet in emergencies.	The National Emergency Telecommunications Plan involves Digicel and BlueSky Samoa.	2AP (government AM radio broadcaster), network of sirens and bells. Digicel can send mass-SMS messages
<b>Tonga</b>	Emergency Management Act 2007, National Emergency Management Plan 2007, draft Tsunami Plan	National Emergency Management Committee, National Emergency Management Office, Tonga Meteorological Service, Regional Meteorological Office in Fiji	National Emergency Management Plan (2007) outlines the roles of the Tonga Broadcasting Corporation (TBC). TBC is expected to continue live broadcasts throughout impact. Work on the TBC Emergency Management Plan is in progress	National Emergency Management Plan (2007) outlines the roles of the Tonga Telecommunications Corporation (TTC). Responsible for maintenance of telecommunication capacity, reporting to Government on capacity status.	Radio Tonga (TBC), commercial media outlets, mobile phones (for calling). Warning sirens being piloted. Digicel uses a bulk SMS system.
<b>Tuvalu</b>	National Disaster Plan (1997, revised 2011), Disaster Management Act (revised 2007)	National Disaster Management Committee, Disaster Task Force, Tuvalu Meteorology Service	No official emergency broadcasting plan. Disaster Task Force responsible for information dissemination via Radio Tuvalu	ICTs are not integrated into national plans. Telecom provider has internal plans.	Radio (Tuvalu Radio), police cars with sirens and loudspeakers, satellite phones (for communication to outer islands)

**Table 6: Role of media in disaster response and preparedness in Micronesia**

Country	Relevant legislation	Main institutions & organisations	Role of broadcast media	Role of telecom	Primary media platforms used
<b>FSM</b>	Disaster Preparedness Plan review currently being approved.	Department of Public Safety, FSMTC, Public Utilities Corporation, Public Transport Agency, local government, Red Cross, International Organisation for Migration (IOM), Salvation Army, and private businesses, National Weather Service Office.	Local radio stations are included in the Disaster Preparedness plan; but lack of awareness of this among stakeholders. Currently no formal emergency broadcasting plans.	Currently no formal plans, but indications that ICT use in disaster response is on the agenda	Police announcements using loud hailers & PA systems, warning sirens (in Pohnpei only) HF radios
<b>Kiribati</b>	National Disaster Act 1993 (was never implemented). National Disaster Management Plan endorsed in 2012.	Disaster Risk Management Office (DRM), National Disaster Management Committee (NDMC), Office of the President, Kiribati Meteorological Service (within the Office of the President)	Currently no formal agreements are in place; informal plans are for the NDMC to make all announcements via Radio Kiribati	An agreement is being developed with Telecom.	Radio Kiribati, police cars & loud speakers, police VHF radios. Currently no mass-SMS systems.
<b>Marshall Islands</b>	National Disaster Management Plan (1997), official current plan is not publically available.	Chief Secretary's Office, Disaster Management Committee, Atmospheric Technology Services Company ATSC (US Military administered on Kwajalein Atoll)	Currently no formal emergency broadcasting plans; informal plans are vague but involve announcements via V7AB (radio)	No formal agreements; telecom industry undergoing change. See <a href="http://www.worldbank.org/en/news/press-release/2013/03/19/world-bank-marshall-islands-launch-new-strategy-to-strengthen-partnership">http://www.worldbank.org/en/news/press-release/2013/03/19/world-bank-marshall-islands-launch-new-strategy-to-strengthen-partnership</a>	Internet (between disaster responders) HF radios (especially to outer islands) Mass SMS systems not used due to legal barriers.
<b>Nauru</b>	Disaster Risk Management Act 2008	National Disaster Risk Management Office (NDRMO), Emergency Operations Centre, Police Commissioner, President	The Disaster Risk Management Act states that TV and Radio will be used for emergency broadcasting but there are currently no formal emergency broadcasting plans	No formal agreements; ongoing discussions	Police and Digicel have satellite phones. NDRMO is considering other warning options (sirens or PA system). Digicel can disseminate SMS warnings
<b>Palau</b>	National Disaster Risk Management Framework (2010)	National Emergency Management Office, Red Cross, Police, National Weather Service	Formal plans describe an expectation of compliance by broadcasters to follow NEOC direction. Media staff must liaise with the NEOC for updates	No formal agreement with telecoms. See also: <a href="http://www.sidsnet.org/msi_5/docs/nars/Pacific/Palau-MSI-NAR2010.pdf">http://www.sidsnet.org/msi_5/docs/nars/Pacific/Palau-MSI-NAR2010.pdf</a>	Radio, house-to-house visits in some areas.

As Tables 4, 5, and 6 illustrate, some countries have highly developed and comprehensive plans integrating a range of communication infrastructures and platforms. For example, Fiji and

Samoa have some of the most comprehensive activities. Fiji, which has a national team that coordinates the response to and information dissemination on the impacts of climate change and disaster preparedness, has a disaster communication plan that includes the use of: telephone, internet, warning sirens, short wave equipment, human resources and key individuals, cars with speakers, word of mouth and NGOs, to inform the public. They also embrace traditional knowledge and warning systems (i.e. observations of natural phenomena). Radio, TV, newspapers and telephone facilities, both landline and mobile, combine to cover all areas. During the 2011 floods, radio broadcasters and others used social network sites to access and disseminate information. In some countries, such as Samoa, Papua New Guinea and Tonga, emergency broadcasters are experimenting with sending out SMS messages to mobile phone owners; however, there remain a few difficulties given the limited number of messages that can be sent at one time (200 in Tonga). There were also reports in Papua New Guinea that early warnings were sometimes confused with spam messages and people failed to take any action when receiving SMS warnings.

## Conclusion: Locating disaster communication in local communicative ecologies

Locating disaster management plans within the local communicative ecology does not privilege high-tech over low-tech or vice versa. For example, Samoa has one of the strongest disaster preparedness policies and coordinating bodies in the region, and its disaster plans interweave older communication practices with new approaches and technologies. The early warning system includes a network of sirens in town areas and a refinement of an SMS system, together with networks of village bells, where successive villages ring their bells to warn the next village, who passes the warning on by ringing their bells. In addition to technical solutions, Samoans utilise traditional knowledge of signs of changing weather patterns (Lefale 2009). In many cases villages go through a separate additional process of identifying the risks and developing plans which supplement the national disaster plans and preparations.

Importantly, face-to-face communication remains the most effective warning system and has been acknowledged and incorporated into disaster planning. Often police are the primary communicators and they are often provided satellite phones and radios so they can access the most up-to-date information. For example, in Kiribati the police drive around all of the islands (including outer islands) to inform people about impending emergencies, and in Niue police make a point of meeting with the village councils who, in turn, go around the village to inform people of the alert and advise them to listen to the radio. They also check to make sure people

have hot water and an emergency kit, and remind them to close their shutters. In the Solomon Islands the police circulate warnings. In other places church bells or conch shells are used. While radio and television are the primary emergency systems in Palau, in the past the governor has also phoned households via landlines and sent people to relay the message to every household. A number of countries continue experimenting with ways to combine face-to-face meetings with mediated forms of awareness information strategies.

An area often neglected in disaster management and climate change communication is language. The use of highly technical terms without translating them into local languages can cause confusion. Information fatigue was observed in some countries like Kiribati and Palau and at least some of this can be attributed to the challenges of translating issues of climate change and disaster planning into locally relevant stories.

Geography remains a key challenge for technicians and others involved in the design and implementation of successful emergency broadcast systems. The vast majority of island nations in the region are geographically dispersed and separated by water or dense forest and vegetation. For example, the government in the Federated States of Micronesia recently purchased a siren warning that is activated by a text message (SMS). Currently the system is only operational in Pohnpei, but they envision that this system will eventually be quite useful for the atoll islands where the siren will be heard across the community; in the past vast distances have hindered effective early warning systems.

In countries such as the Cook Islands, radio and satellite phones are key technologies for reaching the populations in the outer islands. For example, every island has a satellite phone to be used in emergencies and telecommunications companies prepare their staff with High Frequency radios and satellite phones. However, radio alone continues to have shortcomings. In the Cook Islands the radio station that reaches the outer islands transmits on a limited basis and does not broadcast 24/7. Similar coverage gaps can be observed in Palau, the Marshall Islands and the Solomon Islands.

It is important to integrate mobile phones and other ICTs into disaster plans and policies across the Pacific in order to remain relevant in the dynamic and shifting communication environments. To be effective, however, these technologies need to be understood in local contexts. Communicative ecologies provides a useful conceptual framework for this, and, as this paper demonstrates, can help to identify important nuances in affordability, access, trustworthiness, generational and gendered differences, geography, and the influences of cultural and meaning structures and local knowledge in preparing and responding to disasters.

## Acknowledgements

This paper draws from the 'PACMAS: State of the Media and Communication Report'. We therefore wish to acknowledge ABC International Development, who funded the study, and our co-authors, Verena Thomas and Joys Eggins. We thank Vipul Khosla, Research Manager ABC ID, who commented on a draft of this paper.

## References

- Andersen, B. 2013. 'Tricks, Lies, and Mobile Phones: "Phone Friend" Stories in Papua New Guinea' *Culture, Theory and Critique* 54:3, 318-334
- Bengtsson, L; Lu, X; Thorson, A; Garfield, R; Von Schreeb, J. 2011. Improved response to disasters and outbreaks by tracking population movements with mobile phone network data: a post-earthquake geospatial study in Haiti. *PLoS medicine*, 8(8), e1001083.
- Cave, D. 2012. Digital Islands; How the Pacific's ICT Revolution is transforming the region. Accessed January 23, 2014. Available at: [http://www.lowyinstitute.org/files/cave\\_digital\\_islands\\_web.pdf](http://www.lowyinstitute.org/files/cave_digital_islands_web.pdf).
- Donner, J. 2010. 'Framing M4D: The Utility of Continuity and the Dual Heritage of" Mobiles and Development"' *The Electronic Journal on Information Systems in Developing Countries* Vol. 44 (3), pp. 1-16
- Donner, J. 2008. Research Approaches to Mobile Use in the Developing World: A Review of the Literature. *The Information Society* 24(3), 140-159. See: <http://www.tandfonline.com/doi/abs/10.1080/01972240802019970#.VI6eXHtvDXs>
- Duffield, Lee; Watson, Amanda H.A.; Hayes, Mark. 2008. "Media and Communication Capacities in the Pacific region" *ejournalist* Vol 8. (1) p 20-34.
- Farbotko, C; Lazrus, H. 2011. The first climate refugees? Contesting global narratives of climate change in Tuvalu. *Global Environmental Change*, 22(2), pp.382–390.
- Handman, C. 2013. 'Text Messaging in Tok Pisin: Etymologies and Orthographies in Cosmopolitan Papua New Guinea' *Culture, Theory and Critique* 54:3, 265-284
- Heinzelman, J; Waters. C. 2010. *Crowdsourcing crisis information in disaster-affected Haiti*. US Institute of Peace.
- Horst, H. A. 2013. 'The Infrastructures of Mobile Media: Towards a Future Research Agenda' in *Mobile Media and Communication* 1(1). 147-52.
- Horst, H. A; Taylor, E. B. 2014. 'The role of mobile phones in the mediation of border crossings: A study of Haiti and the Dominican Republic'. *The Australian Journal of Anthropology*, 25: 155–170.
- Horst, H; Miller, D. 2006. *The Cell Phone: An Anthropology of Communication*. Oxford: Berg.
- Intermedia Europe. 2012. "Citizens Access to Information in Papua New Guinea", ABC International Development. Available at: <http://www.abcinternationaldevelopment.net.au/wp-content/uploads/2012/09/ABC-PNG-Report.pdf>.

- Jensen, R. 2007. The digital provide: Information (technology), market performance, and welfare in the South Indian fisheries sector. *The quarterly journal of economics*, 879-924
- Lefale, P.F. 2009. Ua 'afa le Aso Stormy weather today: traditional ecological knowledge of weather and climate. The Samoa experience. *Climatic Change*, 100(2), pp.317–335. Available at: <http://www.springerlink.com/index/10.1007/s10584-009-9722-z>.
- Ling, R; Horst, H.A. 2011. 'Mobile communication in the global south' *New Media & Society* 13 363-374
- Lipset, D. 2013. 'Mobail: Moral Ambivalence and the Domestication of Mobile Telephones in Peri-Urban Papua New Guinea'. *Culture, Theory and Critique* 54:3, 335-354
- Mas, I; Morawczynski, O. 2009. 'Designing mobile money services lessons from M-PESA.' *Innovations* 4.2, 77-91.
- Muliaumaseali'I, M. 2014. "#didntfeelathing: Mobile phones and tsunami warnings in Samoa". Accessed from: <https://sites.google.com/site/mobilisingmediainthepacific/research-from-the-field/mobilephonesinsamoa>
- Paton, K; Fairbaine-Dunlop, P. 2010. "Listening to local voices: Tuvaluans respond to climate change" in *Local Environment: The International Journal of Justice and Sustainability* Vol 15 (7) pp 687-698.
- Pertierra, R; Ugarte, E.F; Pingol, A; Hernandez, J; Lexis Dacanay, N. 2002. *Texting selves: Cellphones and Philippine modernity*. Manila, Philippines: De La Salle University Press.
- Reading, A. 2009. 'Mobile witnessing: Ethics and the camera phone in the "War on Terror"'. *Globalizations* 6.1 : 61-76.
- Rika, N. 2013. "Climate Change is a justice issue for Pacific people'. Pacific Islands News Association. Available at: <http://www.pina.com.fj/?p=pacnews&m=read&o=812058780527b13b72dcec48e18d0c>
- Roche, S; Propeck-Zimmermann, E; Mericskay, B. 2013. 'GeoWeb and crisis management: issues and perspectives of volunteered geographic information.' *GeoJournal* 78:1, 21-40.
- Sey, A. 2011. 'We use it different, different': Making sense of trends in mobile phone use in Ghana' *New Media & Society* 13 375-390
- Slater, Don. 2013. *New Media, Development and Globalization: Making Connections in the Global South*. John Wiley & Sons.
- de Souza e Silva, A; Sutko, D.M; Salis, F.A; de Souza e Silva, C. 2011. 'Mobile phone appropriation in the favelas of Rio de Janeiro, Brazil' *New Media & Society*;13 411-426
- Tacchi, Jo. (2014) 'Being Meaningfully Mobile: mobile phones and development' In Servaes, J. (Ed.) *Technological determinism and Communication for Sustainable Social Change*. Lexington Books.
- Tacchi, Jo; Kitner, Kathi. R; Crawford, Kate. 2012. Meaningful Mobility: Gender, development and mobile phones. *Feminist Media Studies*, 12(4), 528-537.
- Tacchi, Jo; Horst, Heather; Papoutsaki, Evangelia; Thomas, Verena; Eggins, Joys. 2013. "PACMAS: State of the Media and Communication Report", Melbourne: PACMAS/ABC International Development. Available at: <http://www.pacmas.org/profile/pacmas-state-of-media-and-communication-report-2013>
- Tenhunen, Sirpa. 2008. Mobile technology in the village: ICTs, culture, and social logistics in India. *The Journal of the Royal Anthropological Institute*, 14(3), 515-534.

- Wallis, C. 2013. *Technomobility in China: Young Migrant Women and Mobile Phones*. NYU Press.
- Wallis, C. 2011. 'Mobile phones without guarantees: The promises of technology and the contingencies of culture'. *New Media & Society* 13. 471-485
- Watson, A. 2011. *The mobile phone: the new communication drum of Papua New Guinea*. PhD thesis, Queensland University of Technology Available at: [http://eprints.qut.edu.au/view/person/Watson,\\_Amanda.html](http://eprints.qut.edu.au/view/person/Watson,_Amanda.html)

---

<sup>1</sup> The Pacific Media Assistance Scheme (PACMAS) is an Australian Aid funded regional media program to support better governance in the Pacific through the development of a diverse, independent and professional media, promoting informed and meaningful public discourse region-wide. The program is managed by the Australian Broadcasting Corporation (ABC) and is based in Vanuatu.

<sup>2</sup> Tables are arranged by region (Melanesia, Polynesia and Micronesia) for the sake of clarity and readability.

<sup>3</sup> perceptions of research participants; statistics on use unavailable.

# Updating warning systems for climate hazards: Can navigation satellites help?

---

**John Handmer**

Centre for Risk & Community Safety, RMIT, Melbourne

**Suelynn Choy**

Centre for Risk & Community Safety, RMIT, Melbourne

**Naohiko Kohtake**

Keio University, Tokyo

---

**Summary:** Warning systems are relied on worldwide as part of disaster risk reduction.

The traditional model of a government monopolistic system supplying warnings through a broadcast approach is now challenged by new media, mobile technologies and the accompanying expectations of individualised warnings to personal mobile devices. We examine this situation, and one novel approach – the use of an augmented signal from the next generation of Japanese positioning satellites - to providing individual warnings to personal devices wherever their owners are. We conclude that delivery to personal devices is feasible and already happening to some extent. Linking these new official systems with the multiple information flows of social media and crowdsourcing remains a major challenge.

## Introduction

Warning systems are increasingly relied on to reduce the risk of disaster by empowering people to improve their safety. These systems typically require the integration of a top-down official alert, with a bottom-up understanding of that alert and their personal risk related circumstances by those receiving the warning. However, the interaction between the official and the people is problematic with the consequence that safety is often not improved: official systems have many technical and other limitations, and those at risk often fail to see the relevance of official communications. These systems are based on a linear flow of information along a complex chain of authority to those thought to be at risk. But the warning paradigm is changing rapidly. Social media and mobile technologies enable communities to generate and share their own warnings and information, which are often more up-to-date and sensitive to local circumstances than official communications. Increasingly, they can also provide information to the official system – some Australian fire

and emergency management services monitor twitter for this purpose. Despite concerns about the legitimacy and accuracy of such information, these 'backchannel' communications are becoming increasingly prevalent during emergencies. This important aspect of the warning process is entirely dependent on the normal functioning of telecommunication infrastructure. At the same time there is anecdotal evidence from fire and emergency management agencies that public expectations, fueled by the near universality of personal mobile devices and social media, have risen to the extent that people increasingly expect a personal warning wherever they are.

A major challenge is to have the official warning system, with its environmental monitoring and predictive capacity, interact positively with the social media and personal devices used by most people. If this is achieved, the reliability of the overall warning system could be enhanced. One promising approach is based on joining the potential of mobile devices with next generation satellite-based navigation systems, such as the system being established by Japan. Such satellite systems also have the potential to provide redundancy and surge capacity for conventional terrestrial based communication arrangements.

In this paper we summarise what warning systems for natural hazards are, how they are designed and what they are intended to achieve – and some of the difficulties in achieving success. We also examine the impact of new technology and social media, and set out an example of an emerging technology and its potential to address some of the long standing issues with warning systems, and the remaining challenges.

## Warning systems

Ideally, warnings provide a signal to that those at risk from disasters so they can take action to improve their safety and reduce losses. "Losses" refer to tangible assets typically valued in money terms such as buildings, livestock, and telecommunications facilities; and to consequential or indirect losses as a result of disruption to commerce, government and people's lives ([BTE 2001](#)). Losses can also be intangible such as lives, psychological trauma and ecosystem services. Warnings are produced by a mix of technology and human and organisational factors, with many decision-nodes and points of potential failure ([Handmer 2000](#)). As a result, many warning systems fail to provide signals in time or in a form that is useful to those at risk. Even when timely signals are provided, people and organisations often do not take the actions necessary to protect their safety and livelihoods.

Warnings systems need to take account of the day-to-day pressures, beliefs and expectations of the people intended to take action on receipt of a warning. This means that systems need to use media familiar to the intended audience(s) and design messages that have meaning to them ([Australian Government 2008](#)). The audiences or groups at risk are many and varied,

such as businesses, tourists, elderly, schools, those in transit. Contemporary best practice in risk communication is that warning design should be based on local needs and expectations, and have meaning for those at risk: there needs to be a shared understanding between those issuing the warning and those receiving it ([EMA 2009](#); [UN-ISDR 2006](#)).

For this to happen, there needs to be mutual learning between those with formal responsibility for the warnings and those at risk. The important implication here is that those at risk need to be involved with warning system design and operation. Warnings need to be delivered by a variety of modes appropriate for the audience in a timely manner so as to allow for people to confirm what they have to do and to take action in time. Warnings need to make sure people know what they can do to improve their safety and reduce losses.

Warnings issued through official channels are almost always complemented by unofficial or informal messages – unless the official warnings are seen as irrelevant ([Parker & Handmer 1998](#)). These are messages sent and received through personal networks both to warn and to confirm official warnings and other signs, such as environmental cues, of an impending emergency. These informal networks are often key to the rapid spread of warnings and to people's ability to obtain credible confirmation of the warning. In addition, very often, informal channels are the only way people receive warnings, because they deliver messages directly to people via media and in language that they understand.

## Warning system design

In Australia the essence of what can be viewed as the traditional approach to warning system design is captured in the *Guide for Flood Warnings* ([EMA 2009](#)). Although the guide is at pains to point out that warnings must be based on local knowledge and that knowledge of local circumstances is key to success, warning systems are shown as a more or less linear chain or process that includes multiple organisations only some of which are under the control of government ([Handmer 2009](#)):

- ***Prediction:*** detecting environmental conditions that lead to the problem, and predicting its severity;
- ***Interpretation:*** identifying in advance the impacts of the predicted event on communities at risk;
- ***Message construction:*** devising the content of the message which will warn people of the impending event;
- ***Communication:*** disseminating accurate warning information in a timely fashion to people and organisations likely to be affected by the event;

- *Protective behaviour*: generating appropriate and timely actions from the threatened community and from the agencies involved; and
- *Review*: examining the various aspects of the system with a view to improving its performance.’

This approach can work very well and is key in many economic sectors including transport, energy supply, offshore oil rigs, etc. However, it is a supply rather than demand approach: people are given information often in a form that means little to them, and without the ability to interact with the information, for example to establish exactly what the implications are for them and their households. This has generally been the case even though the warnings should be based on an assessment of local risks and vulnerabilities. In the time pressured situation of an impending emergency, this approach assumes that the official warning agency has a monopoly on relevant information.

Overlying the system elements are some basic design principles for warnings. These are not always explicit, but are important in how warning systems actually work to improve safety and reduce loss. The principles include compatibility with the existing telecommunications networks targeted at those at risk, underpinned by education and awareness raising activities. Note that in practice additional principles are used, for example the need to ensure that warnings do not exclude classes of people.

For the list of national design principles see:

<https://www.em.gov.au/Emergency-Warnings/Pages/Emergencywarningsguidelinesandprinciples.aspx>

## Issues and difficulties

After major emergencies and disasters, questions are typically raised about the inadequacy of warnings, and there have recently been some high profile failures of warning systems, and cases where the public expected warnings but there were none – e.g. Hurricane Katrina and New Orleans ([Handmer 2006](#)). Part of the difficulty is that a warning that reaches most people but fails to reach the most vulnerable groups or facilities will likely not be seen as a success. Even if it reaches everyone, it will fail if people do not see it as relevant to them or do not know what to do.

This highlights that the real purpose of public warnings is to empower people to make decisions to improve their safety and reduce losses. Warning system designers often ignore this crucial step, and are satisfied when their systems deliver timely alerts, even if these do not result in improved safety. To counter this, we should ask **why agencies should be held responsible for people’s behaviour when the agency has delivered sound advice?** In some

cases warnings appear to encourage people to take high risk action: a tsunami warning in Queensland prompted many to travel to the coast to witness the arrival of the wave; and flood warnings for the NSW town of Grafton saw many having picnics on the town's levee, which was predicted to overtop (Pfister 2002).

Warnings need to satisfy a range of technical and relatively objective criteria such as accuracy, relevance and timeliness – there is little point receiving warnings after the event. Assuming these conditions are satisfied, the source needs to be seen as credible, and usually official sources in Australia are viewed as credible. Also, the medium and message need to be seen as personally relevant by those at risk. It is important to appreciate that what constitutes a personally relevant message is changing as people's expectations of more specific personalised warning messages are probably increasing. The traditional approach has on occasion managed to do this when the number at risk was small enough to allow each household to be telephoned or doorknocked, but even this level of service has depended on people being at home or a fixed place of work. The UN's Platform for Early Warning (UN-ISDR 2006) uses the term "people centred warnings" to emphasise that effective warnings need to keep their ultimate purpose in mind and be focused on the needs and expectations of those at risk.

Typically enormous effort has been put into environmental monitoring and detection, with limited effort on achieving shared meaning and sound decision-making with those at risk.

## New communication technologies

New media and mobile technology could bring individual warnings to everyone, anywhere, anytime, but this has yet to occur. New media's attention to peer to peer communication flows and its capacity, through for example crowdsourcing, to provide real time information on unfolding emergencies, does not fit well with the traditional monopolistic supplier model. However, it does fit with, and potentially greatly enhances, informal warning networks and systems at every stage of the warning chain.

The near universality of new media and mobile phones, may also be driving expectations among those at risk that they are entitled to expect a personalised warning delivered to their personal mobile device. This would have seemed inconceivable a few years ago, but is starting to become a reality through the Australian Emergency Alert system, and to some extent through a range of twitter and Internet feeds that people can elect to receive on their personal devices.

The Emergency Alert (EA) system is the only official approach currently in use that offers an intrusive warning message to personal devices – whether people have elected to receive it or not. In serious emergencies, warnings are issued via Short Message Service (SMS) text

messages to mobile phones and voice messages to landlines within a threatened area, however delivery cannot be guaranteed if telecommunications networks are compromised during an event ([Australian Government 2009](#)). An informal review of EA found the system was regarded as a convenient, trusted and compelling trigger for action, though possible improvements were identified in relation to the timing, content, accuracy and applicability of messages. While EA has been relatively successful since its nation-wide operational implementation in 2009 ([Handmer & Ratajczak-Juszko 2011](#)), drawbacks within the system have been identified in addition to its reliance on the normal phone system. In some cases, messages are delayed and the information conveyed may be inaccurate.

All web based and phone systems are subject to failure through overloading or power failures, or, and importantly during an emergency, as a result of damage to key facilities. Phone systems have very little if any extra capacity in the name of commercial efficiency. This may make sense for business when blame for failures in such systems can be shifted to governments, but undermines the capacity and reliability of these systems in an emergency. There are also privacy issues with the use of mobile phones for warnings. The launch of the Emergency Alert system in 2009 required a legislative amendment to override privacy provisions governing the use of the national telephone number database (see the Emergency Alert webpage). However, this seems overplayed given that in Australia commercial establishments have access to listed numbers, and charities have access to all numbers including those that are unlisted.

Advantages include the ability of mobiles and the phone network to function during power failures albeit for a limited time. If using the mobile network, warnings can reach people where ever there is phone coverage as most people keep their phones with them. Messages can be closely targeted, for example they can be pre-recorded in different languages and be location based. Text messages do not require people to answer the phone.

New media and mobile technology offers solutions to some of the long standing limitations with warning systems, in particular with personal messages delivered to individuals, and the ability to share information from those at risk using it to improve warnings in real time (for example see [Chatfield & Brajawidagda 2013](#)). Crowdsourced information from twitter is being increasingly drawn on to help provide early warnings in a variety of fields including earthquakes by the United States Geological Survey ([Koebler 2013](#)), and by agencies monitoring emerging epidemics.

## The potential of satellite positioning systems for warnings

Global Satellite Navigation Systems (GNSS) have long been recognised as an effective and invaluable technology for providing accurate position information anywhere, anytime on a global scale. These systems include the GPS system of the USA, Russia's GLONASS and

several other new and emerging constellations such as Europe's Galileo and China's BeiDou systems. There are also regional satellite navigation systems that will become operational in the next few years, particularly from Japan and India.

The new Japanese satellite-based navigation system (Quasi-Zenith Satellite System or QZSS), may play a role in addressing some of the issues raised above with conventional warning systems, as well as providing one approach to meeting contemporary expectations of personal warnings. The uniqueness of this system is that it serves not only as a backup providing redundancy to ground-based telecommunications but also as an extension of an effective emergency response solution. That is, the satellite system has the capacity to deliver alert messages as well as evacuation direction (location-based information) to specific groups and areas, unconstrained by the present limitation of ground-based telecommunications. The QZSS alert message system has been developed and successfully tested in Japan through the Red Rescue Project (see below). In mid 2014, the Japanese and Australian leadership formally agreed to cooperate to promote utilisation of QZSS for emergency management, among other uses. The Japanese satellite consortium has also begun discussion with the European Union, in particular the European Space Agency, to identify needs within the Asian and European countries so that satellite based emergency warning services, standardised across different satellite navigation systems, can be developed to serve Europe and Asia, including Australia.

Europe has been working on emergency message services since 2005 using the European Geostationary Navigation Overlay Service (EGNOS) and European Union's Galileo satellite navigation system with the introduction of the ALIVE (Alert interface via EGNOS) Concept ([Mathur et al. 2005](#)). Since then there were follow on projects investigating technical and non-technical benefits as well as advantages of utilising GNSS satellites for disaster alerting ([Dixon & Haas 2008](#); [Wallner 2011](#); [Domínguez et al. 2013](#)). In Japan, investigation to transmit information using the QZSS L1-SAIF signal is currently underway ([Iwaizumi & Kohtake 2013](#); [Sakai & Hiroe 2012](#)). All these systems include information on the location (i.e., latitude and longitude) of the emergency area and a predefined identifier describes the disaster type.

## The Japanese Regional Navigation Satellite Systems

QZSS is a Japanese regional satellite based augmentation system aimed at enhancing the capabilities of current GNSS systems. When fully deployed in 2018, it will consist of three QZSS satellites placed in Highly Inclined Elliptical Orbits (HEO) and one geostationary satellite. The orbit configuration of these QZSS satellites provides continuous coverage at a high elevation angle, providing improved satellite navigation in areas of Japan that challenge

traditional GNSS satellite positioning capabilities, such as central city areas. While intended primarily for users in Japan, the orbit design offers significant advantages to neighbouring East Asia countries and Australia. Figure 1 shows the footprint of QZSS satellite. The first QZSS satellite was launched on 11 September 2010.

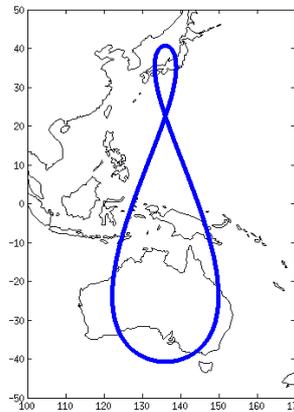


Figure 1: Ground track of QZS-1 orbit.

## A Unique Signal

One unique feature of QZSS is that in addition to the standard GNSS navigation signals, QZSS also has the capability of sending short emergency messages, which none of the current GNSS satellite systems are able to transmit. The messages can be received directly from the satellite by a GPS/GNSS receiver terminal such as in a mobile phone or in-car navigation system. An app would interpret and display the information. Given that mobile phone use and in-car navigation systems are becoming universal with almost everyone involved, the potential coverage and reach of warnings sent to these personal devices is likely to be much greater than the current approaches could achieve.

Another feature of the QZSS provision for alert messaging is that in addition to the wide area coverage provided by the satellite system, the receiver also provides, through their embedded GNSS/GPS capabilities, precise position information. In this way, alert messages can be sent to a specific area depending on the type and content of the disaster information, and only those receivers within the specific area will be activated. Knowing the area of the possible disaster location, the intended users could then be warned, while those outside the disaster area would not be alerted.

The satellite based system offers a number of advantages for real-time disaster alerts over current approaches to sending warnings via personal devices. A disadvantage is that at present the signal is not generally received indoors. Advantages include:

- 1) GPS/GNSS with location information can be used during an emergency. This provides the ability to indicate high priority messages for specific areas and groups;
- 2) The service can cover a wide area simultaneously – e.g. the whole of Australia – because of its wide area broadcast footprint, and within the broadcast area, there is no limit to the number of people who can be warned simultaneously;
- 3) The messages can still be received even when terrestrial communications infrastructure is damaged or not available. This allows for redundancy;
- 4) As the system is independent of mobile phone coverage it would reach people wherever they are, regardless of the existence of mobile phone coverage.

## Red Rescue test project

The Red Rescue Project (for real-time disaster response using small-capacity data packets from the ubiquitous environment) is supported by the Japanese Government. The project commenced in 2009 as a three-year project and has run trials in Japan and Thailand for tsunami warnings. The project leader is NTT DATA Corporation (a Japanese system integration and data company) and the other project members are Keio University, Asia Air Survey, and Pasco. The authors are collaborating with the Japanese consortium to run a trial in Australia.

The **message system**: The emergency message is sent to the user from the QZSS satellite using the L1-SAIF (Submetre-class Augmentation with Integrity Function) signal. This signal is broadcasted on the L1 frequency band (1575.42 MHz). The advantage of the L1 signal is that it is the most widely used signal by the mass-market GNSS/GPS receivers. All, if not most, GNSS/GPS receivers are able to track and acquire this signal. At 212 bits, each emergency message is very short, but a number of messages can be combined to produce a longer message.

Fig. 2 shows a schematic diagram of the QZSS alert messaging transmission system. The system consists of three parts: the transmission, satellite and user segments.

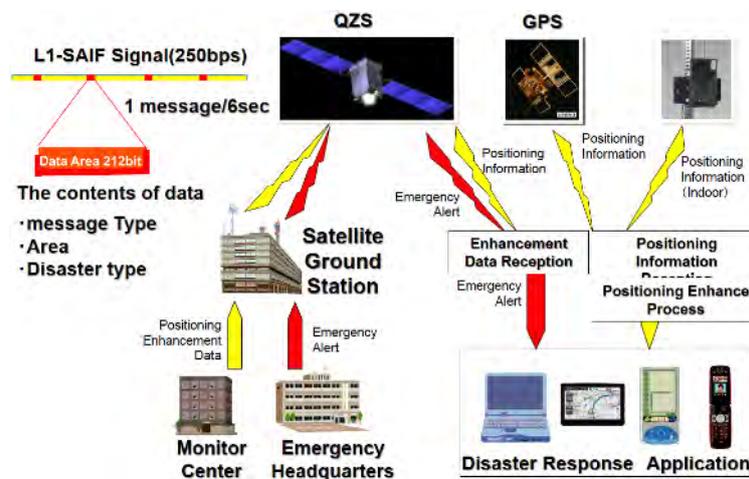


Figure 2. QZSS alert messaging transmission system.

The **Transmission Segment**. This segment consists of the Disaster Management Centre, the Monitor Centre, and the Satellite Ground Control Station.

The transmission segment transmits disaster messages to the satellite segment in the following order: First, the Disaster Management Centre gathers the relevant information. Second, the Disaster Management Centre converts the information into an emergency message for transmission by QZSS. The Disaster Management Centre decides the distribution schedule for providing the information and transmits the emergency message to the Satellite Ground Control Station. Third, the Ground Control Station collects the Monitor Centre's results and generates (enhanced) navigation messages for broadcast on the L1-SAIF signal, which will be used by the user to derive precise position information. The Ground Control Station uplinks both the navigation message and the emergency message to the QZSS satellites.

The **Satellite Segment**. The satellite segment consists of both the QZSS and other GNSS satellites like GPS. The L1-SAIF signal with the enhanced navigation message and the superimposed emergency message are transmitted to the users.

The **User Segment**. The users receive the L1-SAIF signal and position information from QZSS as well as position information from other GNSS satellites on their GNSS receivers. The enhanced navigation message is used to provide accurate position of the users. The L1-SAIF signal contains the emergency message that is decoded by the users' device by an app in order to acquire the disaster information.

For the QZSS alert messaging system, two receiving modes are being developed: One is the wide-area broadcast mode, which can send emergency message simultaneously over a large area; the other is the area-selected broadcast mode, which can send messages to a specified

area ([Iwaizumi et al 2014](#)). The area-selected mode delivers several emergency messages to provide disaster information for all areas depending on the type and content of the disaster information. Therefore, the user segment of this system provides the disaster information to the users by selecting the information of the area corresponding to the location of the user from the received emergency messages ([Iwaizumi et al. 2014](#)).

## Conclusions

We identified a disjunction between the way warning systems are conventionally conceptualised, and the expectations of the public for personal warnings and the realities of contemporary information flows through social media and mobile technologies. To meet this need aspects of mobile technology are now being employed by Australian emergency services through the Emergency Alert system, which delivers a standard text message warning or alert to mobile phones. However, the monopolistic supplier model is not intended to absorb the real time information available via crowd sourcing. In addition, mobile phones and the mobile phone network have many limitations. Nevertheless, some agencies in Australia and elsewhere are starting to incorporate crowd sourced information, in particular from twitter, into their monitoring and warning systems.

The Japanese satellite system is also a supply driven approach, although it would deliver messages to people's personal devices which could be tailored to their circumstances via apps. It has the potential therefore to address one of the shortcomings of the traditional model. It is not likely to become a replacement for existing systems, but it can augment and strengthen them by providing an independent way of sending warnings. This developing system has the capacity to transmit messages to mobile phones and in-car navigation units for disaster warning and response via the GNSS location capacity now part of all smart phones, rather than through the phone networks. This approach appears to offer significant advantages over current systems: it is not reliant on ground based telecommunications infrastructure and can provide warnings anywhere to anyone in a defined location. It could also provide a backup system when local communications infrastructure fails. It is not affected by telecommunication traffic congestion and can warn millions of people simultaneously, providing both a way to distribute urgent messages as well as surge capacity for wide-area warnings.

An Australian trial of the QZSS satellite warning system is planned for 2015. A major challenge is how this system and other existing systems can take advantage of crowd sourced information, and the informal networks facilitated by social media.

## Acknowledgements

We thank the RMIT University Science, Engineering and Health College Research & Innovation Office, the Bushfire and Natural Hazards Cooperative Research Centre (BNHCRC) and the RMIT School of Mathematical and Geospatial Sciences for providing funding for the project, “Next Generation Warning Systems”, which this paper draws from. We also acknowledge our collaborators on the project: Dr Joshua Whittaker and Dr Marc Demange of RMIT and Dr Michael Rumzewicz of the BNHCRC.

## References

- Australian Government. 2009. News Release. ‘Rudd Government Implements COAG Agreement on Telephone-Based Emergency Warning Systems,’ 23 February 2009, Canberra. Available at: <http://www.royalcommission.vic.gov.au/Documents/Document-files/Exhibits/WIT-032-001-0261.pdf>
- BTE. 2001. Bureau of Transport Economics, *The Economic Costs of Natural Disasters in Australia*. Canberra.
- Chatfield, AT; Brajawidagda, U. 2013. Twitter Early Tsunami Warning System: A Case Study in Indonesia’s Natural Disaster Management, *System Sciences (HICSS), 2013 46 Hawaii International Conference*, DOI: 10.1109/HICSS.2013.579.
- Dixon, CS; Haas, R. 2008. GNSS User Requirements in Emergency Management, RIV NAV’o8 Conference, London, UK.
- Domínguez, E; Simón, FJ; Thomas, P; Zheng, Y; Wittmann, E; Lekaim, D; Tossaint, M; Jeannot, M. 2013. ESA’s Multi-Constellation Regional System Land Users Test-Bed Integrity Algorithms Experimentation Results, to be presented at the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2013), Nashville, TN, September 2013
- EMA. 2009. Emergency Management Australia. *Flood warning: an Australian guide (3<sup>rd</sup> Edition)*, Emergency Management Australia, Canberra. Emergency Alert. Available at: <http://www.emergencyalert.gov.au/frequently-asked-questions/who-can-use-it.html>. For the actual amendment see: [http://www.austlii.edu.au/au/legis/cth/num\\_act/tapnda2009556/sch1.html](http://www.austlii.edu.au/au/legis/cth/num_act/tapnda2009556/sch1.html). Page accessed 12 November 2014.
- Handmer, J. 2000. Are flood warnings futile? *The Australasian Journal of Disaster and Trauma Studies*. Available at: <http://www.massey.ac.nz/~trauma/issues/2000-2/> (2000-2) ISSN: 1174-4707.

- Handmer, J. 2006. American exceptionalism or universal lesson: the implications of Hurricane Katrina for Australia, *Australian Journal of Emergency Management*. 21(1) Feb 2006, 29-42.
- Handmer, J. 2009. *Warnings and information*, Prepared for the 2009 Victorian Bushfires Royal Commission, Centre for Risk and Community Safety, RMIT University. May 2009. Witness Statement – 044-001-0002-R.
- Handmer, J; Ratajczak-Juszko, I. 2011, *Systematic Review of Reports on Emergency Alert*, Report prepared for the Office of the Emergency Services Commissioner by the Centre for Risk and Community Safety, RMIT University, Melbourne
- Iwaizumi, D; Ishida, T; Iino, S; Kohtake, N; Buist, P. 2014 GNSS-based Emergency Message Service: Lesson Learned and Future Prospects, 7<sup>th</sup> Advanced Satellite Multimedia Systems Conference, 13<sup>th</sup> Signal Processing for Space Communications Workshop, 8 - 10 September 2014.
- Iwaizumi, D; Kohtake, N. 2013. Evaluation of reachability and promptness in delivering disaster and evacuation information using an augmentation signal of the QZSS system, 64<sup>th</sup> IAC, Beijing, China, 2013.
- Koebler, J. 2013. The USGS is tracking earthquakes with Twitter, *Motherboard*. Available at: <http://motherboard.vice.com/blog/the-usgs-is-tracking-earthquakes-with-twitter>. Accessed 20 November 2014.
- Mathur, AR; Ventura Traveset, J; Montefusco, C; Toran, F; Plag, HP; Ruiz, L; Levy, J. 2005. Provision of emergency communication messages through SBAS: The ESA ALIVE concept, ION GNSS 2005, Long Beach, US.
- Parker, DJ; Handmer, J. 1998. The role of unofficial flood warning systems, *Journal of Contingencies and Crisis Management*, 6(1), 45-60.
- Pfister, N. 2002. Community response to flood warnings: the case of an evacuation from Grafton, *Australian Journal of Emergency Management*, Vol 17, No 2. Available at: <https://ajem.infoservices.com.au/items/AJEM-25-02-09#sthash.mNiBnC1c.dpuf>
- Sakai, T; Hiroe, N. 2012. Broadcasting Nationwide Emergency Message by QZSS L1-SAIF Signal, presented at the Proceedings of the 2012 IEICE General Conference, 2012.
- UN-ISDR. 2006. *Developing Early warning Systems: a checklist*. Available at: <http://www.unisdr.org/2006/ppew/info-resources/ewc3/checklist/English.pdf>

Wallner, S. 2011. Status of Definition of Dissemination of Emergency Alerts through GNSS, presented at the Sixth Meeting of the International Committee on Global Navigation Satellite Systems (ICG), Working Group B: Enhancement of performance of GNSS services, organized by the Government of Japan, Tokyo, Japan, 5 - 9 September 2011

# Acoustic Coupled Disaster & Remote Communications Systems

**Ulf Müller-Baumgart**

Serval Project Inc.

**Paul Gardner-Stephen,**

Flinders University

**Andrew Bettison,**

Flinders University

**Romana Challans**

Flinders University

**Jeremy Lakeman**

Flinders University

**Summary:** Following disasters, and in other infrastructure-deprived settings, such as remote areas, the need for communications is profound. However, the ability to provide communications solutions in such situations is extremely difficult because of the lack of functional infrastructure, and the logistical difficulty or impossibility of bringing in additional hardware. Therefore it is important to create communications solutions that can operate using existing locally available hardware.

In this paper we describe one possible solution based on acoustic coupling of mobile telephones with existing two-way radios, such as are often carried in remote areas of Australia, and are fitted to many vehicles that are used in such areas.

We describe a number of related software systems and some simple experiments that demonstrate the feasibility of the general concept, before describing a possible integration of such technologies with the secure digital communications capabilities offered by the open-source Serval Mesh software.

We argue that such an integration is not only possible, but also has the potential to allow secure digital communications in a variety of scenarios, without the need for any new or additional hardware.

## Introduction

Disaster situations have many similar properties to peace-time communications in remote areas and developing countries. In each of these three contexts there is a profound need to

communicate in order to ensure the survival and well-being of people in the area, although the particular dangers and challenges vary.

For example, in a disaster zone there may be a need to communicate the need for assistance when all local communications infrastructure has failed. Similarly, in a remote area, such as the vast expanse of the Australian Outback, there may be a total lack of conventional communications infrastructure (Crouch & Davies 2013). Finally, in developing countries, there may be a mixture of functional, absent or simply unaffordable communications infrastructure ([Yang 2011](#); [Akbari et al 2004](#); [Patricelli et al 2008](#)).

In all three situations, there is desire to enable communications for a variety of purposes. Moreover, in each scenario there are situations where secure communications are required. In a disaster zone this may be to protect the privacy of individual health records, or to enable humanitarian responders to organise without interference from local militia or other parties. The need for privacy also exists in remote areas, including the need to satisfy privacy legislation for medical, economic or other forms of communications. In Australia privacy requirements under law derive primarily from the *Privacy Act* (Commonwealth) of 1988 (as amended). In international jurisdictions there often exist instruments that similarly impose privacy regulations, although the specifics vary considerably. Finally, in developing countries all of these issues may be present, and in particular, individuals may wish to transfer funds using mobile payment platforms without the opportunity for middle-men to intercept and steal payment codes ([Morawczynski & Miscione 2008](#); [Luo et al 2010](#)).

The challenges to communications in such situations exist in combination with the need for secure communications in these environments. The lack of available, functional, affordable and secure communications infrastructure presents many obstacles.

The Serval Project ([Gardner-Stephen et al 2011](#); [2013a](#); [2013b](#); [2013c](#); [2014](#)) was created to address this challenge, by creating open-source software called the Serval Mesh that can be installed on existing Android smart-phones to allow them to easily carry and disseminate encrypted communications for their owners and for other parties. This application can also be shared from phone to phone, allowing it to be deployed during disasters, in remote areas or developing countries, without recourse to any communications infrastructure.

The primary limitation of the Serval Mesh software is that it is extremely difficult to establish long-range communications between mobile telephones without the use of cellular or Wi-Fi infrastructure. Some solutions are being developed to address this situation, such as the Serval Mesh Extender device ([Gardner-Stephen et al 2013b](#)). However, the need for additional hardware does not constitute a viable solution for situations where it is not possible to obtain the hardware in a timely manner, or where the cost would be prohibitive in relation to local

wages. Therefore there is a need for a solution that can use radio hardware that is already present.

In many of the target situations there will exist some local communications capability in the form of two-way radio, such as HF, VHF or UHF Citizen Band (CB) radio, or its local equivalent. Such systems typically have a range measured in kilometres to tens of kilometres, and thus represent an attractive resource.

From a technical perspective, the challenge is how to make use of an analogue radio system designed for voice communications to easily transfer digital information. At a minimum, it must be possible to automatically modulate and demodulate the communications, so that a human operator is not required to perform this function. That is, human interaction should be limited to, at most, activating the radio transmitter when required.

One approach that is possible and has been used since the 1960s or earlier to interface digital communications systems to analogue bearers is acoustic coupling. Acoustic coupling is simply the creation of a system where the digital system produces an analogue representation, i.e. modulation, of the digital communications and plays it as a sound, which is carried over the analogue bearer. The receiving end of the digital system then listens for such modulated transmission, and demodulates it to recover the digital message ([Serrano 1983](#); [Gutzmer 1992](#)). Such MODulator-DEModulator systems include the dial-up modems common during the early decades of the internet-era ([Serrano 1983](#); [Gutzmer 1992](#)). However, it is also possible to use a corresponding mechanism to use two-way radio systems to carry the modulated digital transmissions ([Sano 1994](#)).

There are numerous existing technologies for acoustic coupled communication in the amateur radio community. Data transmission is accomplished by using simple baseband modulation schemes in the audio frequency range (eg. AFSK), embodied in software that drives a sound card or speaker, such as the following examples. PSKmail ([PSKmail 2014](#)) is a widely known program to send digital encoded messages over the air. The AirChat program ([AirChat 2014](#)) by Anonymous uses a similar approach to transmit data. They have all in common the use of Fldigi ([Freese et al 2014](#)) as the underlying modulation software. Fldigi provides many more modulation schemes. It has the opportunity to be used as a basis for much more complex modulation systems.

Independent of any particular modulation scheme, our interest is in the ability of a common mobile telephone to perform the modulation and demodulation, using common two-way radio systems, such as the hand-held or vehicle-mounted VHF and UHF CB radio systems found throughout regional and remote Australia.

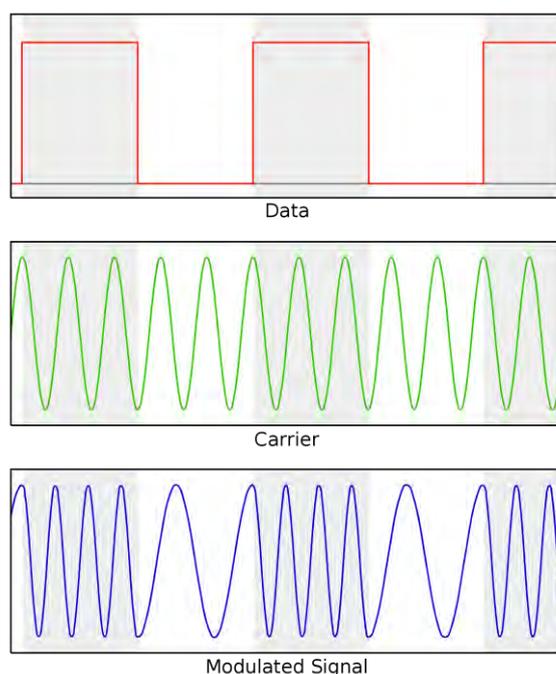
The remainder of this paper describes our current thinking on how this might be possible, what candidate radio systems and modulation schemes and software might be leveraged, how these can be integrated with the Serval Mesh, and what the properties of such a combined system might be. We conclude by outlining our plans to realise such a system.

## Introduction to Acoustic Coupling

In the process of acoustic coupling, modulation can be achieved by using common modulation schemes. Usually radio transmission involves modulating the carrier according to some scheme, e.g., frequency shift keying (FSK), where digital signals are represented by modulating different frequencies over the carrier ([Usselman 1949](#)). One of the more basic forms of this modulation scheme uses two frequencies to represent the different states of the digital stream. Usually the carrier frequency would be, for example, higher representing a 1 and a bit lower for a 0.

Audio Frequency Shift Keying (AFSK) is performed by generating an audio signal that encodes the digital information as a series of frequency shifts about a centre frequency ([Rappaport 1989](#); [Robertson & Wood 2005](#)).

For example, one might use a centre frequency of 1000 Hz, which might then be lowered to 800 Hz to represent a 0 and increased to 1200 Hz to represent a 1. In both cases the duration of the signal is not altered, only the modulation frequency. The centre frequency itself is never used. The resulting audio signal can be transmitted via a normal voice channel like a plain radio. A simple FSK scheme is illustrated in Figure 1.



**Figure 1 – Modulation by Frequency Shift Keying.** Binary digits or logic-levels are represented by different frequencies. In this example a binary 1, represented by high logic level is encoded at a higher frequency (grey background) than a binary 0, represented by a low logic level (white background) (Tims 2006).

As the voice channel bandwidth is usually limited from 300 Hz to 3400 Hz the usable bandwidth is very narrow (Gruen et al 1975, Jayapalan 1987). The modulation method needs to take account of this situation. The limited bandwidth of the channel places an upper bound on the amount of data that can be transmitted per unit time. While the theoretical limit of a simple modulation scheme is around 1.5KB/sec, the practical limit tends to be much lower due to a variety of factors (Sklar 2001). To extend the usable throughput, more complex modulation methods, e.g. PSK500 (PSKmail 2014), or QAM (PSKmail 2014) could be used.

## Proof-of-Concept Acoustic-Coupled Communications Systems

To establish the basic feasibility of the central premise of this paper, several simple tests were performed using either a smart-phone speaker to modulate or microphone to demodulate a digital transmission carried by radio.

The software used was PSKmail, which in turn uses fldigi as the underlying software to do the modulation. The modulation scheme is THOR22 (PSKMail 2014). It scheme modulates data at a rate several bytes per second by using a multi tone modulation comparable to MFSK (FSK with multiple frequencies).

In THOR22, the set of multiple frequencies (tones) change over time. This provides resistance to common error sources in radio transmission such as frequency shifts or offsets, e.g., by the Doppler effect or to multi-path propagation. The channel width is a mere 524 Hz, allowing its use on even quite poor radio transmissions paths. The software for THOR22 is available as open source, and therefore presents no licensing barriers to distribution and use.

A preliminary test was performed where the transmitter and receiver were acoustically coupled without a radio path, i.e., were placed next to each other. An Android mobile telephone was used to generate and play the audio-modulated data (Figure 2). This was received without error on another Android mobile telephone (Figure 3) and laptop computer (Figure 4). This confirmed that the modulation-demodulation components were correctly configured and working.

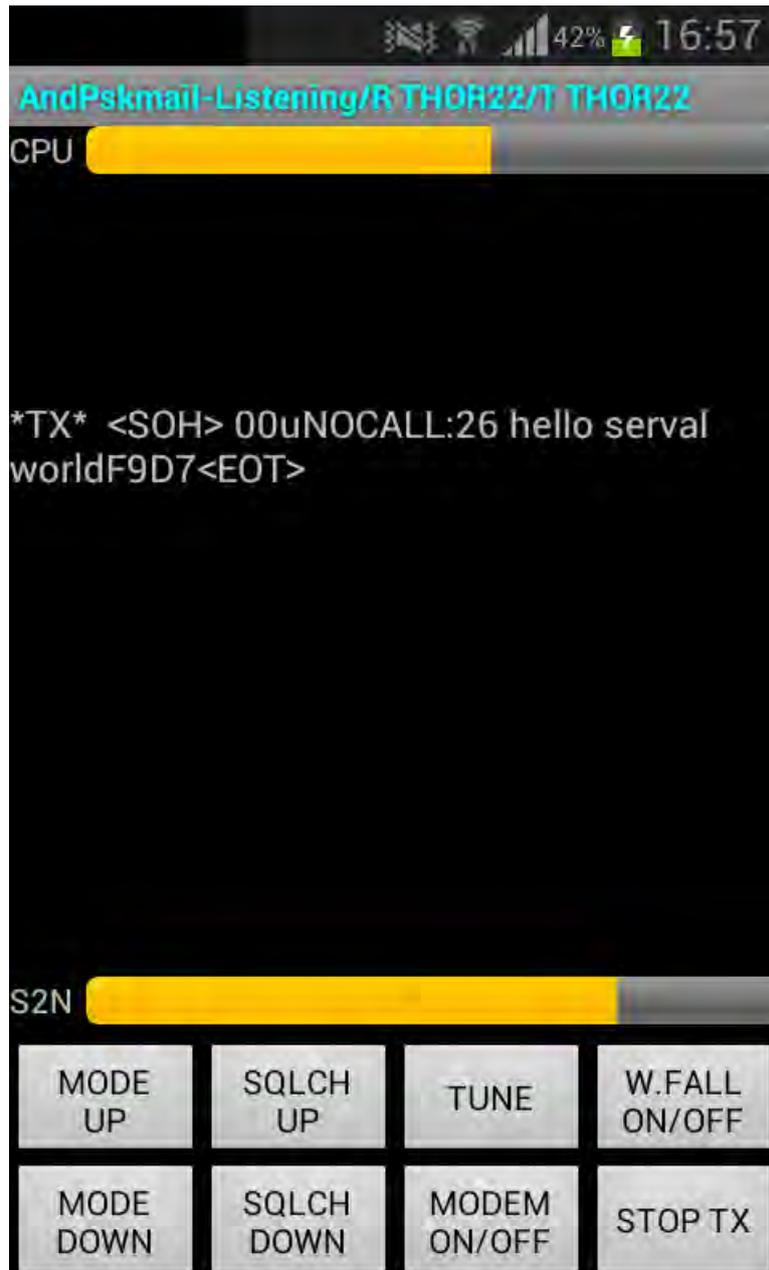


Figure 2 – Android PSKMail program after sending the test message.

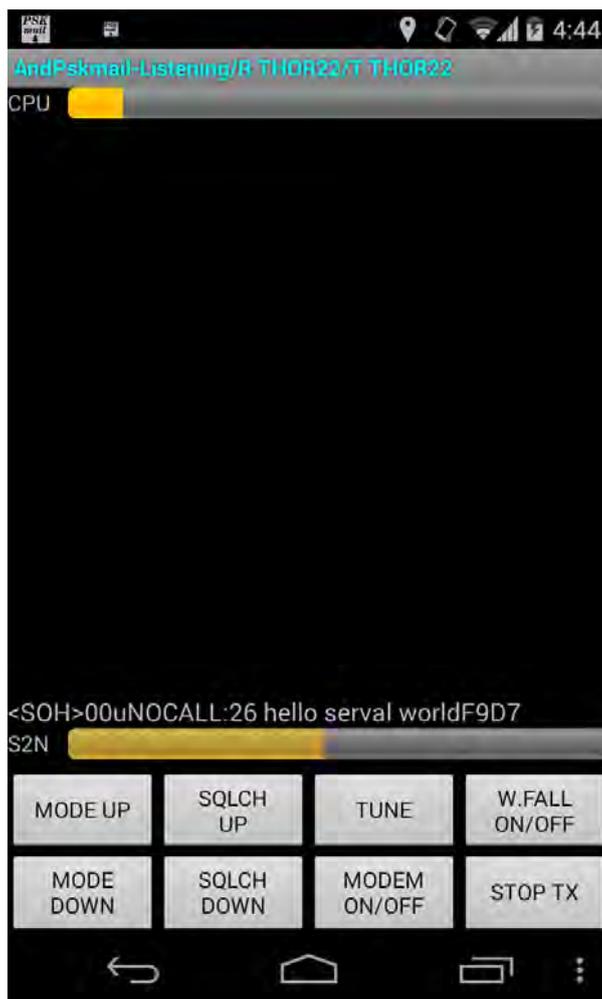


Figure 3 – Android PSKMail program after receiving the test message.

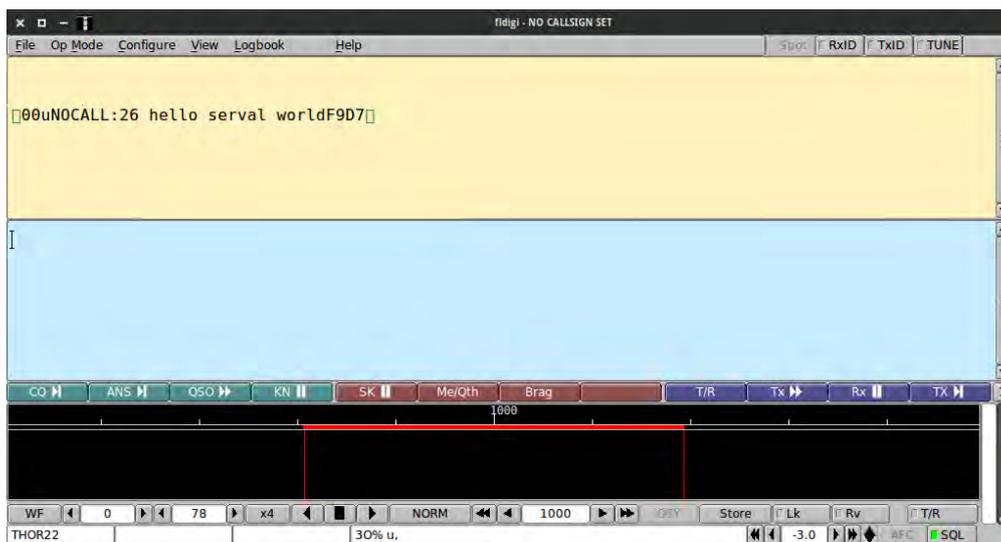


Figure 4 – Laptop version of fldigi after receiving the test message.

A radio transmission test was done using a car radio and a low-power FM transmitter of the type commonly used to interface MP3 and CD players with older car sound systems. The FM transmitter was a low-cost unit obtained via eBay for less than \$10, is unlikely to be high fidelity or to have a particularly wide usable bandwidth, and was presumably not designed with digital data transmission in mind. Hand-held CB radio handsets would have also provided an appropriate test platform, however we had no such hardware on hand.

It proved impossible to use the THOR22 modulation in this environment. Some experimentation yielded successful results with the PSK125 modulation scheme, as can be seen in Figure 5.

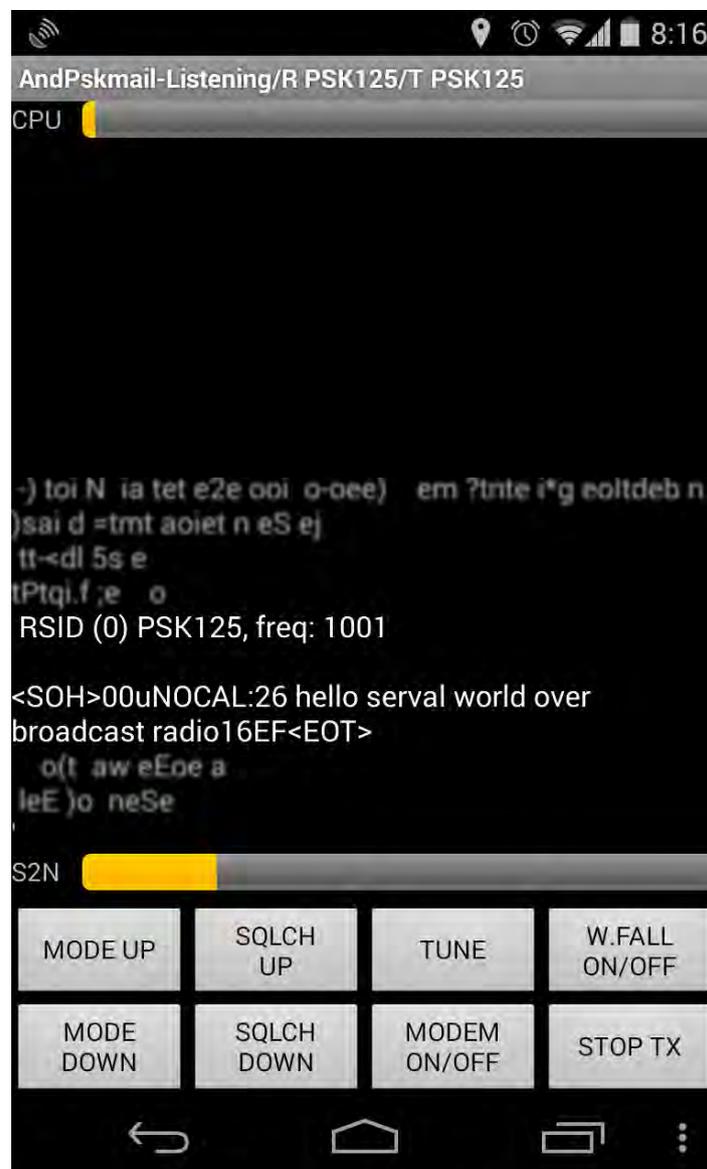


Figure 5 – Mobile phone display after receiving a test message (highlighted) via acoustic coupling over vehicular FM radio.

## Acoustic Coupled Serval Mesh Concept

From the above discussion it becomes clear that the bandwidth available to an acoustically coupled system will be extremely limited, on the order of 1 KB per minute. Thus communications will necessarily be limited to extremely succinct forms of communication.

Previous work on the Serval Mesh has focussed on enabling the efficient transmission of text messages and XML forms ([Gardner-Stephen et al 2014](#)) via low-bandwidth high-cost satellite links using a purpose written compression library ([Gardner-Stephen et al 2013a](#)). This has realised the capability to send useful text messages and compressed digital forms, e.g., of household or personal health assessment, using just a few bytes to several tens of bytes depending on the complexity.

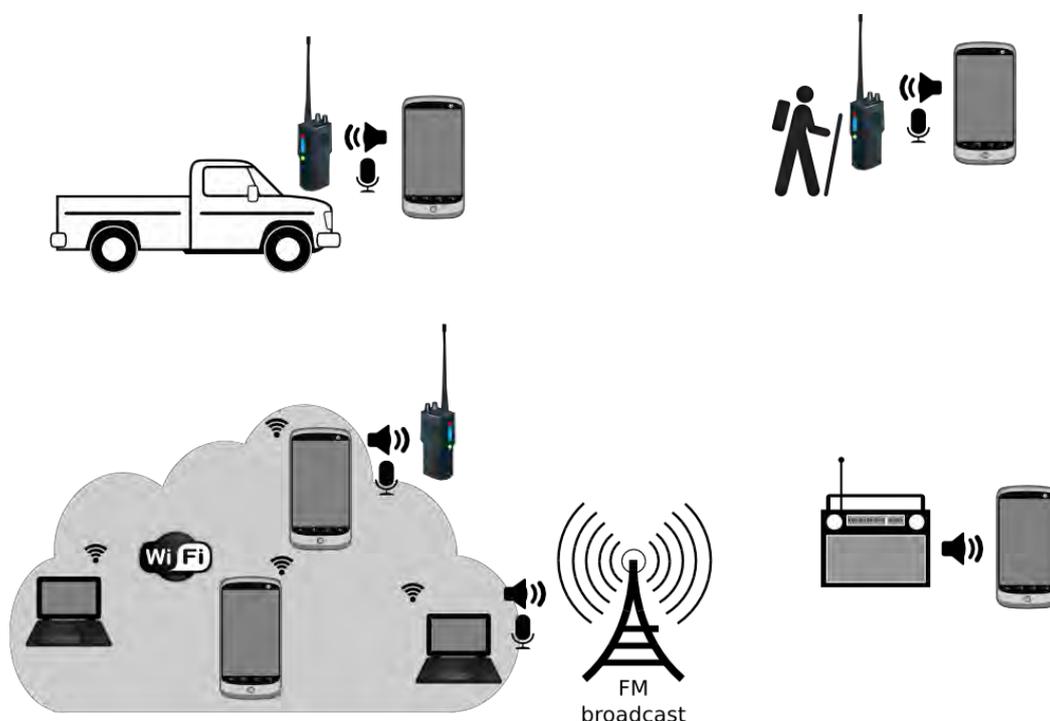
By limiting communications to these compact forms, and allowing for communications overheads, it should be possible to transmit of the order of 10 messages per minute. While such a transmission rate could be easily overwhelmed by a large user-base, in many situations the number of users in a geographic area will be limited, and so the available bandwidth has the potential to support a reasonable number of users. However, to function effectively, it will be necessary to include some mechanism for each participating transmitter to learn and remember which messages have already been transmitted by other stations, so as to minimise redundant transmissions. Similarly, mechanisms already designed into the Serval Mesh to allow deletion of content throughout the network after it has been received will be required. In all cases messages will be transmitted in encrypted form, so that only the intended recipient(s) can decode and read them, unless they are specifically sent out as a public message. Where messages are sent publicly, they will still be cryptographically verified, allowing receivers to have confidence that the message has not been fabricated or tampered with. This allows the possibility of efficiently disseminating information throughout rural and remote communities.

Integrating the acoustic coupled data transport with the existing Serval Mesh protocols makes it possible to share a single UHF or VHF radio among many users, as the Serval Rhizome protocol will allow messages sent from any device to find their way to the nearest radio, and similarly when they have been received by the radio at the far end, to be disseminated to other devices in that area. Thus the acoustically coupled radio transport becomes an addition transport in a Serval Mesh complementing the existing Wi-Fi, cellular, satellite and other transports that are already supported. Likewise, any interconnection between the Serval Mesh and the global communications network can be automatically leveraged in such an integrated scheme. Thus, for example, if someone is seeking emergency assistance, their call for help can

propagate through all available channels until it is received by a party who can respond, or can be delivered to such a party through contact with the Internet.

By using a radio with VOX activation the transmission would be triggered automatically by the phone by start sending a modulated message. This would give the possibility to provide a fully automated transmission system by simply placing a phone next to a VOX-activated radio at each end.

Figure 6 illustrates this concept by showing a number of mobile telephones running the Serval Mesh software, some of which are acoustically coupled to hand-held or vehicle mounted CB radios. A message entering the system through of these devices will eventually be replicated throughout the system so that the intended recipient can receive it.



**Figure 6 – Potential connectivity options.** The cloud in the lower-left represents a local Wi-Fi mesh network. One or more devices in this mesh may host acoustically-coupled transports. These could include broadcast FM, which could provide broadcast of selected data to many devices simultaneously, using common FM radios as the receiver (lower-right in the figure). Alternatively, devices in the mesh could be acoustically coupled to two-way radio units, such as Citizen Band radio. Such transmissions could be received by one or more parties using vehicle-based (upper-left) or hand-held (upper-right) radio receivers.

## Anticipated properties, limitations and challenges

Giving consideration to the opportunities and limitations described above, we anticipate that such a system would be capable of synchronising small amounts of data, including private messages and public announcements among a modest infrastructure-deprived community.

The use of voice-activated (VOX) radios brings the potential for automatic transmission of data. This would require considerable engineering effort to realise in an efficient manner, in

particular to adapt the Rhizome protocol so that it can manage automatic communications and make effective use of the channel, avoid transmission collisions between devices, and to remember the state of the device(s) that are reachable via radio.

This problem becomes even more complex if there are more than two radios that can transmit on the channel, or if there is no VOX capability in the radio to allow automatic transmission.

The modulation schemes surveyed in this paper all have throughputs that are of the order of kilobytes per minute, and thus will be limited in the data volume that they can be used to communicate per unit time. Considerable work will be required to make use of this limited bandwidth as efficiently as possible. It will almost certainly prove necessary to limit the types of data that will be carried by such media, for example allowing only text messages and other compact data, but excluding large files. The natural broadcast nature of radio transmission does, however, allow the possibility to transmit data such that it can be simultaneously received by multiple stations. This in turn has the potential to render possible the dissemination of general information, such as weather forecasts or the disposition of local services.

There also exist regulatory challenges to this concept, because the class licences for citizen band radio do not necessarily permit digital communications. This requires further exploration.

Finally, some effort would also be required to port the various amateur radio modulation programs to Android and other mobile operating systems, however this carries little technical risk.

## Conclusions/Recommendations

Despite the limitations and challenges of this approach, it seems to the authors that it should be possible to broadcast concise packets of data such as weather information, local news and limited private correspondence in a disaster zone or remote area where there is currently no such possibility. It is primarily in such information vacuums that this capability has the potential to protect life and property against various challenges, and thus derives its value. Therefore the authors intend to explore the realisation of this system as resources permit, with the intention of implementing the necessary protocols and undertaking initial trials in the Australian Outback.

## Acknowledgements

The Serval Project and authors wish to acknowledge the support of the Flinders University, the NLnet Foundation, the Shuttleworth Foundation, the Open Internet Tools Project, the New America Foundation and other private and institutional supporters.

## References

- Akbari, ME; Farshad, AA; Asadi-Lari, M. 2004. The devastation of Bam: an overview of health issues 1 month after the earthquake. *Public Health* , Volume 118 , Issue 6 , 403 – 408
- Crouch, A; Davies, S. 2013. A coordinated satellite and terrestrial microwave backhaul for cellular mobile in remote and regional Australia [online]. *Australian Journal of Telecommunications and the Digital Economy*, Vol. 1, No. 1, Nov 2013: [2.1]-[2.19]. Availability: <http://search.informit.com.au/documentSummary;dn=776009909539470;res=IELBUS> SSN: 2203-1693. [cited 12 Dec 14].
- Freese, D. et al. 2014. Fldigi. Available at: <http://www.w1hkj.com/Fldigi.html>, retrieved 13 Oct 2014.
- Gardner-Stephen, P; Bettison, A; Challans, R; Hampton, J; Lakeman, J; Wallis, C. 2013a. "Improving Compression of Short Messages." *Int'l J. of Communications, Network and System Sciences* 2013.
- Gardner-Stephen, P; Caldicott, E; Challans, R; Lakeman, J; Bettison, A; Gardner-Stephen, D; Lloyd, M; Malossane, T; Wallis, C. 2014. "Succinct Data: Extreme Compression for ODK Forms." To appear in *Global Humanitarian Technology Conference (GHTC), 2014 IEEE*.
- Gardner-Stephen, P; Challans, R; Lakeman, J; Bettison, A; Gardner-Stephen, D; Lloyd, M. 2013b. "The serval mesh: A platform for resilient communications in disaster & crisis." In *Global Humanitarian Technology Conference (GHTC), 2013 IEEE*, pp. 162-166. IEEE.
- Gardner-Stephen, P. 2011. "The Serval Project: Practical Wireless Ad-Hoc Mobile Telecommunications." Available at: [http://developer.servalproject.org/files/CWN\\_Chapter\\_Serval.pdf](http://developer.servalproject.org/files/CWN_Chapter_Serval.pdf), retrieved Oct 13, 2014 .
- Gardner-Stephen, Paul; Bettison, Andrew; Challans, Romana; Lakeman, Jeremy. 2013c. "The Rational Behind The Serval Network Layer For Resilient Communications." *Journal of Computer Science* 9, no. 12 (2013): 1680.
- Gruen, H; Divita, PS; Werneth, CJ. 1975. "Variable Bandwidth Voice and Data Telephone Communication System." U.S. Patent 3,875,339, issued April 1, 1975.
- Gutzmer, HA. 1992. "Acoustic coupler for high-speed modem." U.S. Patent 5,134,649, issued July 28, 1992.
- Jayapalan, JP; Lu, CC; Miller, WJ; Stephenson, JE. "Digital voice transmission having improved echo suppression." U.S. Patent 4,652,703, issued March 24, 1987.
- Luo, X; Li,H; Zhang,J; Shim, JP. 2010. "Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services." *Decision Support Systems* 49, no. 2 (2010): 222-234.

- Morawczynski, O; Miscione, G. 2008. "Examining trust in mobile banking transactions: The case of M-PESA in Kenya." In *Social Dimensions of Information and Communication Technology Policy*, pp. 287-298. Springer US, 2008.
- Patricelli, F; Beakley, JE; Carnevale, A; Tarabochia, M; Von Lubitz, Dag KJE. 2009. "Disaster management and mitigation: the telecommunications infrastructure" *Disasters* Volume 33, Issue 1, pp 23–37. Available at: <http://onlinelibrary.wiley.com/doi/10.1111/disa.2008.33.issue-1/issuetoc>
- Rappaport, TS. 1989. "Indoor radio communications for factories of the future." *IEEE Communications Magazine*, 27, no. 5 (1989): 15-24.
- Robertson, B; Wood, T. 2005. "Audio FSK encoded digital data packet embedded in the audio message portion of an EAS protocol transmission, and related methods." U.S. Patent Application 11/091,735, filed March 28, 2005.
- Sano, H. 1994. "Method and arrangement of echo elimination in digital telecommunications system." U.S. Patent 5,313,498, issued May 17, 1994.
- Serrano, AL. 1983. "Modem telephone interface circuit." U.S. Patent 4,367,374, issued January 4, 1983.
- Sklar, B. 2011. *Digital communications*. Vol. 2. NJ: Prentice Hall, 2001.
- Tims, K. 2006. "An example demonstrating Binary [Frequency-shift Keying](http://commons.wikimedia.org/wiki/File:Fsk.svg)." <http://commons.wikimedia.org/wiki/File:Fsk.svg>, retrieved Dec 12, 2014.
- Usselman, GL. 1949. "Frequency shift keying." U.S. Patent 2,461,456, issued February 8, 1949.
- Airchat. 2014. Various contributors.. AirChat. Available at: <https://github.com/lulzlabs/AirChat>, retrieved 13 Oct 2014.
- PSKMail. 2014. Various contributors. 2014b. Available at: <http://pskmail.org>, retrieved 13 Oct 2014.
- Yang Ran. 2011 "Considerations and suggestions on improvement of communication network disaster countermeasures after the Wenchuan earthquake," *Communications Magazine, IEEE*, vol.49, no.1, pp.44,47, January 2011 doi: 10.1109/MCOM.2011.5681013 Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5681013&isnumber=568103>

# Warrnambool Exchange Fire – Resilience and Emergency Management

---

**Mark A Gregory**

RMIT University, mark.gregory@rmit.edu.au

**Kaye Scholfield**

RMIT University, kaye.scholfield@rmit.edu.au

**Khandakar Ahmed**

RMIT University, khandakar.ahmed@rmit.edu.au

**Dorothy McLaren**

RMIT University, dorothy.mclaren@rmit.edu.au

**James Williams**

RMIT University, james.williams@rmit.edu.au

**Helen Marshall**

RMIT University, helen.marshall@rmit.edu.au

---

**Summary:** Effective emergency management of a disaster at a single point of failure is vital if the effects of the disaster are to be mitigated. The immediate impacts of a disaster highlight stakeholder perspectives. There is no one-size-fits-all solution to every disaster. Nevertheless, analysing features, aftermath, impact and interim services made available after a disaster provide lessons that can be utilised to avert or mitigate the effects of similar events in the future. This paper provides lessons learnt from the a fire that occurred in 2012 in the Warrnambool telephone exchange located in Victoria, Australia and proposes a strategy that provides increased network resilience and more effective emergency management once the copper-based core switching in exchanges is progressively replaced by fibre service area modules.

## Introduction

A fire occurred on November 22, 2012 at 4.35 AM in the vicinity of the Maintenance Control Room at Telstra's Warrnambool Exchange building in Victoria, Australia. The exchange acts as a transmission hub for telecommunications connecting about 100,000 people from South West Victoria, about 15,000 square kilometres. Within four minutes of the fire alarm, the local fire fighters were on the scene; however, by the time fire was put out, it had caused significant damage to essential telecommunication equipment. The cable connection between the Telephony and Broadband Communications Equipment and the Main Distribution Frame, and other internal building cables connecting the site to the remainder of the Telstra network, were destroyed. The Warrnambool Exchange is a single point of failure for much of the

telecommunications infrastructure in the region, and the fire led to the loss or degradation of regional telecommunication services for up to 20 days ([Gregory & Scholfield 2013](#)).

## A. Immediate aftermath

Telstra's Major Incident Management group released an immediate initial assessment at 5.46 AM on 22 November 2012 and a final fire investigation report on 27 March 2013. Services impacted included:

- 61,856 PSTN telephony services
- 14,409 ADSL services and consumer broadband
- 56 ISDN services
- 40 3G-Mobile Base Stations
- 138 Metropolitan Area Network (IPMAN) services
- 13 Telstra Internet Direct services
- Multi Service Edge Router failure (Impact summary 268 x Business DSL, 16,094 x ADSL, 4 x Internal use Frame Relay/ATM, 47 x Frame Relay/ATM, 40 x 3G Mobile Base Stations)
- Specialised Mobile Radio (SMR) services, Loss of all Radio Coverage Warrnambool & Port Campbell
- Loss of communications to Digital Video Network equipment at Warrnambool & Terang node for Sky Racing (Television feed to horse racing track)

## B. Impact from different perspectives

The economic and social impacts on three broadly defined groups – local businesses, community service providers and individuals – varied across the affected region surrounding Warrnambool, a city with a population of approximately 33,000. The estimated daily economic impact of a complete telecommunication outage to Warrnambool city was estimated to be up to \$0.4 million per day in the worst case or approximately 5 per cent of its daily economic output. The direct cost to the Great South West Coast region was estimated to be up to \$0.95 million per day, or approximately 3 per cent of the region's daily output (DBCDE 2013). The financial effect on the community appear to have been greater than initial reports due to financial claims continuing after investigative reports were published (Gregory & Scholfield 2013; [International 2013](#)).

### 1) Local Businesses

In modern society, business relies upon electronic financial transactions carried out using online banking or EFTPOS. However, due to the outage, local businesses were unable to utilise any form of electronic financial transactions resulting in reduced business activity and missed commercial opportunities. Utility providers reported interruptions in monitoring and controlling essential distributed networked systems. The local tourism industry was negatively impacted by loss of access to online booking systems and customer interaction. The retail sector had reduced activity during the Christmas trading period. The important agricultural sector was unable to retrieve timely information about commodity markets and lost access to its suppliers and customers.

### 2) Community Service Providers

Community service providers were severely impacted and lost capacity to manage or coordinate staff and volunteers and to perform otherwise routine activities. The affected community service providers included health and welfare organisations, council and emergency services including ambulance, police and the regional volunteer fire fighting authority which was to play a major role in information dissemination.

### 3) Individuals

The impact on individuals was considerable, due to the inability to get funds for commodities or to call work, family and friends or to notify organisations like banks. Casual staff working hours in the retail and health sectors were reduced in some instances and some businesses were forced to cease trading during the outage. People had to travel for up to four hours to find ATMs and return home, to purchase prepaid mobile phone services for the surviving Optus 3G mobile cellular network or to complete other tasks. Elderly people who were living alone, people with telecommunication-connected medical devices and people with health concerns were insecure and found to have increased levels of anxiety and a sense of isolation. Community efforts to mitigate the outage effects on the vulnerable were considerable.

## II. Relevant disasters

An Australian bushfire, referred to as “Black Saturday” (Teague et al. 2010) on February 7, 2009 took 173 lives, ravaged thousands of hectares of land and burned down hundreds of houses. Eight Telstra regional mobile cellular towers, 2800 fixed phone lines, 2100 ADSL internet connections and 39 ISDN phone lines went out of operation. Telstra invested \$15 million to repair and upgrade its network in the affected areas. During that time, Telstra installed four new exchanges in Marysville, Narbethong, Kinglake and Kinglake West, and built new mobile cellular network base stations to provide permanent and improved mobile

coverage to the affected areas. Whilst this disaster affected a much smaller region than that affected by the Warrnambool Exchange fire, the loss of infrastructure meant a similar widespread loss of telecommunications services until the infrastructure was rebuilt or replaced by portable systems.

Queensland, another Australian State, experienced a series of natural disasters during the summer of 2010-11 with the destruction wrought by Severe Tropical Cyclone Yasi ([Boughton et al. 2011](#)). The entire state, 1,727,000 square kilometres, was declared disaster affected with the tragic death of 37 people. 159 Telstra mobile cellular network sites, 60 GSM mobile sites, 94000 fixed line services and 32000 ADSL broadband services were disrupted and went out of service for periods that in some areas lasted weeks.

The Warrnambool Exchange fire, followed by the network outage affecting 100,000 people of South West Victoria, was quite different from a natural disaster. In contrast to a natural disaster, the Warrnambool and surrounding communities were affected only by the loss of telecommunications, and community life continued unabated: most businesses still opened, homes were still occupied, roads and other infrastructure were operational. There was no lead time for preparations to be made and contingency plans to be deployed. The impact and consequences of the event for people and organisations outside the affected area ranged from no disturbance at all if interaction with people and organisations within the affected area was not required, through to significant disturbances to commercial life, personal interactions and communications with people, businesses and government within the affected region.

Incidents of large scale loss of service due to the partial or complete destruction of a telecommunications exchange are relatively rare events. In May 2011 an incident similar to the Warrnambool Exchange fire was reported in Malaga, Spain ([Movistar 2011](#)). It was suspected that the fire was ignited by lightning.

On 8 May, 1988, a fire occurred in the main switching room of the Hinsdale Central Office of the Illinois Bell telephone company ([FTIC 1989](#)). It was one of the largest switching systems in the state, connecting 38,000 customers including hospitals, business and Chicago's O'Hare and Midway Airports. Each day, the facility was used to process 3.5 million calls. The aftermath of the fire at the centre was significant at Hinsdale and the surrounding regions. Telephone service was lost for almost 40,000 local phone lines. Illinois Bell took two weeks to completely restore telephone service for the affected region.

On 18 July, 2001, a 60 car CSX transportation freight train derailment occurred in a freight through-route tunnel under Howard Street in Baltimore, Maryland. The Howard Street tunnel housed an Internet pipe serving seven of the biggest US Internet Information Services Providers (ISPs). The fire burned through the pipe and damaged these cables which were used

for voice and data transmission, causing backbone slowdowns for ISPs such as Metromedia Fiber Network, Inc., WorldCom, Inc., and PSINet, Inc (Wikipedia 2001).

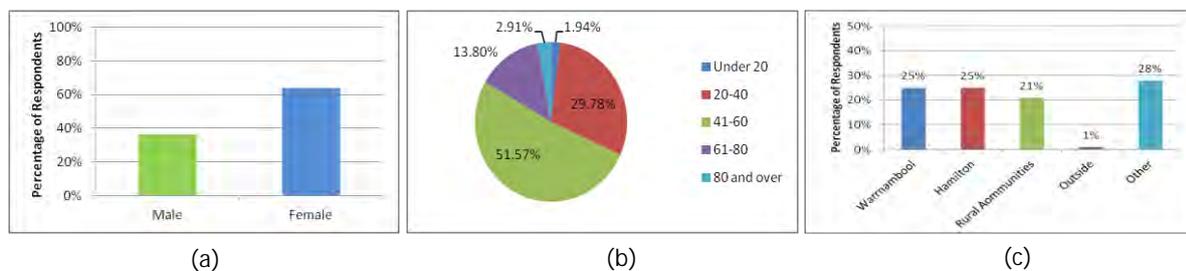
Fifty years ago, on 22 September, 1961, an incident of a similar nature was recorded in the Canberra suburb of Civic, Australia (DBCDE 2013). In that event, a telephone exchange was damaged destroying 5,402 fixed line telephone services. The cause of the fire remains unknown. To restore this exchange, 200 skilled people worked 12-hour shifts to install new equipment in temporary facilities. The restoration process took seven weeks to be completed.

### III. Social Impact Assessment

Two surveys and several community discussion group sessions were carried out in order to assess the impact of the Warrnambool Exchange fire (Gregory & Scholfield 2013). An online survey was not possible, so paper-based surveys were printed, distributed and collected. In addition, cards with the survey address were printed and distributed inviting people to go online once their Internet service resumed. Media and community partners assisted in raising awareness of the research. Initial surveys from residents in South West Victoria were collected between December 2012 and the late January 2013. A survey conducted in the second half of 2013 focused on how the loss of telecommunications connected devices affected people.

The survey questions were grouped into sections which provided respondents with the opportunity to comment on how the outage affected different aspects of their lives.

Personal (non-identifiable) demographic and geographic information was collected, including a section that identified the response as being from the perspective of an individual, business owner/operator, community member or other (as specified). Those who wished to respond from more than one perspective were asked to fill in separate surveys for each category. Length of disruption (in days) was canvassed for landlines, mobile phones and internet access, with capacity to nominate differing lengths of disruption per item. The nature of communication disruptions was identified as either friends/family related or business related, with the opportunity to comment further if desired.



**Figure 1 – Personal demographic and geographic information: a) Gender b) Age Group 3) Demography**

Impact on business and commerce was surveyed with questions regarding retail and work-related concerns. Respondents were invited to tick boxes if they had found it difficult or impossible to make essential purchases (food and fuel), pay bills or make bookings. For those who were regularly employed, information was sought as to the impact on their usual place of work, particularly inability to conduct business (shut down), reduced ability to process orders, loss of customers or difficulty in conducting tasks (such as accessing email). In each case, additional comments were also invited.

Health and health-related concerns were canvassed, including both actual health emergencies and concerns for health and safety due to the outage, through both specific questions and comment boxes. General comments were also sought regarding impact on community life and any positive impacts arising from the lack of telecommunications. Estimates of financial cost were sought with tick boxes for specific dollar amounts and, again, the opportunity to comment more broadly.

Two questions invited comments on non-essential activities that people would have liked to do but were unable to, and activities that people really needed to do but were unable to, because of the outage. Planning for the future was also queried, and respondents were asked to identify whether or not they had begun to think about and plan for the potential for other, similar, events in the future. This included an invitation to elaborate on alternative or future plans. Finally, the opportunity to make other comments was offered.

The responses received reflected the geographic spread of the population across the affected region and the particular business and personal interests of each respondent. There was a lower response from the northern areas possibly because the greatest effect was in Warrnambool and its immediate surroundings. Approximately 50% of the responses were divided equally between Warrnambool and Hamilton, the region's second largest city. 21% of responses were from rural communities and small towns of less than 1,000 residents. Just 1% of the responses were from people outside of the affected area. The smaller communities of Colac and Portland provided 5% of total responses. Two thirds of respondents were female with the largest number (138) being from females aged between 41 and 60. A survey data set was processed using NVivo10 (QSR International 2013) and the survey questions were then coded to create sub-categories or themes. The analysis showed recurring themes including work, access to money, health and safety, communication and impact on the community.

#### IV. Steps taken in the immediate aftermath

The response and restoration process in any disaster involves the provision of an interim service and a permanent solution. Telstra, the owner and operator of the Warrnambool Exchange, provided both.

## A. Interim Service

Telstra deployed Mobile Cells on Wheels (COW), Mobile Exchanges on Wheels (MEOW) and Satellite COWs (SatCOWs) to provide interim services to some customers, including emergency service organisations, some hospitals and some priority assistance customers (Piltz 2013).

All cellular mobile services, including non-Telstra customers, received access to the Triple Zero service (911) as Telstra rebuilt the mobile cellular network connectivity as a priority. However, customers without a mobile remained isolated and unable to access emergency services. Additionally, Telstra deployed satellite phones to emergency service locations and distributed interim mobile and satellite phones to customers based on a medical priority list.



**Figure 2 – a) Satellite Cells on Wheels b) Mobile Exchange on Wheels, Source: (Piltz 2013)**

## B. Long Term Restoration

In restoring the Warrnambool Exchange, Telstra followed a similar approach to that adopted for other recent disasters, such as the Victorian “Black Saturday” Bushfires in 2009 (Teague et al. 2010), Cyclone Yasi in 2010 (Boughton et al. 2011) and the Victorian floods of 2011 (Comrie 2011). This approach is based on 3 day, 3 week and 3 month horizons for restoring services. Telstra utilised 110 highly skilled technicians working rotating 12 hour shifts under the guidance of design, data configuration, logistics and project management experts. The complete restoration process took three weeks and was completed on Wednesday 19 December 2012. Telstra’s operations groups including Service Delivery, Network Construction, Network and Access Technologies and Network and IT operations worked together coordinated by the Telstra Global Operations Centre to achieve restoration in the following sequence (Piltz 2013):

### 1) Building services restoration

The very first restoration step was taken immediately after Telstra regained access to the exchange. Temporary facility access and roofing, provision of power and lighting were completed on the first day.

This initial building restoration work provided the repair teams with an environment within which they could access and temporarily repair other services such as air-conditioning.

### 2) Transmission equipment

The opening step towards restoring telecommunication services was the complicated transmission equipment repair. This included repairing or replacing parts of the transmission equipment and fixing cabling within equipment racks. As the transmission equipment supports the functionality of other services customer services remained unaffected at this stage.

### 3) Data node and mobile service restoration

The next focus area was the data node (IP based routing). Once the transmission equipment and associated cables were interconnected the IP routing equipment provisioning became available for the restoration of limited data and mobile cellular services.

The next restoration step was the repairing or replacing links to the adjoining and remote mobile cellular base stations and this work commenced on 23 November 2012. The reconnection of directly connected mobile base stations needed the cabling within the exchange to be restored. The data node was also required to be connected to the exchange transmission equipment.

By the end of this step, mobile cellular voice services started functioning as regional mobile cellular base stations were reconnected, tested and put into an operational state. At this time some of the internet and other data services were also restored as cabling was re-commissioned and tested. According to Figure 3(a), all of the mobile cellular base stations were restored within the period 22 to 29 November 2013.

During that time, the older Optus 3G mobile cellular sites were in operation due to this network connecting to a different transit point. Mobile devices within range of the Optus network were able to access Triple Zero services. However, the Optus network was quickly swamped during peak times when people realised it was operational and rushed to get prepaid access to this network.

#### 4) Restoration of call switching capabilities

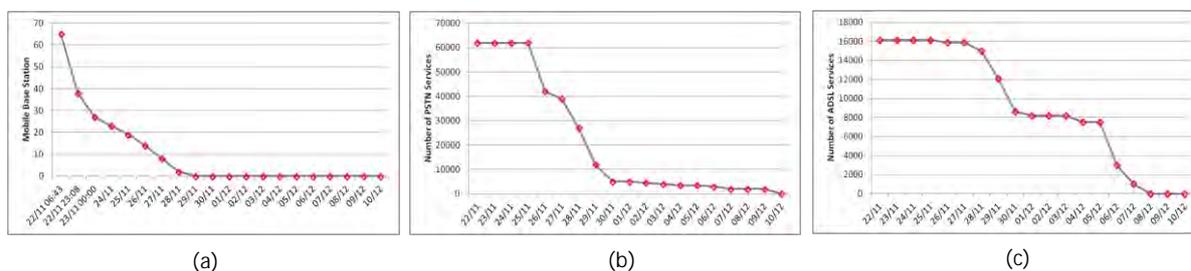
Re-parenting of PSTN services to South Melbourne, the upstream exchange, was commenced on 25 November 2014. Other than restoring the core telephony switch, PSTN switching for Warrnambool and surrounding smaller exchanges were rerouted to a central switch in South Melbourne by using the restored transmission equipment and reconfiguring the Ericsson AXE exchange at Warrnambool. By taking this action Telstra reduced the restoration time necessary to return full service to the region.

As illustrated in Figure 3(b), within a six day period from 25 to 30 November 2012, 92 per cent of PSTN services were restored. However, it took another seven days to restore the remaining 5000 PSTN services.

#### 5) Restoration of Internet services

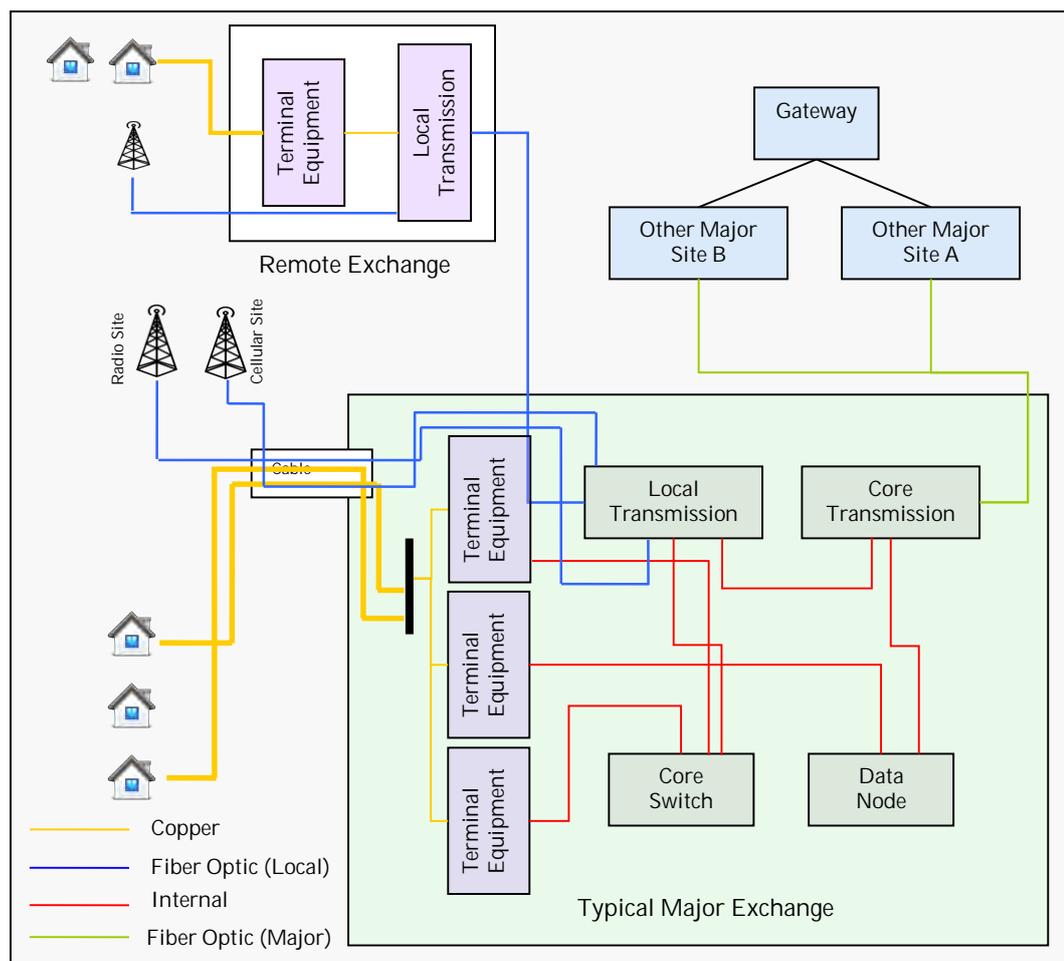
Restoration of Internet services was the last major activity undertaken. This involved replacing the destroyed DSLAMs and terminal equipment within the Warrnambool Exchange.

Figure 3(c) shows how the internet service restoration progressed for an initial period and then had a delay before further restoration occurred due to other restoration activities. The timing of the internet service restoration was linked to the reconnection of remote exchanges and the rerouting of PSTN services.



identified as vital to restoring region wide telecommunications coverage. From the technical perspective this early restoration of mobile cellular services had several advantages including:

- The least amount of equipment restoration and cabling repair required within the Warrnambool Exchange. (Transmission and limited fibre cables)
- The central cellular switch is not located within the exchange building.
- All terminal equipment is located at the base stations remote to the building.
- Temporary (MEOW & COW) solutions are already in service and can be integrated.



**Figure 4 – Typical Major Exchange Equipment, Source: Telstra**

## V. Typical exchange architecture

Telstra reported that the incident caused damage to equipment which included

- i) transmission equipment,
- ii) core telephony switch,
- iii) data node,
- iv) terminating equipment,

- v) v) external cables, and
  - vi) vi) internal cables,
- as shown in Figure 4.

## A. Transmission equipment

Transmission equipment uses optic fibre or radio systems to provide connections beyond the exchange building.

The transmission equipment was considered in two functional groups: core transmission equipment, which provides connection from the major exchange to the backhaul network, and local transmission equipment, which provides a connection from the exchange to the remote regional exchanges. The local and core transmission equipment is also connected to the central switch and data node within the major exchange.

For a major exchange, redundant transmission equipment is installed so that an alternative path is available to maintain service in the event of any element failing. In the Warrnambool Exchange fire the redundant transmission equipment also failed, resulting in a total loss of transmission capability that impacted all data and voice services.

## B. Core telephony switch

Core telephony switches enable establishment of a connection path between two parties. Modern fixed telephone networks are based on a limited number of core switches located in major exchanges. Although terminal equipment contains limited switching capability, in most cases the core switch is required to establish a connection path.

A core telephony switch is generally not duplicated in an alternative location. However, within a core switch, the hardware elements are typically duplicated. This means that any single card or device fault will not interrupt service.

The core telephony switches in the Warrnambool Exchange supported the local and regional terminal equipment. The fire damaged the core switches (including the duplicate hardware elements), rendering it impossible to connect voice calls from remote and local terminal equipment.

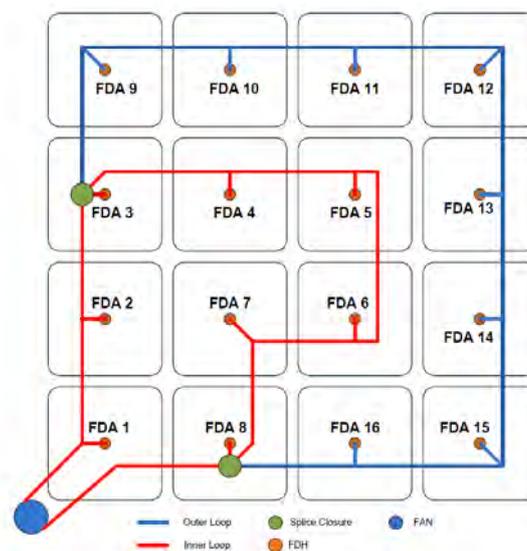
## C. Data node

The data node routes all data services to the correct location, including IP management, cellular data, Internet, EFTPOS and xDSL services. Failure of the data node prevents routing of data services connected to terminal equipment in the major exchange and in remote exchanges. It also includes loss of connectivity for cellular data.

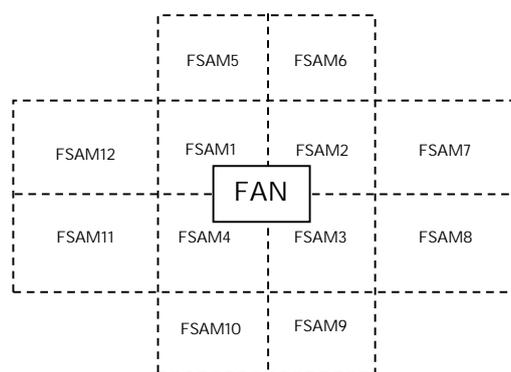
Similar to the core telephony switch, individual components of a data node are duplicated and any single fault will not cause system outage, but the Warrnambool Exchange fire caused both equipment and redundant equipment failure.

#### D. Terminal equipment

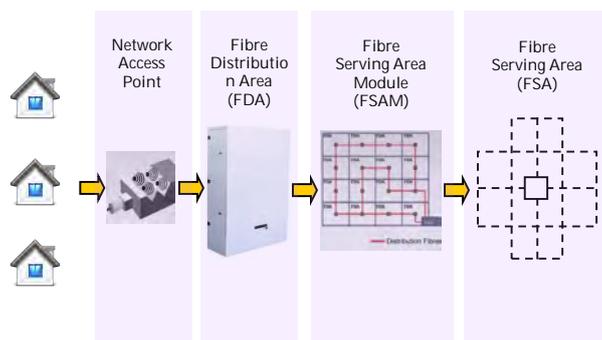
The terminal equipment comprises copper line termination (CLT) devices and optical line termination (OLT) devices. For a copper network, a CLT converts the signal from analogue to digital, and for a fibre network, the OLT converts the signal from electrical digital to light. The digital signal is then sent to either the core telephony switch to connect a call, or the data node to receive routing information. The local transmission equipment carries signals from remote exchange terminal equipment to the core switch and the data node.



(a) Schematic diagram of Fibre Service Area Module



(b) Fibre Serving Area



(c) Network Design Replicating Module

**Figure 5 – a) Schematic diagram of Fibre Service Area Module b) Fibre Serving Area c) Network Design Replicating Module, Source: (Ferris 2011)**

Voice terminal equipment may provide limited switching capability. In general, voice terminal equipment comprises one or more terminal switching stages, with each stage catering for 500-2,000 services. In the event the terminal switching stage is disconnected from the core telephony switch, sufficient capability may remain within the terminal switching stage to enable voice calls to other services connected to the same stage.

However, if the voice call is between a customer on one switching stage and a customer on another terminal unit, or a mobile service, or outside of the region, the call must traverse the core switch. As stated above, if the core switches are not operational, most calls cannot be connected.

Terminal equipment, either within the same device as voice or as separate equipment, also provides data capability. In general, it includes equipment for the provision of ADSL and other data service equipment. However, unlike with voice services, terminal equipment used to deliver data services requires a connection to the data core in the major exchange in order to operate.

## E. External cable

Multiple cables of both copper and optic fibre enter a typical major exchange. Copper cables provide connection of fixed line services (telephony and lower speed data) to homes and businesses. Optic fibre cables provide high speed data services to some business customers, links to cellular bases, remote exchanges and special services such as Sky Racing. Optic fibre cables are also used for core network cables that provide connections between major exchanges. Typically, critical cables enter an exchange such as Warrnambool in different places and occupy different locations on the street to prevent the cables being damaged by the same event.

## F. Internal cable

Within the exchange building, many cables are used to interconnect the various functional elements, and to connect the functional elements to the point where external cables terminate. Internal cabling is normally installed on cable trays suspended from ceilings or beneath raised floors. In both cases, the cables are combined and follow limited routes within the building. These internal cables are essential for the provision of services. The internal cables are represented in red in Figure 4.

## VI. Container-based resilient approach

Improving network resilience, which is the ability to provide and maintain an acceptable level of service in the event of network degradation, is an important focus for network planners and the Warrnambool Exchange fire demonstrates that, at times, planning can be outweighed by events.

Future planning for a resilient network should include identification of new resilient technologies, resilient network designs and how infrastructure can be built and utilised to provide increased resilience to combat a range of events such as a major fire or natural disaster.

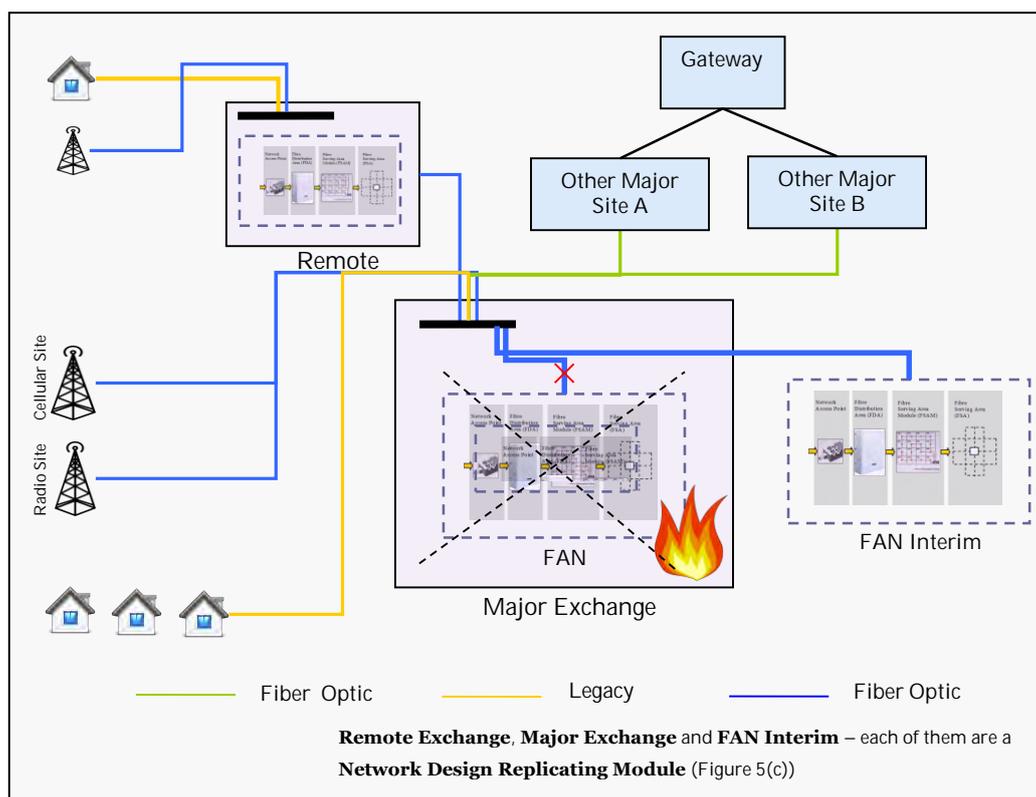
Modern telecommunication networks retain infrastructure single points of failure due to the cost and complexity of duplication when the single point of failure is a major facility such as a regional telephone exchange. The trade-off between improved network resilience and the practicalities of network design and operation often leads to compromises that may result in the strategic acceptance of single points of failure existing within a network.

Australia, similar to many other nations, is using more optical fibre in its access networks, which reduces the cabling and equipment found within a typical major exchange. The introduction of fibre into access networks decreases the amount of cabling that typically enters a typical major exchange building and as the fibre is brought into the exchange there is an opportunity to improve network resilience by adopting an approach that provides faster service restoration capability in the event of a major fire or some other natural disaster that affects the serviceability of the exchange infrastructure and internal systems.

Containerisation of key telecommunication systems including access network termination, aggregation and transit systems would provide a vital capability that could be deployed to enhance or replace existing facilities in the event of a major infrastructure failure. The use of COWs, MEOWs and SatCOWs has now become common place, not only to enhance network capability for special sporting or other social events, but also to replace capability destroyed in a natural disaster.

In the case of the South West Victoria region, the Warrnambool Exchange is a single point of failure that hosts backhaul link endpoints, aggregation and access network technologies. As the Australian national broadband network brings about a change in the access network technologies there will be a reduction in copper utilisation and an increase in the use of fibre within the access network. Access network copper feeder cables connecting consumers to access, aggregation and backhaul within the Warrnambool Exchange will be replaced with fibre over the next five to ten years.

As an example of how containerisation of key systems would improve resilience consider a fibre to the premises access network. Figure 5 (a) shows a typical Fibre Service Area Module (FSAM). By moving away from copper to an all or partial fibre access network, the exchange could be redesigned, as shown in Figure 6, in such a way that the Fibre Access Node (FAN) and FSAM modules (Ferris 2011) could be caged into one or more containers. In this scenario the point of interconnect is the container and the fibre entering and leaving the building would terminate at the containers.



**Figure 6 – Proposed Architecture of a Major Exchange**

In the situation where an exchange hosts a FSAM, which consists of a series of up to 16 Fibre Distribution Areas (FDA) that are linked by fibre in a double loop configuration. A single fibre sheath connects the FSAM and Fibre Distributions Hubs (maximum 16) to a nominated FAN. A single fibre sheath is typically 21 mm thick and contains 312 cores with separate tubes for distribution, trunk, GPON or Ethernet and P2P fibres. An FSAM may cover a small town or a

part of suburb in the case of large cities. Approximately 2000 to 3000 premises could be accommodated depending on the location and network planning or topology.

The FAN houses active equipment to service a FSA. Fibres from the FDHs are terminated in the FAN using high density fibre distribution management frames before being used as input to 2.5 GPON line cards or 10 GPON line cards. If the building is destroyed then a new interim mobile container could be brought in and placed adjacent to the destroyed building. The external fibre cables could be patched and rerouted into the replacement container providing immediate service restoration.

A key reason why this approach is more suitable for the restoration of an all or partial optical access network is the reduction in cabling from the more than 250,000 copper pair entering the Warrnambool exchange to what could be less than 10,000 fibres necessary to support an all or partial optical access network for a region the size of South West Victoria. Also the task of restoring the facility can be delayed whilst the interim mobile container is brought online.

Similar to the approach presented to restore fibre networks, the mobile cellular networks are already geared towards central switching and could be readily restored utilising exchanges on wheels or containerisation. There is a synergy that can be leveraged as the shift from copper to fibre access networks occurs and this will significantly enhance network resiliency and emergency management efficiency.

## VII. Conclusion

Presented in this paper is a practical strategy for enhancing emergency management and network resiliency as the shift from copper to all or partial optical access networks occurs. Existing copper access networks are problematic for any shift to a more resilient network due to their age and design but with the onset of all- or partially-optical access networks there is an opportunity to design infrastructure installations for a more resilient operation and faster restoration if a disaster occurs at an infrastructure single point of failure. The Warrnambool Exchange fire provided an opportunity to closely review the effects of a single point of failure being destroyed by fire and the service restoration that followed. The research findings highlighted the need to reduce the impact of infrastructure single point of failure disasters by moving to an infrastructure build approach that permits duplicated containerised facilities containing key telecommunication systems to be installed and made operational quickly.

## Acknowledgements

This work was supported by a 2013 Research grant from the Australian Communications Consumer Action Network: 'Warrnambool Exchange Fire Consumer Impact Analysis'.

## References

- Boughton, G.N; Henderson, D.J; Ginger, J.D; Holmes, J.D.; Walker, G.R.; Leitch, C.J.; Somerville, L.R.; Frye, U.; Jayasinghe, N.C.; Kim, P.Y. 2011. Tropical Cyclone Yasi -- Structural damage to buildings. CTS Technical Report No 57, Cyclone Testing Station School of Engineering and Physical Sciences James Cook University Queensland Available from: [https://www.jcu.edu.au/cts/publications/content/technical-reports/jcu-078421.pdf/at\\_download/file](https://www.jcu.edu.au/cts/publications/content/technical-reports/jcu-078421.pdf/at_download/file).
- Comrie, Neil. 2011. Review of the 2010–11 Flood Warnings & Response. Available from: <http://www.floodsreview.vic.gov.au/about-the-review/final-report.html>
- DBCDE. 2013. *Inquiry to learn lessons from the Warrnambool exchange fire* [cited February 2014]. Available from: [http://apo.org.au/files/docs/DBCDE\\_WarrnamboolInquiryLessons\\_June2013.pdf](http://apo.org.au/files/docs/DBCDE_WarrnamboolInquiryLessons_June2013.pdf).
- Ferris, Peter. 2011. NBN Co. Briefing Engineers Australia – Sydney Division
- FTIC. 1989. *Hinsdale Central Office Fire Final Report 1989* [cited March 1989]. Available from: [https://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=OCCKQFjAB&url=http%3A%2F%2Fwww.telephonecollectors.info%2Findex.php%2Fdocument-repository%2Fdoc\\_download%2F12082-the-hinsdale-challenge-1988-executive-summary&ei=3\\_wHVMr8K8W8ugS\\_oYCOcg&usq=AFOjCNFNa3g1j9CPPXos7iDIjceyvU-KnQ&sig2=ECdZpb3sUiuID2XYIkrQ-g&bvm=bv.74649129.d.c2E](https://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=OCCKQFjAB&url=http%3A%2F%2Fwww.telephonecollectors.info%2Findex.php%2Fdocument-repository%2Fdoc_download%2F12082-the-hinsdale-challenge-1988-executive-summary&ei=3_wHVMr8K8W8ugS_oYCOcg&usq=AFOjCNFNa3g1j9CPPXos7iDIjceyvU-KnQ&sig2=ECdZpb3sUiuID2XYIkrQ-g&bvm=bv.74649129.d.c2E).
- Gregory, Mark A; Scholfield, Kaye. 2013. Warrnambool Exchange Fire Consumer Impact Analysis. [cited February 2014]. Available from: <https://accan.org.au/grants/completed-grants/623-warrnambool-exchange-fire-consumer-impact-analysis>
- QSR International. 2013. NVivo. [cited February 2014]. Available from: [http://www.qsrinternational.com/products\\_nvivo.aspx](http://www.qsrinternational.com/products_nvivo.aspx)
- Movistar. 2011. *Fire in Telefonica Exchange in Malaga*. 123 Marbella Internet Services, Sunday, May 8th, 2011. Available from: <https://www.123marbella.co.uk/fire-in-telefonica-exchange/>.
- Piltz, David. 2013. Warrnambool Exchange Fire Investigation Report, Telstra Corporation Limited.
- Teague, Bernard; Mcleod, Ronald; Pascoe, Susan. 2010. *2009 Victorian Bushfires Royal Commission* Final Report Summary [cited February 2014]. Available from: [http://www.royalcommission.vic.gov.au/finaldocuments/summary/PF/VBRC\\_Summary\\_PF.pdf](http://www.royalcommission.vic.gov.au/finaldocuments/summary/PF/VBRC_Summary_PF.pdf)
- Wikipedia. 2001. Howard Street Tunnel Fire, [cited February 2014]. Available from [http://en.wikipedia.org/wiki/Howard\\_Street\\_Tunnel\\_fire](http://en.wikipedia.org/wiki/Howard_Street_Tunnel_fire)

# How the Internet of Things Changes Everything

## The next stage of the digital revolution

---

Kate Carruthers

UNSW Australia

---

### Summary: The Digital Revolution Continues with the Internet of Everything

In many ways the Internet of Things will change everything, as devices and software mesh and become part of the connected fabric of the Internet. This article explores the context and potential offered by the growth of the Internet of Things (IoT). It provides an overview of this next phase of the digital revolution that is underpinned by the growth of the social web, web 2.0, and the convergence of technologies such as mobile and ubiquitous broadband. This article also attempts to provide some insight into the potential value of the Internet of Things market in the future.

The opportunities offered by the Internet of Things also raise serious questions about privacy and security in a connected world. As Umair Haque noted recently: "At some point, we should all question the value of an internet that objectifies you, tracks you, and polices you...without your consent." (Haque 2014)

### Where we started – Web 1.0 and Web 2.0

The first generation of the digital revolution was about democratisation of communication, and it culminated in Web 2.0 with the development of the social web as exemplified by applications like Facebook and Twitter.

Over a number of years Web 2.0 evolved to be founded on (Dawson 2007):

1. Participation
2. Standards
3. Decentralisation
4. Openness
5. Modularity
6. User control
7. Identity

The combination of a reasonably sound standards framework for web protocols and application programming languages, along with cultural practices such as openness, meant that consumers were fairly well protected in the Web 2.0 world. However, issues of privacy and security were only at a rudimentary stage in the Web 2.0 world.

In the Web 2.0 landscape the average person could understand issues such as privacy and security. Governments were able to legislate to protect consumers and business regulation remained effective to protect people. Financial standards such as the Payment Card Industry Data Security Standard (PCI DSS) provided security for credit card transactions and card providers offered consumer protection for online transactions.

## Changes on the horizon with the Internet of Things

The digital revolution continues with the Internet of Things (IoT). Objects that were once inanimate are now embedded with sensors and accelerometers, thus gaining the ability to communicate. Initially proposed by Kevin Ashton in 1999 ([Ashton 2009](#)), the Internet of Things (IoT) refers to identifiable objects and their virtual representation in a web like structure. Thus devices are becoming empowered by software, sensors and networking capabilities to create new information networks. The resulting information networks are creating new business models that are starting to disrupt existing business models.

A key feature of Internet of Things devices is their potential to transform a device from a single-purchase item into a service that generates recurring income. Internet of Things value is not in the devices, but in the new services related to the devices. The connectedness of Internet of Things devices is critical and relies upon mature, well-defined and well-understood wireless communications protocols such as WiFi, ZigBee and Bluetooth ([Lee et al. 2007](#)). In the Internet of Things context these technologies are supported by 4G LTE, software defined networks, and APIs.

Objects are becoming embedded with sensors and gaining the ability to operate and communicate independently of human intervention. This ability for objects to act autonomously is the key differentiator to previous incarnations of the Internet. This next generation of the Internet is being referred to as the "Internet of Things" (IoT), or "Machine to Machine" (M2M), or "Internet of Everything" (IoE).

In the Internet of Things world computing power tends to be distributed, reducing reliance on centralised platforms. Devices are able to connect via traditional commercial networks as well as using peer-to-peer connectivity that bypasses traditional regulated networks. Connections between devices are API based and allow many-to-many connections via well-defined APIs, thus reducing development overhead. And many of the applications are

network neutral – that is they do not care which network they use for communications as long as it is available; for example they can seamlessly switch between 4G LTE, Wi-Fi or Bluetooth networks.

## Internet of Things driven by convergence

### Technology Convergence

The Internet of Things is driven by the convergence of a number of technologies, and it is this convergence that gives rise to the possibilities for new business models and for new ways of enabling devices to interconnect and operate in more sophisticated ways.

Ubiquitous communications networks mean that sensor-equipped devices can be deployed in many locations that were impossible in the past. Mobile connectivity enables deployment of field devices into environments that have previously not been possible, for example devices and applications in agriculture can now be deployed using commodity technology at reasonable cost.

3D printing will enable the re-engineering of existing supply chains in novel ways. Over the next decade 3D printing is likely to shift manufacturing away from traditional factories and to enable true just-in-time production.

Sensor networks will enable devices to assess their environment and to act autonomously in response to environmental stimuli; they will also be able to direct other devices to act in response to their sensor data. There are already Internet of Things devices capable directing other devices autonomously based on sensor-derived data. With the vast amounts of data being generated by the Internet of Things devices this enables the use of big data tools and techniques to draw useful inferences and to drive new activity. The feedback loops made possible by big data will have the capacity to fuel innovation in Internet of Things.

Peer-to-peer networks provide an alternative and low cost connection mechanism for Internet of Things devices. For example, it will not be necessary to connect every device in an agricultural application to a mobile phone network to collect data. Instead the devices will be able to connect peer-to-peer and collect data for transmission by a mobile connection hub. Cloud computing provides the scalable application hosting and data storage environments for the Internet of Things. The distributed nature of Internet of Things devices, and the vast amounts of data that will be generated by these sensor-enabled devices, requires scalable and relatively cheap storage. With the evolution of cloud computing and storage solutions such as Amazon AWS and Microsoft Azure this becomes accessible for new entrants such as startups, and reduces operational costs for larger organisations.

The combination of artificial intelligence, commodity sensors and software-defined networks means that devices will be able to operate autonomously. Further, it means that the

supporting software-defined networks will be able to re-route data in response to environmental factors informed by sensor data and enabled by artificial intelligence algorithms.

## Powered by APIs

The application ecosystem has been made possible by the evolution of API driven connectivity. APIs, or Application Programming Interfaces, have evolved from the web 2.0 phase of the Internet to act as the glue between diverse and often unrelated systems and applications. An API is a set of standardised pre-defined ways that have been defined for connecting to the program. This enables software developers to publish their API to enable external applications and systems to interact with their software. APIs became prevalent during the growth of the social web in the period from 2004 and are an important enabler of connectivity between devices in the Internet of Things.

## Fuelled by the application ecosystem

The Internet of Things will be powered by software applications or applications. We have already seen a proliferation in applications for smart phones and tablets; there is no reason to assume that this will reduce.

*"Between 2008 and 2017, Google Play and Apple's App Store will be responsible for a mind-blowing number of mobile app downloads: 350 billion." (Essany 2012)*

On the software development or application development side of the Internet of Things market, a recent global survey of 1,400 software developers (Evans Data 2014) indicated that 17.1% of those surveyed are currently working on Internet of Things applications, and that 23% of those surveyed expect to begin work on them in the next six months. This means that there will be a substantial supply of applications and application developers to fuel development of the Internet of Things ecosystem.

This application ecosystem will be enabled by APIs and supported by the emerging standards landscape. These standards help to define how software, systems and devices can interact with each other. It is still early days from an Internet of Things standards perspective and there are a number of competing standards emerging, for example:

- Industrial Internet Consortium
- AllJoyn
- WebRTC
- Z-Wave Alliance
- Zigbee Alliance
- Open Interconnect Consortium
- Thread
- Internet of Things Consortium

Based upon the experience of the emergence of standards in earlier generations of the Internet it is likely take several years for the standards landscape to settle down and for the winners to emerge.

## New Business Models for the Internet of Things

An important feature that changes business models for hardware and devices is that Internet of Things connected devices are transformed from a single-purchase product into a service that generates recurring income. Thus much of the Internet of Things value is not in the devices, but in new services related to the devices. This change in the ability to monetise hardware and related ongoing services means that revenue and competition in the Internet of Things space will be active.

### Characteristics of the new business models

The Internet of Things lends itself to open source models, and it enables businesses to use collaboration and loose confederations rather than deep vertical integration. Agile, change-ready organisations will be able to capitalise on developing new applications and services within the Internet of Things.

The devices that form the Internet of Things are connected devices, and these connected devices are typically being controlled via smart phones or tablets and applications (also known as apps). We are seeing an explosion in applications and this is likely to continue to be driven strongly by the Internet of Things:

*"Between 2008 and 2017, Google Play and Apple's Apps Store will be responsible for a mind-blowing number of mobile app downloads: 350 billion."*  
([MacQueen 2012](#))

These Internet of Things applications will collect vast amounts of personal data from their users, and typically store this information in a cloud-hosting environment. Third parties who do not have a direct business relationship with the user whose data is stored often provide those cloud-hosting services. This, along with the proliferation of data being captured and stored by Internet of Things devices, means that privacy and security will emerge as key business concerns on a scale not yet seen.

### Value of the Internet of Things Market

The profits that business leaders are predicting in relation to Internet of Things are enormous:

*"The Internet of Things, I think will be the biggest leverage point for IT for the next 10 years, \$14 trillion in profits from that one concept alone."* ([Chambers 2013](#))

And, while Cisco research estimates that there is US \$14 trillion value in the Internet of Things market ([Cisco 2013](#)), they also break it down thus:

- 1) Asset utilisation (reduced costs) of \$2.5 trillion
- 2) Employee productivity (greater labour efficiencies) of \$2.5 trillion
- 3) Supply chain and logistics (eliminating waste) of \$2.7 trillion
- 4) Customer experience (addition of more customers) of \$3.7 trillion
- 5) Innovation (reducing time to market) of \$3.0 trillion

In addition to these kinds of estimates of market value, mergers and acquisitions provide a useful insight into the state of the Internet of Things market. Some recent Internet of Things acquisitions include:

- Google bought Nest for US \$3.2 billion in January 2014 ([Panzarino 2014](#))
- Google and Nest bought Dropcam for US \$555 million ([Kumparak 2014a](#))
- Samsung bought SmartThings for US \$200 million ([Kumparak 2014b](#))
- Vodafone bought Cobra Automotive for £115 million ([Vodafone 2014](#))
- Zebra Technologies bought a unit of Motorola for US \$3.45 billion ([Crowley 2014](#))

With acquisitions like this it is clear that existing business leaders are positioning themselves to be significant players in the Internet of Things market.

## Pervasive computing, the Internet of Things and security

Internet of Things devices are pervading every area of modern life. Wearable devices collect and transmit data about our daily habits. With the increasing prevalence of devices like Google Glass, that record and transmit everyday life, or the dashboard cameras proliferating in vehicles, we are seeing increasing personal data being tracked and stored. Home and portable devices also track our media consumption, with much of the data being recorded and stored with cloud services. This tracking and storage of usage data for Internet of Things devices and applications enables the use of big data to mine the data and determine useful insights into consumer behaviour.

Other trends that are converging with Internet of Things will power the ability to monitor user activity. Among these trends is big data, the ability to mine extremely large data sets for insights about users. Even metadata analysis provides enormous amounts of information about individual user's life. Cloud storage is another key technology that enables Internet of Things. However, cloud and device data remains vulnerable to improper access, as the recent iCloud hack demonstrates ([Pauli 2014](#)). When even large companies like Apple are unable to effectively keep user data secure, this raises concerns about smaller startups that provide similar cloud-based services.

Much of the Internet of Things device and application data is not well secured, and users do not understand the plethora of details that are stored and transmitted about them. A good example of this is the data embedded in a tweet ([Perez 2014](#)), which reveals much more about the user than a mere 140-character message. Or the vast amount of data embedded in the images that users share so readily on social media, as shown by the *I Know Where your Cat Lives* project ([Mundy 2014](#)).

The issues that have been with us since the early days of the Internet remain – these include privacy, user control over their own data, and security. However, now due to the scale of personal data that is being collected, stored, and transmitted, these issues have increased in importance. International regulation and standards need to be addressed in a coherent and focused way. At present, Internet of Things is a bit like the Wild West.

Earlier in 2014 a family found that their home baby monitor device had been hacked ([Lee 2014](#)) and someone was yelling abuse at their baby. This is a good example of the risks of unsecured Internet of Things devices being installed in homes by users. Typically users will not consider the security implications of installing Internet of Things devices on their home networks. The question of how can users be educated about the risks inherent in these devices remains to be addressed. Further, device manufacturers and software developers have yet to recognise the issues of security and privacy that they must address in relation to the Internet of Things.

The Internet remains inherently insecure. Every week we see another bank or major retailer suffer a hack or security attack ([Collins 2014](#)). Further, recent revelations of the Shellshock and Heartbleed vulnerabilities show that some of the fundamental building blocks of the Internet remain a risk factor. This means that the Internet of Things is being constructed on the already insecure foundation of the existing Internet.

The 2014 Target attack is instructive of the kind of security problems the Internet faces. The attack vector for Target was an external third-party HVAC supplier who had access to their internal network. Existing regulations like PCI DSS did not protect them. Another good example is the recent JP Morgan hack ([Bloomberg 2014](#)); JP Morgan is protected by an inordinate amount of regulation, as are all banks, but still was hacked. Following is a summary of the existing legislation to which JP Morgan is subject to the following regulation:

- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Gramm-Leach-Bliley Act (GLB) Act
- Electronic Fund Transfer Act, Regulation E (EFTA)

- Free and Secure Trade Program (FAST)
- Fair and Accurate Credit Transaction Act (FACTA), including Red Flags Rule
- Federal Rules of Civil Procedure (FRCP)

The plethora of existing regulation did not protect JP Morgan or their consumers. The real question remains as to how to best protect people and organisations in this changing technical landscape. The solutions are likely to be a combination of effective standards, good business security practice and culture, and the application of appropriate security technology.

## Security within the Internet of Things

If even banks are not safe then in what ways can Internet of Things users and regulators ensure that protection is in place? Traditional security approaches relied upon setting up a secure perimeter that was guarded by firewalls and similar technologies. But how does one put a perimeter defence around the Internet of Things?

We have already seen several successful attacks that launched DDoS attacks from dryers, refrigerators, and other Internet of Things devices ([Greene 2014](#)).

*“The global attack campaign involved more than 750,000 malicious email communications coming from more than 100,000 everyday consumer gadgets such as home-networking routers, connected multi-media centers, televisions and at least one refrigerator”* ([Proofpoint 2014](#))

And, as Bruce Schneier points out it is

*“...often impossible to patch the software or upgrade the components to the latest version. Often, the complete source code isn't available. Yes, they'll have the source code to Linux and any other open-source components. But many of the device drivers and other components are just 'binary blobs' - no source code at all. That's the most pernicious part of the problem: No one can possibly patch code that's just binary.”* ([Schneier 2014](#))

This inability to make security patches to many existing devices on the Internet is a great challenge, and now we are adding a new layer of Internet of Things devices that are also difficult to patch. It has already been reported that Wi-Fi enabled light bulbs can be hacked and are unable to have security patches applied.

With the growth in connected medical devices the threat of malware becomes an existential one. Rather than merely stealing data the malware could actually harm a human being.

Security is the next 'big thing' that needs to be resolved for the Internet of Things. It is important to ensure that private information remains private and that malware is unable to access critical devices.

## Consumer privacy and consent

Consumer privacy faces new challenges in this age of truly pervasive computing. The very services that enable personalisation and customisation of applications and devices also require the collection and storage of personal data.

Users can be tempted to trade convenience for their data, as evidenced by the popularity of Facebook and its personal data fuelled revenue model. Users often do not understand the privacy implications of their agreement to use various software and devices.

It is not always possible to ensure that a meaningful consent can be obtained in an Internet of Things context. For example, one might question how the user of a connected motor vehicle can understand and give consent in respect of the data that their car is now collecting and reporting. A good recent example of the London agreement ([Bajekal 2014](#)) that required users to agree to give their first-born children in return for free Wi-Fi access.

From a regulatory perspective the proposed solution to this issue is 'privacy by design' ([Privacy by Design 2014](#)). However, it is unlikely that cottage industry of application developers working in bootstrapped startups around the world will ever hear about this notion.

## Internet of Things and the Future

*"We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run." - Amara's law ([Amara, undated](#))*

The impact of the convergence of various technologies – such as big data, 3D printing, autonomous sensor networks, software defined networks, etc. – into the Internet of Things will go through the standard technology hype cycle ([Gartner 2014](#)). In the long term it is hard to predict where these new technologies will lead us. However, it is unlikely that anyone can stop the changes in computing and business models that are enabled by the Internet of Things.

The most interesting developments in the Internet of Things are likely to happen at the interstices between the API ecosystem and other emerging technologies, such as 3D printing and remote sensor networks. Yet many of these emerging technologies face some 'wicked problems' ([Rittel & Webber 1973](#)) before they are ready for general commercial adoption. For example, self-driving or autonomous cars seem to be an obvious new product in the Internet

of Things. However, some of the technical challenges in getting them ready for the public roads mean they will not be viable in the short term (Ross 2014). Instead, autonomous vehicles may proliferate in closed or controlled environments like mining sites well before they appear on our public roads (Diss 2014). Therefore the Internet of Things will not be just a consumer phenomenon; it will enable a significant change in the way industrial work is done as well.

What is absolutely clear about the future of this market is that both large companies, like Cisco or GE, and startups see the future of the Internet of Things as critical to growth. The possibilities inherent in the Internet of Things are encouraging large players to cooperate so as to share competitive advantage across industry sectors. The recently announced deal between GE, Verizon, Cisco and Intel is an example (Dignan 2014) of this phenomenon. The Internet of Things is the next stage in the digital revolution that is reshaping our world and we can expect to see it drive changes in the way we socialise, work, and consume media and other products.

## References

Amara, Roy. 'Amara's Law, [http://en.wikipedia.org/wiki/Roy\\_Amara](http://en.wikipedia.org/wiki/Roy_Amara); accessed 14 October 2014

Ashton, Kevin. 2009. 'That 'Internet of Things' Thing: In the real world, things matter more than ideas.' *RFID Journal*, 22 June 2009. Available at: <http://www.rfidjournal.com/articles/view?4986>; accessed 14 October 2014

Bajekal, Naina. 2014. 'Londoners Unwittingly Exchange First Born Children For Free Wi-Fi', *Time*, September 29, 2014. Available at: <http://time.com/3445092/free-wifi-first-born-children/>; accessed 4 October 2014

Chambers, John, Cisco Chief Executive Officer. 2013. 'All Things D Conference interview', May 2013. Available at: <http://allthingsd.com/20130529/ciscos-john-chambers-and-boxs-aaron-levie-the-full-d11-interview-video/>; accessed 31/8/2014

CISCO. 2013. White paper 'Embracing the Internet of Everything for your Share of \$14 trillion'. Available at: [http://www.cisco.com/web/about/ac79/docs/innov/loE\\_Economy.pdf](http://www.cisco.com/web/about/ac79/docs/innov/loE_Economy.pdf); accessed 14 October 2014

Collins, Keith. 2014. 'Data Breaches in the US', *Bloomberg* 4 September 2014. Available at: <http://www.bloomberg.com/infographics/2014-08-21/top-data-breaches.html>; accessed 4 Sep 2014

- Crowley, Amy-jo. 2014. 'Why Zebra's buyout of Motorola's enterprise business will fuel IoT growth', *CBR Online*, 17 April 2014. Available at: <http://www.cbronline.com/news/tech/networks/networking/why-zebras-buyout-of-motorolas-enterprise-business-will-fuel-iot-growth-4216325>; accessed 14 October 2014
- Dawson, Ross. 2007. 'Launching the Web 2.0 Framework', May 30, 2007. Available at: [http://rossdawsonblog.com/weblog/archives/2007/05/launching\\_the\\_w.html](http://rossdawsonblog.com/weblog/archives/2007/05/launching_the_w.html) ; accessed 31 August 2014
- Dignan, Larry. 2014. 'GE, forges Internet of things alliances with Verizon, Cisco, Intel', *ZDNet*, 9 October 2014. Available at: <http://www.zdnet.com/article/ge-forges-internet-of-things-alliances-with-verizon-cisco-intel/>; accessed 14 October 2014-12-07
- Diss, Kathryn. 2014. 'Robotic trucks taking over Pilbara mining operations in shift to automation', *ABC*, 26 April 2014. Available at: <http://www.abc.net.au/news/2014-04-25/computer-controlled-trucks-taking-over-in-pilbara-mining-wa/5412642>; accessed 14 October 2014
- Bloomberg. 2014. Editorial. 'Why the JP Morgan hack is scary' *Bloomberg*, 6 October 2014. Available at: <http://www.bloombergtv.com/articles/2014-10-06/why-the-jpmorgan-hack-is-scary>; accessed 14 October 2014
- Essany, Michael. 2012. 'The Decade of 350 billion app downloads', *Mobile Marketing Watch*, November 19, 2012. Available at: <http://www.mobilemarketingwatch.com/the-decade-of-350-billion-app-downloads-26932/>
- Evans Data Corporation. 2014. Survey, July 2014. Available at: <http://www.evansdata.com/press/viewRelease.php?pressID=212>; accessed 4 October 2014
- Gartner. 2014. Gartner Hype Cycle. Available at: <http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp>; accessed 14 October 2014
- Greene, Tim. 2014. 'Bot Herders Launch DDoS attacks using IoT Devices', *Network World*, 24 September 2014. Available at: <http://www.networkworld.com/article/2687169/security0/bot-herders-can-launch-ddos-attacks-from-dryers-refrigerators-other-internet-of-things-devices.html>; accessed 14 October 2014
- Haque, Umair. 2014. Twitter 2 September 2014. <https://twitter.com/umairh/status/506546721007370240>; accessed 2/9/2014

- Lee, Jin-Shyan; Su, Yu-Wei; Shen, Chung-Chou. 2007. "A Comparative Study of Wireless Protocols: Bluetooth, U WB, ZigBee, and Wi-Fi," Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE, vol., no., pp.46, 51, 5-8 Nov. 2007 doi: 10.1109/IECON.2007.4460126. Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4460126&isnumber=4459874>; accessed 4 October 2014
- Kumparak, Greg. 2014a. 'Google and Nest Acquire Dropcam', *TechCrunch* 20 June 2014. Available at: <http://techcrunch.com/2014/06/20/google-and-nest-acquire-dropcam-for-555-million/>; accessed 14 October 2014
- Kumparak, Greg. 2014b. 'SmartThings acquired by Samsung', *TechCrunch* 14 August 2014. Available at: <http://techcrunch.com/2014/08/14/smartthings-acquired-by-samsung-for-around-200-million/>; accessed 14 October 2014
- Lee, Adriana. 2014. 'Another connected home hack emphasizes the need for stronger passwords', *Read Write Web*, 30 April 2014. Available at: <http://readwrite.com/2014/04/30/connected-home-hackers-stop-yelling-at-babies-foscam#feed=/tag/internet-of-things&awesm=~oEe6yipkTkz40o>; accessed 14 October 2014
- MacQueen. David. 2012. 'App Download Forecast 2008 – 2017', November 08 2012. Available at: <http://www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&a0=7934>; accessed 31/8/2014
- Mundy, Owen. 2014. Online project, I Know Where Your Cat Lives. Available at: <http://iknowwhereyourcatlives.com/about/>; accessed 31 August 2014
- Panzarino, Matthew. 2014. 'Google just bought connected device company Nest', *TechCrunch* 13 January 2014. Available at: <http://techcrunch.com/2014/01/13/google-just-bought-connected-device-company-nest-for-3-2b-in-cash/>; accessed 14 October 2014
- Pauli, Darren. 2014. 'JLaw, Kate Upton exposed in celeb nude pics hack: 100 women victimised as Apple iCloud accounts reportedly popped', *The Register*, 31 Aug 2014. Available at: [http://www.theregister.co.uk/2014/08/31/jlaw\\_upton\\_caught\\_in\\_celeb\\_nude\\_pics\\_hack/](http://www.theregister.co.uk/2014/08/31/jlaw_upton_caught_in_celeb_nude_pics_hack/); accessed 31/8/2014

- Perez, Sarah. 2010. 'This is What a Tweet Looks Like', April 19, 2010, *ReadWrite*. Available at: [http://readwrite.com/2010/04/19/this\\_is\\_what\\_a\\_tweet\\_looks\\_like](http://readwrite.com/2010/04/19/this_is_what_a_tweet_looks_like); accessed 31/8/2014
- Privacy by Design. 2014. Available at: <http://www.futureofprivacy.org/privacy-by-design/>; accessed 14 October 2014
- Proofpoint. 2014. Media Release, 'Proofpoint Uncovers Internet of Things (IoT) Cyber attack', January 16, 2014. Available at: <http://investors.proofpoint.com/releasedetail.cfm?ReleaseID=819799>; accessed 14 October 2014
- Rittel, Horst W. J; Webber, Melvin M. 1973. 'Dilemmas in a General Theory of Planning', *Policy Sciences* 4: 155–169, 1973. Available at: <http://link.springer.com/article/10.1007%2FBF01405730>; accessed 14 October 2014
- Ross, Philip E. 2014. 'Self-Driving Cars Face Serious Roadblocks, Experts Say', *IEEE Spectrum*, 10 September 2014. Available at: <http://spectrum.ieee.org/cars-that-think/transportation/self-driving/future-of-self-driving-cars-detroit-panel>; accessed 14 October 2014
- Schneier, Bruce . 2014. The Internet of Things Is Wildly Insecure - And Often Unpatchable, *Wired*, Jan 2014; accessed 10 October 2014
- Vodafone. 2014. Media release, 'Vodafone completes acquisition of Cobra Automotive Technologies', Vodafone 8 August 2014. Available at: [https://m2m.vodafone.com/cs/m2m/insight\\_news/2014-06-18-vodafone-completes-acquisition-of-cobra-automotive-technologies](https://m2m.vodafone.com/cs/m2m/insight_news/2014-06-18-vodafone-completes-acquisition-of-cobra-automotive-technologies); accessed 14 October 2014

# Enabling Technologies for Effective Deployment of Internet of Things (IoT) Systems: A Communication Networking Perspective

---

Jamil Y. Khan

Dong Chen

Oliver Hulin

School of Electrical Engineering & Computer Science  
The University of Newcastle

---

**Summary:** The demand for IoT (Internet of Things) systems that encompass cloud computing, the multitude of low power sensing and data collection electronic devices and distributed communications architecture is increasing at an exponential pace. With increasing interests from different industrial, business and social groups, in the near future it will be necessary to support massive deployment of diverse IoT systems in different geographical areas. Large scale deployment of IoT systems will introduce challenging problems for the communication designers, as the networking is one of the key enabling technologies for the IoT systems. Major challenges include cost effective network architecture, support of large area of coverage and diverse QoS (Quality of Service) requirements, reliability, spectrum requirements, energy requirements, and many other related issues.

The paper initially reviews different classes of IoT applications and their communication requirements. Following the review, different communications and networking technologies that can potentially support large scale deployment of IoT systems for different industrial, business and social applications are discussed. The paper then concentrates on wireless networking technologies for IoT systems with specific focus on deployment issues. The deployment discussion concentrates on different IoT systems QoS and networking requirements, cost, coverage area and energy supply requirements. We introduce a sustainable low cost heterogeneous network design using short range radio standards such as IEEE 802.15.4/Zigbee, IEEE 802.11/WLAN that can be used to develop wide area networks to support large number of IoT devices for various applications. Finally the paper makes some general recommendations towards sustainable network design techniques for future IoT systems that can reduce the OPEX and CAPEX requirements.

## I. Introduction

The Internet of Things (IoT) concept introduces a new and ubiquitous computing, and communication paradigm where smart objects can exchange information to support intelligent applications in an autonomous manner. Without human intervention, smart objects located in various application domains could interact with each other to accomplish

many tasks, ranging from health care to a simple ON/OFF activity of a light bulb. According to the Institute of Network cultures, an IoT is defined as *"a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols, where physical and virtual 'Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network"* (Atzori 2010: 2787-2805), (Xu et al 2014).

Advances in the semiconductor, computing and communication techniques have empowered embedded wireless computing to support evolutionary new networking architecture that could meet IoT requirements in a seamless manner. It is now evident that in future IoT applications will be deployed in almost all segments of the modern society and industry to carry out a wide range of activities. Hence, it is critical to change the fabric of the key communication infrastructure of the Internet to enable seamless communication among the intelligent devices. Such changes will be a paradigm shift from human-to-human communication towards intelligent machine-to-machine communication. The conventional concept of the Internet as an infrastructure network reaching out to end-user terminals will fade, giving rise to an interconnected scenario where smart objects will use pervasive computing environments (Jin et al 2014: 112-121). IoT applications will spread in many existing and new ICT (Information and Communications Technology) areas including those where the Internet has not yet reached. The application requirements will therefore significantly diversify, requiring embedded intelligent network architecture.

The IoT concept introduces a major shift in ICT areas where, instead of connecting end-user devices, the physical objects will connect with one another and interact with anything. The concept of interconnected objects was developed from the deployment of RFID (Radio Frequency Identification Device) for automatically identifying and tracking objects. The idea was supported with the emergence of wireless sensor networks in the mid to late 1990's where advanced monitoring applications emerged (Miorandi et al 2012: 1497-1516). Embedded computing and low power wireless communication devices efficiently support connectivity among intelligent objects. Recently, the concept of IoT has further advanced into the Internet of Nano Things (IoNT) (Akyildiz & Jornet 2010: 58-63), (Balasubramaniam & Kangasharju 2013: 62-68). The IoNT concept has been labelled as systems where miniature, possibly passive sensors in some cases, interconnected through nano-networks could obtain fine grain data from hard-to-access locations such as the human body or inside complex machines. Some of the leading ICT companies such as Cisco, IBM are now pushing the boundary of the IoT to call the area as the IoE (Internet of Everything), which is a further generalisation of the IoT concept.

Application domains of the IoT or the IoNT are not limited by current-day applications only; they will evolve as the enabling support infrastructure improves. The IoT will be an enabler to many application domains, including supply chain management, transport and logistics, manufacturing, aerospace and automotive, healthcare, security and safety, social services, etc. According to analysts, 50 to 100 billion devices will be connected by the Internet by the year 2020 (Mobile world). The global market for sensors is expected to increase to US\$91.5 billion by 2016, representing a compound annual growth rate of 7.8% ([Zaslavsky 2013](#)). The IoT application domains will come in different sizes and shapes that generate small to massive amount of data. For example, a Boeing jet could generate 10 TB (terabytes) of data per engine every 30 minutes. In an aircraft, although the physical size of a network could be small, the number of data generators could be massive.

On the other hand, a smart electricity grid system may cover a very large geographical area (distribution area), but the sensor density and data volume may not be as high as that in an aircraft network. This necessitates the development of enabling technologies to support such future systems. One of the key enabling technologies of the IoT is the communication network that allows flows of information among different entities ([Kim et al 2014: 61-76](#)). This paper focuses on the design of communication networks for future IoT systems that could be deployed in different industrial and social sectors.

The paper is structured in the following manner:

- Section II reviews several major IoT applications and their deployment scenarios to develop the design needs for communication networks.
- Section III reviews different possible communication network structures based on current and emerging standards for various IoT systems.
- Section IV presents a low cost heterogeneous network for distributed IoT applications. This section also discusses the energy requirements for the IoT communication networks and present a new heterogeneous networking algorithm and firmware design.
- Section V presents some simulation and test bed measurement results for IoT communication systems.
- Finally, conclusions are presented in section VI.

## II. IoT Applications and Systems

In 1999 Kevin Ashton first proposed the concept of the Internet of Things (IoT) that quickly gained popularity among researchers and various technical forums ([Zaslavsky 2013](#)). The IoT concept came into the industrial limelight when the International Telecommunications Union (ITU) published the first report on IoT in 2005. Since then, the concept of IoT has been embraced by researchers, various standards bodies such as the Institute of Electrical & Electronic Engineers (IEEE), the European Telecommunication Standards Institute (ETSI), the Internet Engineering Task Force (IETF), the ITU and many other national and international organisations.

In recent days, many international research programs have been initiated, e.g., EU framework FP7 program, National Institute of Standards and Technology and National Science Foundation (NIST) in the USA. Rapid development of low-power electronics, communication technologies and data analytic techniques allowed widespread deployment of IoT applications and systems.

According to Gartner, a leading international Information Technology research company, the number of installed IoT connected devices will reach 26 billion by 2020, up from 0.9 billion in 2009 ([Gartner IoT 2013](#)). According to Cisco, the number of internet-connected devices has reached 8.7 billion in 2012 ([Forbes 2013](#)). Connected IoT devices are utilising the machine to machine (M2M) communication architecture for the connectivity. The first generation of IoT applications was based on the Radio Frequency Identification (RFID) technology for logistics, retail and similar other sectors. The IoT applications later integrated with cloud computing and wireless sensor network architecture. The main components of an IoT system are smart devices, distributed computing capabilities and seamless communications capabilities as shown in figure 1. A smart object can be characterised by the following attributes ([Miorandi et al 2012: 1497-1516](#)).

- It has a unique identity, which is addressable by other autonomous devices.
- The object can autonomously connect with other devices and can execute certain tasks.
- It has computing capabilities to accomplish certain tasks either in a standalone or in a cooperative manner.
- It may possess some capabilities to sense surrounding physical environments and/or phenomena or can trigger certain processes based on its sensing capabilities. The triggered processes either could reside within itself or could exist in a distributed fashion.
- Some of the objects may have to roaming capabilities supporting mobile applications.

The above general attributes could be used in different IoT applications ranging from simple applications such as sensor-based light ON/OFF to control of autonomous connected vehicles on public roads to improve the reliability of future transportation systems. Market sectors and application areas of the IoT are quite large and will expand with time. It is not possible to describe all areas; however, here we can group these applications into a number of major categories and characterise the areas in terms of their communication needs. IoT application and market sectors can be grouped into following seven categories (Atzori et al 2010: 2787-2805). Each of the categories of applications is summarily described below.

- Smart home/buildings
- Smart City
- E-Health and medical systems
- Road traffic and transportation systems
- Environmental monitoring
- Business inventory and product management
- Industrial automation and manufacturing

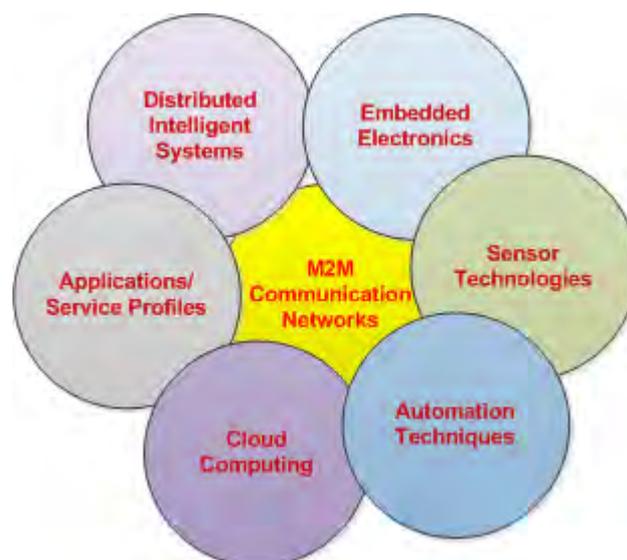


Figure 1: Basic building blocks of IoT Systems.

Smart home/buildings: IoT devices and networks could be deployed in homes and/or in large buildings. Sensor devices can be installed inside homes or buildings to implement energy efficiency, security & safety applications, appliance control using home area networks (HAN) and many other applications (Sterling & Tareter 2009: 281-326). Most of the applications are sensing and monitoring; however new applications are emerging to support network-connected devices as can be seen in a smart grid environment. Some advanced smart home appliances could use connectivity to get locally generated information from onsite renewable energy generators to schedule the operation of appliances. Most of the

applications in this environment will operate in either local area or personal area networking (LAN/PAN) environments with short transmission distance between nodes. Appliances within a HAN could use the smart meter as the gateway/router for connections to implement demand management system by exchanging data with the electricity company server.

**Smart City:** A smart-city based IoT system will encompass many utility services, where many providers could offer advanced services. This environment can be seen as a cyber-physical eco-system where advanced communication and computing infrastructure will be necessary to support services. Services in this environment could include road traffic control, parking administration, pedestrian safety; general safety & security, basic services such as electricity, water and other services management, street lighting control, etc. Smart cities could support fragmented IoT services where different service providers could have their own real infrastructure or use some form of virtual infrastructure by sharing common resources.

Applications in these environments could have multi-level QoS requirements, which may impose many restrictions on the infrastructure design. For example, some safety applications could trigger many sensors requiring low latency data transfer capabilities from its network as well as high transmission bandwidth to transmit video. Similarly an electricity grid control system may require a very low latency transmission link in case of a fault generated within a grid but may not require high transmission bandwidth.

One of the critical issues in a smart city IoT environment is also the sheer number of devices that need to be serviced. From the communication networking point of view, both traditional client server architecture and device-to-device communications support needs to be provided. The smart-city IoT environment could be quite complex; particularly because in future it may be possible to provide many civic facilities in connected modes. For example, various government agencies and companies in the USA and other countries are contemplating the development of connected car systems which may reduce city parking space requirements by transport movements based on the commuter's requirements rather than where currently commuters plan their tasks based on transport schedules. This could be a huge growth area that requires significant research and development effort to develop new infrastructure.

Another significant area within a smart city is the security and surveillance system. IoT enabled devices could significantly enhance the current network of security cameras to track down intruders or offenders. Networked security sensors and automated cameras could work out the movement paths of intruders enabling security services to act more quickly. For example, expensive items could be tagged with active radio transmitters that could emit signature signals while stolen goods are being carried through the mesh of sensors located in

buildings and on roads/pathways. Such IoT applications could be part of future municipal or city networks. A smart city network needs to be implemented based on advanced heterogeneous network architecture.

It is necessary to use a heterogeneous network in a smart city due to variable requirements for the likely range of applications. For example, the security applications will require short range high density sensor networks for acquiring electronic signatures but the detected information needs to be transmitted either in a unicast or in a multicast manner over a low latency long distance network to activate appropriate security measure. In this case the sensing network might comprise a Zigbee type network where the low latency long distance network could be an LTE (Long Term Evolution) wide area network (Edson et al 2014).

E-health and medical systems: This is a specialised IoT area serving aged care, indoor/outdoor patient care and ambulatory services. Aged care services could include monitoring people and helping in the diagnostic processes by providing appropriate data in a suitable manner. Use of a Wireless Body Area Network (WBAN) could significantly improve aged patient care in his/her own home or in care accommodation (Yuce & Khan 2011). WBAN devices and sensors can provide appropriate data to care providers to monitor the wellbeing of elderly persons, thus reducing the cost of care and at the same time improving the quality of the care. In other areas, medical systems could connect non-critical patients for statistics gathering from autonomous sensors to improve the quality of life of patients. Such systems require implementation of distributed systems with appropriate mobility support. In future advanced medical systems could be developed where patient monitoring devices could exchange data among themselves to control care activities such as connected drug delivery systems. Hence, e-health systems need to support personal, local and wide area type networks to implement various systems.

Road traffic and transportation systems: Road traffic systems are currently using basic ICT systems such as automatic traffic signals, online traffic monitoring, Global Positioning System (GPS) based guidance systems, public transport scheduling systems, in network control systems, etc. However, this area could immensely benefit from the application of IoT/M2M communication systems. Recently significant R&D interests have been generated in the automobile sector for connected and autonomous cars where vehicles can exchange information either among themselves or with other entities to enhance and improve route guidance systems, offer enhanced transportation services and improve pedestrian safety (Euisin et al 2014: 148-155).

In order to support the connected car environments significant research development activities have started involving the VANET (Vehicular Ad hoc Network) standards based on IEEE 802.11p and Dedicated Short Range Communication (DSRC) standards. Connected car

systems could be extended to improve total road traffic systems safety by connecting with pedestrians via their smart phones and also with train systems to avoid crashes at rail crossings. Such systems need to be totally autonomous and should be able support data exchange between different entities with a high degree of confidence. To avoid car/pedestrian collisions, Honda is now trialling VANET based collision avoidance systems in USA in conjunction with the Qualcomm ([Wu et al 2014](#)). The use of IoT based systems for the transport sector will enhance the reliability and safety of road traffic systems as well as allowing offering new modes of public transport systems. To support vehicular IoT systems it is necessary to work on vehicular industry standard based systems.

**Environmental Monitoring:** IoT systems can be used to monitor various environmental, weather and agricultural (including livestock) data in order to improve both the environment and farm productivity. Real-time information processing capabilities coupled with the ability to connect a large number of devices that communicate among them could offer an advanced platform to improve early warning systems to reduce the risks to human as well animal life. For example, interconnected sensors over a wide-area network could accurately detect fire or flood danger and inform humans about impending dangers. Current day bushfire systems generate alarms mainly from visual inspection or using satellite monitoring systems. In dense bush when a grass fire starts on the ground the smoke will not be recognised until the fire has advanced so that smoke and flames are visible or detectable from satellite. In such cases ground-based sensors could send early warnings to the nearby population using autonomous systems. Similarly mobile-connected robot based systems or fixed sensor-based systems could be used in the industrial complexes to provide necessary data in case of an accident or to monitor standard environmental data. Hence, connected systems could offer significant advantages for indoor and outdoor environmental monitoring applications.

**Business inventory and product management:** RFID technologies are significantly deployed in many business sectors for inventory management, throughout the supply and inventory management. The RFID based sensors allows the systems to identify products and provide them tracking abilities. Such RFID based systems are used in many forms, in-house to track product inventory as well as inter-site movements using local and wide area networks. For example, recently satellite based M2M systems are becoming popular for inventory and supply chain management in order to locate and monitor the movement of shipping containers across regions or a country as well as for transcontinental movements. A number of satellite M2M service providers offer advanced services that include ORBCOMM, Iridium, Globalstar, Inmarsat and few others (M2M Satellite). For future applications other type of sensors, including biosensors in combination with RFID technologies could allow

control of production processes, improving the quality of product and shelf life, and timely delivery of products.

Industrial automation and manufacturing: Applications of IoT systems in the manufacturing shop floor are in their infancy state. Many industries use sensor-based systems to control manufacturing processes based on tailor-made applications. However, some IoT applications are emerging in the mining and control engineering areas mainly for safety and monitoring applications (Xu et al 2014). Also, the emergence of cloud computing systems will increase the deployment of IoT systems on manufacturing shop floors. Communication requirements for this class of applications could vary from a PAN-sized network to a wide area distributed network.

This section provided a brief overview of different classes of IoT applications. Discussion shows that various IoT applications will require support of different class of communication networks to support their respective QoS and network coverage needs. In the following section we briefly discuss the different communication network architecture and standards to support future IoT systems.

### III. Communication Networks for Future IoT Systems

The communication network is one of the key building blocks of the IoT and cloud computing systems. As mentioned in the previous section, the IoT concept has been developed based on the M2M communication architecture. For success of IoT industries it is necessary to develop an open industry standard that is vendor-independent and can easily interwork with other functional modules. Figure 2 shows a functional model of the M2M communication network based on the ETSI (European Telecommunications Standards Institute) model (ETSI TS102 690). Figure shows that the network is divided into three layers: area, access and core networks. The *area network* is close to the IoT devices providing direct connectivity to these devices. It is generally assumed that these devices will operate at low power level, hence a network connection is necessary in the vicinity of these basic IoT devices. It is most likely that most of the IoT devices will use wireless connectivity to connect to an area network.

Next level in the network hierarchy is the *access network* that connects several area networks as well as some enhanced IoT devices to concentrate data. The access network also connects to the M2M gateway devices that concentrate many M2M functions and capabilities. Most of the M2M service capabilities and applications will be distributed over a large area connected via the core network. Communication between devices need to be offered at different levels to implement many IoT applications. For example, a sensor in an area network may activate a switch in the same or different area network. If the sensor and

switch are in the same area network then it may necessary for corresponding applications to provide device to device connectivity. Hence, new device to device and traditional client server connectivity models must be maintained within the M2M communication architecture for the IoT applications.

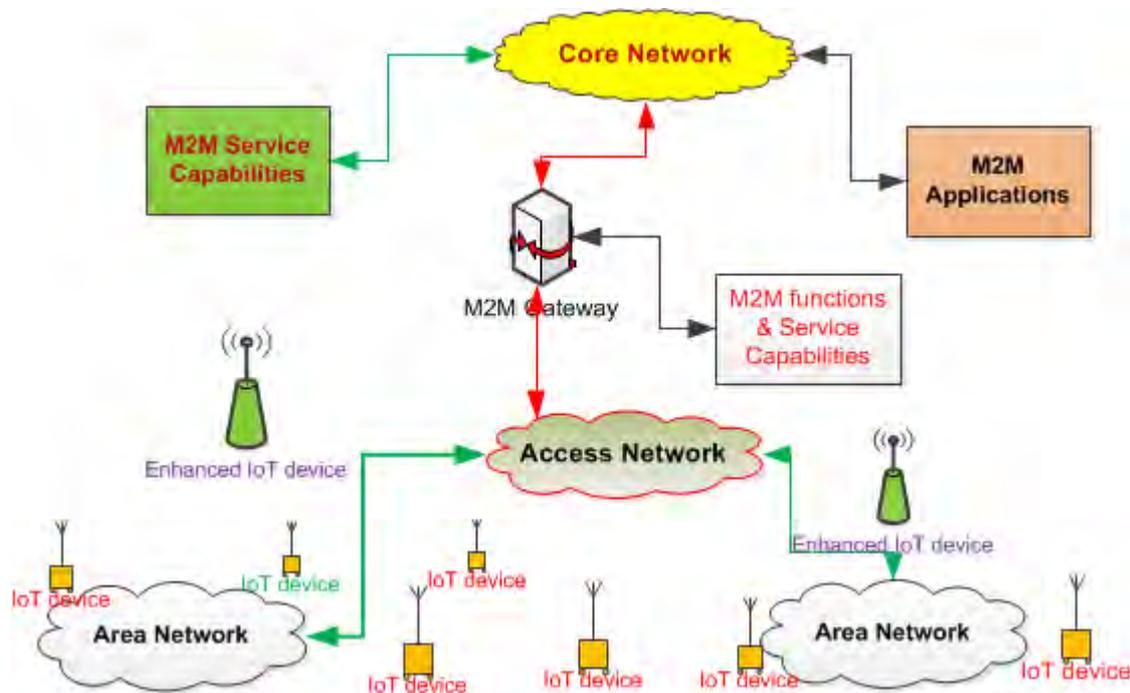


Figure 2: Machine to machine communication architecture for IoT systems based on the ETSI standard.

Considering the IoT categories discussed in Section II and the M2M communication architecture, it will be necessary to use multiple communications technologies to provide connectivity for range of IoT applications. These communication standards are broadly categorised either as wired or wireless communication systems. Wired communication systems also include fibre-based optical networks. Some of the current key communication network standards that could be used for IoT communications are listed in Table 1 (Iniewski 2010). Most of the networks are multi-service networks i.e. these networks can serve multiple types of traffic. Some of the wireless networking standards which are more appropriate for IoT applications are described later.

Table I: Summary of Communication Networking Technologies.

Network Type	Network Size	Standard	Main Features
Wired	Wide area	DSL, FTTN or FTTH	DSL: 2-20 Mbits/sec, FTTN/FTTH: 2 – 1000 Mbits/sec Both standards are infrastructure based
	Local Area	Ethernet: IEEE 802.3 family	Fast Ethernet: 10 Mbits/sec to 100 Mbits/sec Gigabit Ethernet: 1, 10, 40,100 Mbits/sec
		Homeplug: HomePNA/IEEE1901	14 Mbits/sec to 200 Mbits/sec
Wireless (Terrestrial)	Wide area	2G: GSM/GPRS/EGPRS	GPRS data rate: 56 to 114 kbits/sec, EGPRS: up to 236 kbits/sec
		3G: UMTS	Up to 2 Mbits/sec
		3.5G: HSPA, WiMAX (IEEE 802.16)	HSPA: up to 42 Mbits/sec, WiMAX: up to 70 Mbits/sec
		4G: LTE	Up to 100 Mbits/sec
	Local Area	WLAN: IEEE 802.11	2 Mbits/sec to 400 Mbits/sec
	Personal Area	Bluetooth/IEEE 802.15.1 Zigbee/IEEE 802.15.4/6LoWPAN WirelessHART/IEEE 802.15.4/IEC62591 ECMA368 (Ultra Wideband) ISA100.11a	Bluetooth: 1 to 10 Mbits/sec, IEEE 802.15.4: 250 kbits/sec ECMA368: up to 480 Mbit/sec ISA100.11a: 250 kbits/sec
Satellite	Wide area	LEO: Low Earth Orbit Satellite	160 to 2000 km height, constellation of 25 satellites (ORBCOMM), data rate upto 50 Mbits/sec

GSM: Global System for Mobile, GPRS: GSM Packet Radio System, EGPRS: Enhanced GPRS, UMTS: Universal Mobile Telecommunications System, HSPA: High Speed Packet Access, WiMAX: Worldwide Interoperability for Microwave Access, LTE: Long Term Evolution, WLAN: Wireless Local Area Network, 6LoWPAN: IPv6 Low Power Wireless Personal Area Network,

#### Basic requirements of IoT Networks:

Before developing network architecture it is important to understand basic IoT networking requirements. IoT devices and applications will generate data from various sensors and electronic devices which are generally short data bursts of a few bits to maximum of a couple

of hundred bits, generating either in a synchronous or asynchronous fashion. Most of the IoT devices operating in area networks should be operating in a low power environment so that sensor nodes battery or the energy source could last for very long time. Frequent energy source replacement could be the main impediment towards the mass deployment of these devices and applications.

In order to operate in low power environments it is necessary to provide network access to these devices in the vicinity of their deployments. Hence, it is very likely that short range wireless standards such as IEEE 802.15.4 based standards will be more frequently used in the area networks. Some area networks may also use the IEEE 802.11 based WLAN standards, particularly when longer transmission range is required. The access network will require different networking standards. Access networks could use the IEEE 802.11 WLAN standard to support enhanced IoT device support; also using a mesh network architecture can offer backbone networking capabilities to the area networks. Wide area networking standards such as GPRS, HSPA, LTE, and WiMAX etc. could also be used to connect gateways and/or sparsely distributed IoT devices.

Alternatively, it may be possible to use satellite-based systems in the access network to support remote devices or mobile devices. For example, ORBCOMM is now one of the largest M2M satellite companies offering services for supermarket chains and logistics companies worldwide. Finally, the core network within the M2M network hierarchy could be implemented using either wired or wireless based wide area networking standards or based on satellite networks.

Network design for IoT systems requires significant multi-dimensional optimisation. Instead of going through different network design techniques, in the next section we present a low cost IoT network design techniques based on the IEEE 802.15.4 and IEEE 802.11 standards.

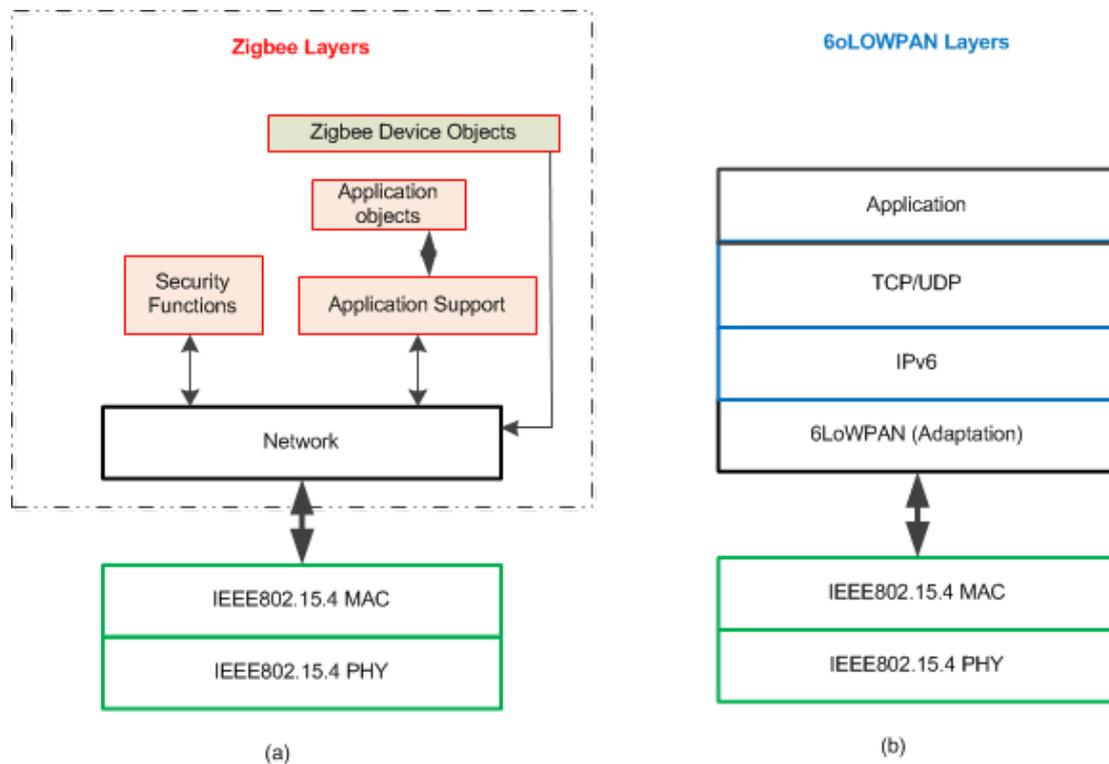
## **IV. Low Cost Heterogeneous Network Design for IoT Applications**

In recent times many low cost wireless networking standards have been developed mainly to support low data rate short-range networking applications, primarily for sensor networking applications. Most of the IoT applications can be seen either as basic or as enhanced sensor network type applications. The IEEE 802.15.4 standard that has developed the Physical layer and MAC (Medium Access Control) layers for the short range radios has now been adopted by many other organisations such as Zigbee, IETF, HART communication foundation, IEC and others, to further develop the protocol stack for different system developments.

Figures 3a and 3b show the Zigbee and 6LoWPAN protocol stacks developed on top of the basic IEEE 802.15.4 protocol stack. Figure 3 shows that Zigbee and 6LoWPAN standards

have introduced different higher layer functionalities on top of the basic 802.15.4 radios. Zigbee layers introduce networking, security and application layer functionalities whereas the 6LoWPAN protocol provides end to end IP (Internet Protocol) connectivity using higher layer protocols. The IEEE 802.15.4 standard is evolving to support various applications and operating environments. Initially the standard only supported the 2.4 GHz ISM (Instrumentation Scientific Medical) unlicensed band for the radio but recently the standard is also supporting 700/800/900 MHz band which reduces the transmission loss paving the way for lowering the transmission power, hence increasing the battery lifetime of a node/device. The IEEE 802.15.4 MAC layer use a simple random access protocol known as the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) which is similar to the MAC protocol used by the IEEE 802.11 based wireless standard.

Use of the CSMA/CA protocol reduces the network device complexities and node energy requirements if a network is properly designed. WirelessHART and ISA100.11a use the IEEE 802.15.4 physical layer but MAC layers have been modified for these standards. Based on features, cost and functionalities, the IEEE 802.15.4 based standards are ideal for IoT networking applications, particularly in the area network. Also, this standard can be combined with the IEEE 802.11 based medium to high data rate WLAN standard to implement both area and access network designs. Key features of the IEEE 802.15.4 and IEEE 802.11 standards are listed in Table 2.



(a) : Zigbee protocol stack,

(b): 6LoWPAN protocol stack.

Figure 3: Zigbee and 6LoWPAN protocol stacks built on top of the IEEE 802.15.4 layers.

Table2: Some of the key features of the IEEE 802.15.4 and IEEE 802.11 standards

Parameters	IEEE 802.15.4	IEEE 802.11
Operating frequencies	700/800/900 MHz, 2.4 GHz	2.4/5 GHz, 0.9/60 GHz in 2016
Data rates	20, 40 and 250 kbits/sec	2 Mbits to 1 Gbits/sec
MAC protocol	CSMA/CA	CSMA/CA
Transmission format	Beacon & non-beacon based	Beacon & non-beacon based
Transmission power	Up to 10 mW	Typically up to 250 mW
Transmission range	10-50 metres	Up to 300 metres
Receiver sensitivity	-85 dBm @ 2.4 GHz -92 dBm @ 800/900 MHz	-89 dBm @ 6Mbits/sec -73 dBm @ 54 Mbits/sec

In Figure 4 we propose a low cost based heterogeneous IoT city network architecture using the IEEE 802.15.4 and 802.11 standards. The area network consists of several sensor clusters, sensor nodes, traffic control systems and building IoT systems connected via relay nodes to a dual radio routers. The sensor clusters could be distributed in a city area where low power sensor nodes could be gathering various data. This area network could support device-to-device communications as well as the client/server applications via the access and the core network. Device-to-device applications can easily be supported when using the 6LoWPAN standard because each device is IP addressable. Nodes within the area network could communicate with other devices either by using cluster head nodes or by using relay nodes. A large area network could be segmented in sub-networks each served by an area router.

The design introduces a dual radio router to support network heterogeneity. The dual radio router on one side will exchange information with the 802.15.4 devices which have shorter transmission range. On other side the dual radio router will connect to mesh routers within the access network. The mesh routers could be located further away from the dual radio router. Hence we propose to use an 802.15.4 and 802.11 standard based on the dual radio router. In our laboratory we have developed the dual radio router architecture by resolving the co-existence problem which is described briefly later.

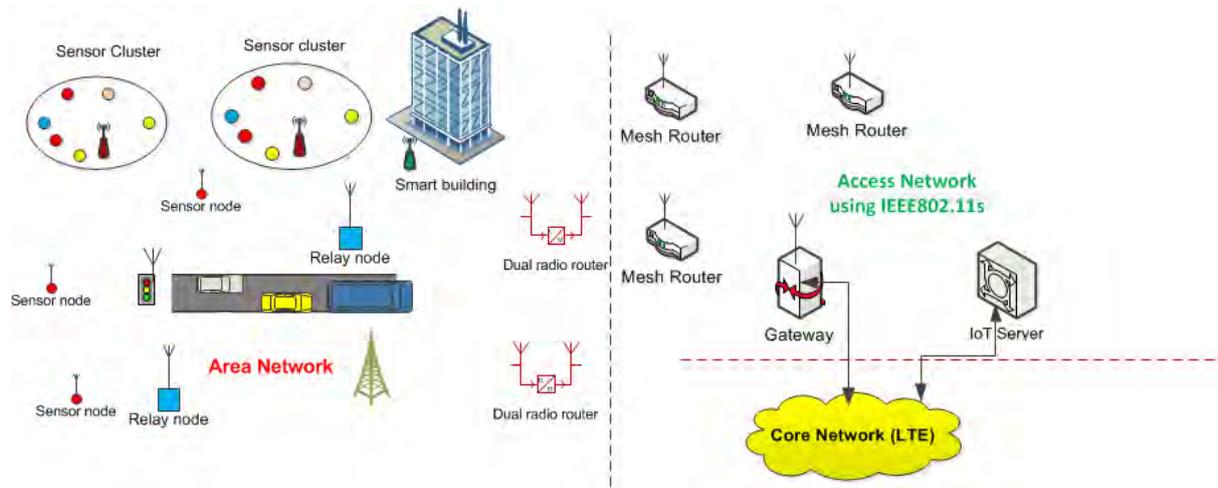


Figure 4: A heterogeneous low cost city IoT network using IEEE 802.11, IEEE 802.15.4 and LTE standards.

For a low cost IoT network we propose to use an IEEE 802.11s standard based mesh network on the access network side. The access network could connect several area networks and provide connectivity between area-to-area networks or between areas to the core network. The access network may also connect enhanced IoT devices. For a city network the core network could either be served by the 4G LTE network or it may be possible to use 3G/3.5G standards. In the core network it may be possible to use the broadband network infrastructure if an appropriate termination is available.

Short-range radio-based area network design introduces two major challenges: they are mainly deployment challenges. One of the challenges is the share of transmission spectrum by the IEEE 802.15.4 and IEEE 802.11 standards. This problem is referred as the co-existence problem and currently researchers are trying to solve the problem with minimum complexities. The other challenge is the energy supply to sensor and relay nodes which are typically battery powered. Both of the above problems are being studied at the University of Newcastle telecommunications networks research group.

To solve the first problem we have developed a new packet area scheduling technique using a control signalling system known as the *Blank Burst (BB)* (Chen et al 2014). Due to the limitations of the paper size the algorithm is not described here; the algorithm has been developed using the dual radio router protocol stack which is shown in Figure 5. This figure shows the area network interface on the left side and the access network interface on the right hand of the protocol stack. We have implemented two new layers on top of the IEEE 802.11 protocol to implement the area packet scheduler using BB control signalling. The protocol stack allows packet to flow between IEEE 802.15.4 and IEEE 802.11 networks.

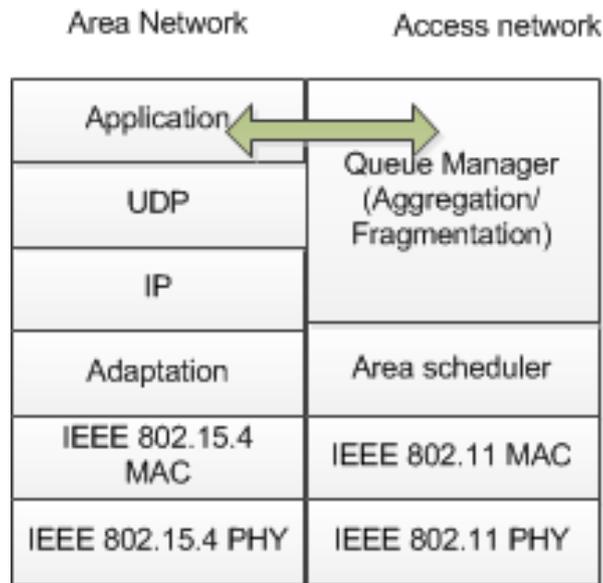


Figure 5: Dual radio router protocol stack.

## V. Simulation And Test Bed Measurement Results

Figure 6 shows the performance of an area network involving 30 sensor nodes within two clusters with one relay node and a dual radio router. An OPNET based simulation model was developed to study the performance of the area network. The figure shows the packet success rates (PSR) for three different transmission scenarios. In the first scenario (blue line) only the sensor nodes are transmitting packets where only device to device communications exist. The figure shows the PSR value for different offered loads.

In the second scenario the offered traffic is received by the dual radio router and then forwarded to the access network by using the access network interface of the router. In this case both interfaces of the dual radio router are operating at 2.4 GHz. Figure 6 shows the PSR in scenario 2 (orange line) drops due to collisions between the IEEE 802.15.4 and IEEE 802.11 devices. In order to solve the problem we introduce the BB signalling technique which is represented by the Scenario 3 simulation results (grey line). Results show that the introduction of the BB control signalling technique completely eliminates the inter-network packet collisions yielding the same PSR as the scenario 1 when the IEEE 802.11 radio was silent. Our packet scheduler enables the low cost area network to operate at very high efficiency.

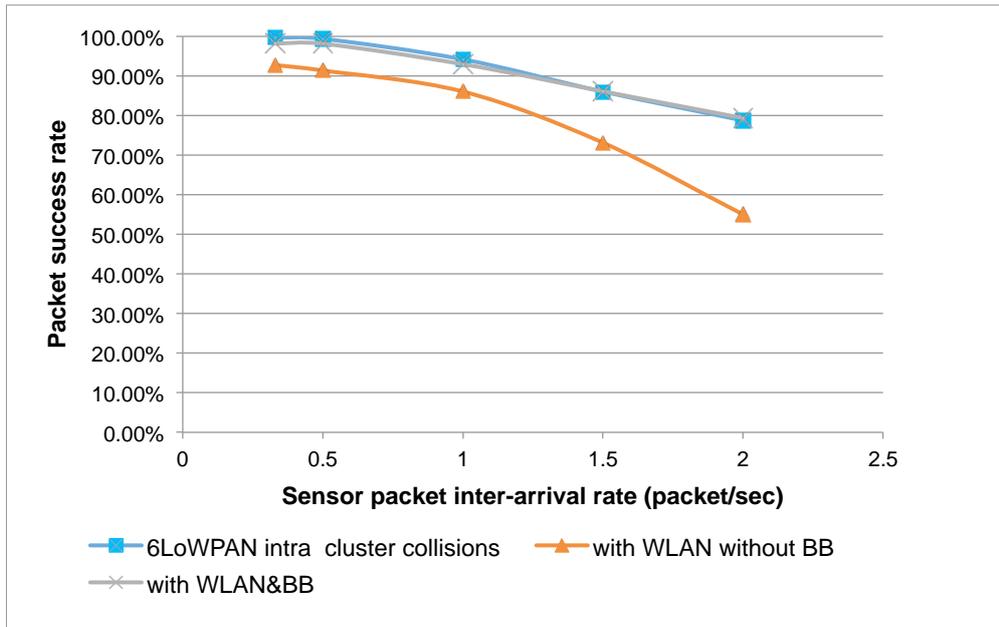


Figure 6: Packet success rate in the IEEE 802.11/IEEE 802.15.4 heterogeneous area network.

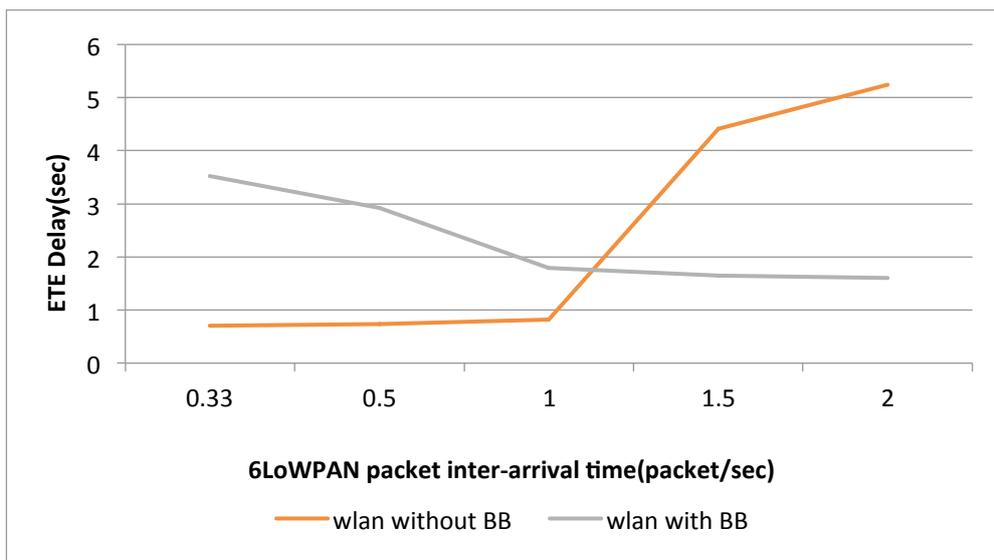


Figure 7: End-to-end delay area to access network packet transmission.

Next we examine the end-to-end delay of IoT packets transmitted from sensor nodes to the access network using the dual radio routers. Figure 7 shows the end-to-end delay for simulation scenarios 2 and 3. In scenario 2, all the received packets are directly related to the access network thus introducing minimum delay. However, the delay increases with increasing traffic due to inter-network collisions. In scenario 3, sensor data is aggregated at the dual radio router and then forwarded to the access network to reduce the signalling overhead and delay. Figure 7 shows that for low offered load the delay is higher than the scenario 2, which is due to higher aggregation delay. The aggregation delay decreases with

the traffic load. At the higher traffic load scenario 3 shows lower end to end delay due to elimination of inter-network packet collisions. Both results show that the performance of the heterogeneous access network is enhanced when the developed dual radio router is used in combination with the BB signalling technique. It is worthwhile to mention here that new IEEE 802.11 devices will also appear in the 900 MHz spectrum; hence in future the coexistence problem will exist in other frequency bands.

The next design and deployment challenge is energy availability for the sensor and router nodes in the area and also in access networks. To solve the energy issue we have developed solar powered IoT nodes and routers based on the IEEE 802.15.4 radio operating in the 900 MHz band. Figure 8 shows the developed solar IoT node which is currently used in a campus network test bed. This is a proof-of-concept design which we have developed as a part of an energy scavenging sensor network design project.

The foundation for this proof of concept node design utilises the Texas Instruments (TI) CC430F5137RF900 development board which is a small PCB (Printed Circuit Board) solution designed by TI to allow rapid prototyping and testing of sub GHz wireless sensor network projects. The node utilises the CC430 IC which combines the TI MSP430 microcontroller with a CC1101 transceiver into a single chip. The development board provides accessible I/O and is typically powered by two AAA batteries. Utilising the TI Code Composer Studio IDE a custom mesh network was implemented and programmed on to the custom sensor nodes.

To then develop this microcontroller into a deployable wireless sensor node a stackable two-layer PCB design was formulated. The first layer interfaces the CC430 I/O ports and power connections onto the custom PCB which comprises a 2 x AAA battery holder, solar charging circuitry and 8 digital and 8 ADC (Analog-to-Digital Converter) capable IO ports. The IO ports are broken out into a header allowing for rapid prototyping with sensors as developmental needs change. The initial design utilised 3V temperature and humidity sensors switched by the digital IO and read by the ADC ports. A second small PCB interconnects on top of this first layer which contains the solar panels. This creates a small form factor complete sensor node device with dimensions 90x60x25 mm (excluding external casing). The design provides a self-sustaining yet flexible wireless sensor node device capable of quick sensor installation and adjustment.

The power supply design is a simple 6V 16mA 40x50 mm solar panel connected in parallel to the batteries and microcontroller with a current-blocking protective diode. Voltage regulation is maintained by the battery voltage and CC430 on-board regulator. The panels were sized to ensure a sufficiently small charge rate would be achieved at maximum sunlight

so as not to damage the batteries over time, but also selected to allow an effective recharge rate each day, as the graphs demonstrate, for reasonable packet transmission rates.



Figure 8: Proof of concept solar IoT node.

The design was finalised with a 3D printed external casing. This allows for adjustments made in the design to allow for ventilation or sensor access depending on the specific sensor solution required. The flexible solar panel stackable design means that the solar panels can be mounted within the casing (necessitating a window to light the panels). Alternatively, and more simply, the panels can be located on the exterior of the casing with wiring fed back to the second layer PCB.

The developed IoT node was tested for the durability of the energy scavenging power supply. The IoT node was placed on a side window where direct sun light was available for about 4-5 hours/day and programmed to transmit packets to another node located about 20 metres away. The node was using 0 dBm transmission power. Figure 9 shows the node voltage profile which is supplied by two AAA batteries. The battery voltage was monitored for nine days, three days for each packet transmission rate.

Results show that the IoT nodes can operate in an uninterrupted manner when powered by solar panels even inside a room. The min/max value of the battery voltage depends on the weather. When measurements were carried out for the highest packet rate the days were perfectly sunny, whereas other days were cloudy or partially cloudy. Minimum operating voltage of this sensor node is 1.8 volts. The measurement shows that these low-power sensor nodes can operate for a very long period without changing batteries. Currently we are measuring the battery voltage by equipping several nodes with different active and passive sensors

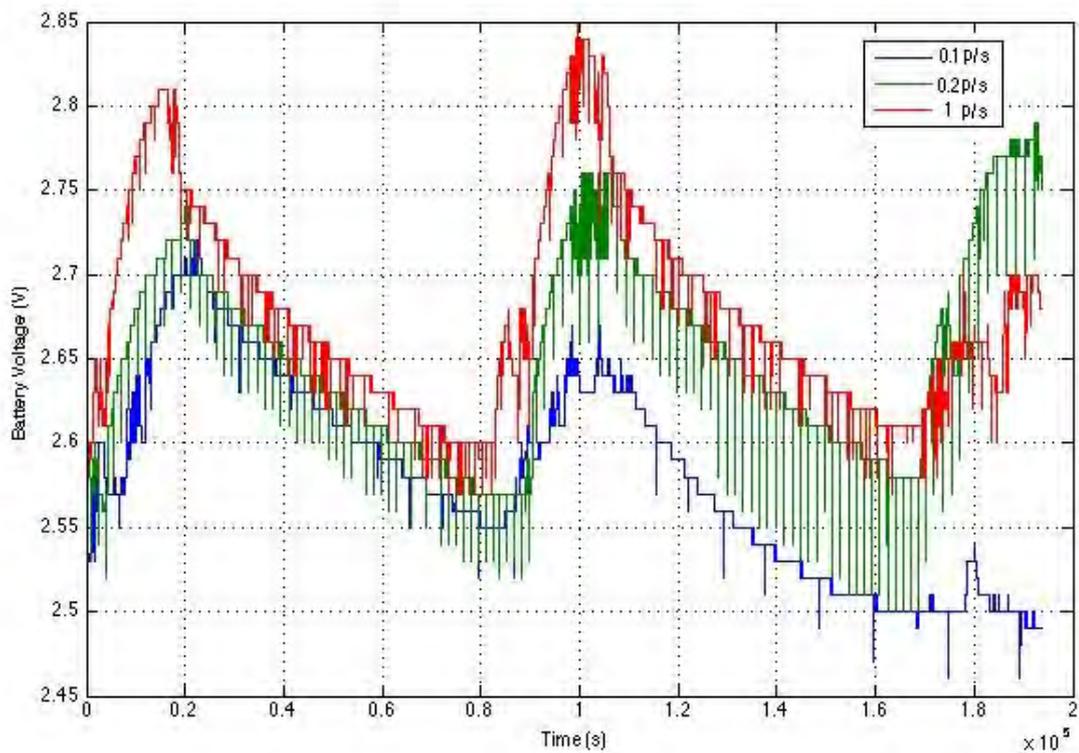


Figure 9: Battery voltage charge/discharge profile for different packet transmission rates measured over three days.

## VI. Conclusions

This paper presented a comprehensive review of the IoT applications and communication network design techniques. The paper reviewed different communication technologies suitable for IoT applications. The review showed that both wireless and wired networks could be used to develop future IoT systems; however, due to the nature of the system, wireless technologies will dominate the networking area. We presented a low-cost wide-area network design architecture which can be developed for both city and rural area applications using low-cost network devices. The proposed energy-scavenging-based heterogeneous network has very low CAPEX (Capital Expenses) compared to a cellular network based system. IoT nodes and networks can be developed at a low cost when embedded wireless technologies are used. Embedded wireless technologies will be scalable and easily upgradable as they are based on international standards.

The OPEX (Operational Expenses) cost of the proposed network is virtually zero because the greater part of the area and access networks will be developed on embedded wireless devices where many devices will scavenge their energy from natural sources, thus the operating energy cost will be minimum. Some OPEX cost could occur when 3G/4G networks or

broadband connectivity could be used in the core network or to support a distributed access network. IoT is an evolving area; many new technologies including embedded wireless technologies will emerge which may further reduce the cost of deployments in future.

## Acknowledgements

The authors would like to thank the Australian Research Council and Ausgrid for supporting part of the project.

## References

- Akyildiz, I. F; Jornet, J. M. 2010. "The Internet of Nano-Things", *IEEE Wireless Communications*, December 2010, pp. 58-63.
- Atzori, L; Iera, A; Morabito, G. 2010. "The Internet of Things: A Survey", *Computer Networks*, 54(2010), pp2787-2805.
- Balasubramaniam, S; Kangasharju, J. 2013. "Realizing Internet of Nano Things: Challenges, Solutions and Applications", *IEEE Computer*, February 2013, pp. 62-68.
- Chen, D; Khan, J.Y; Brown, J. 2014. 'An Area Packet Scheduler to Mitigate the Coexistence Issue in a WPAN/WLAN Based Heterogeneous Network' submitted for review *IEEE WCNC 2014*, New Orleans, USA, 9-12 March, 2104.
- Edson, A; Marques, L; dos Passos, D; Macedo, R; Dias, K; Nogueira, M. 2014. 'Interoperability issues on heterogeneous wireless communication for smart cities', *Computer Communications*, early access article, <http://dx.doi.org/10.1016/j.comcom.2014.07.005>
- Euisin, L; Eun-Kyu, L; Gerala, M; Oh, S. Y. 2014, 'Vehicular Cloud Networking: Architecture & Design Principles', *IEEE Communication Magazine*, February 2014, 148-155.
- Forbes. 2013. Forbes Magazine 1 July 2013. "How many things are currently connected to the internet of Things (IoT)?" Available at: <http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/>
- Gartner. 2014. Media release. "Gartner says a Thirty-Fold increase in internet-connected physical devices by 2020 will significantly alter how the Supply Chain operates" March 24, 2014. Available at: <http://www.gartner.com/newsroom/id/2688717>
- Iniewski, K. 2010. *Convergence of Mobile & Stationary Next-Generation Networks*, John Wiley & Sons.

Jin, J; Gubbi, J; Marusic, S; Palaniswami, M. 2014. "An information framework of creating Smart City through Internet of Things", *IEEE Journal of Internet of Things*, DOI: 1109/JIOT.2013.2296516,

Kim, J; Lee, J; Kim, J; Yun, J. 2014. "M2M Service Platforms: Survey, Issues and Enabling Technologies", *IEEE Communications Surveys & Tutorials*, vol: 16, no:1, First quarter, 2014, pp. 61-76.

M2M Satellite. 2013. "M2M Connectivity". Available at:  
<http://www.m2mconnectivity.com.au/technologies/satellite>

Miorandi, D; Sicari, S; De Pellegrini, F; Chlamtac, I. 2012. "Internet of things: Vision, applications and research challenges", *Ad hoc Networks*, 10 (2012), pp. 1497-1516.

Mobile World. 2014. Mobile World Live 23 April 2014. "Huawei predicts 100B connected terminals by 2025". Available at: <http://www.mobileworldlive.com/evolving-ict-market-create-infinite-opportunities-huawei>

Ardis, Kristopher. 2013. "What's to come: the IoT's role in smart grid evolution". *Smart Grid News*. Dec 3, 2013. Available at:  
[http://www.smartgridnews.com/artman/publish/End\\_Use\\_Smart\\_Homes/What-s-to-come-the-IoT-s-role-in-smart-grid-evolution-6200.html#.VDb\\_6\\_mSzh4](http://www.smartgridnews.com/artman/publish/End_Use_Smart_Homes/What-s-to-come-the-IoT-s-role-in-smart-grid-evolution-6200.html#.VDb_6_mSzh4)

Sterling, L; Tareter, K. 2009. *Intelligent Lifestyle Applications*, MIT Press, 1st edition, 2009, 281-326.

Wu, X; Mincic, R; Al-Stouhi; Misener, J; Bai, S; Chan, W-H. 2014. 'Car Talks to Phones: A DSRC Based Vehicle – Pedestrian Safety System', *Proc. Of the IEEE VTC Fall*, 14-17 September, Vancouver, 2014.

Xu, L. D; He, W; Li, S. 2014. "Internet of Things in Industries: A Survey", *IEEE Trans. On Industrial Informatics*, DOI:10.1109/TII.2014.2300753, early access article available from IEEE Explore, 2014, early access article available for IEEE Explore, 2014.

Yuce M; Khan, J. Y. (editors). 2011. *Wireless Body Area Networks: Technology, Implementation, and Applications*, Pan Stanford Publishing, 2011.

Zaslavsky; A. 2013. "Internet of Things and Ubiquitous Sensing" *Computing Now*, September 2013,

# Project-Based Management Technique for Radiofrequency Spectrum Planning and Allocation

## Part Two: The Project Management Plan

Andrew J Kerans SMIEEE

School of Engineering and Physical Sciences  
James Cook University  
Townsville, Queensland, Australia

**Summary**—Spectrum Management is the regulatory action of defining the use of the radiofrequency spectrum. Often this requires the clearance of a large number of incumbent systems to make way for new technologies such as Fourth Generation Mobile Broadband (4G). While great economic benefits may be derived from the new technologies the clearance of any band will come at a cost. It is important both costs and benefits be quantified and compared. In many Administrations, including Australia, these processes are carried out without a defined project management structure. In a series of two papers the Authors combine over 40 years of radio systems and planning experience to suggest a methodology for project-based management of spectrum planning activities. This paper provides an outline of a recommended project management plan structure and references that may be useful to spectrum planners throughout ITU- Region 3; the Asia – Pacific.

**Keywords**—*project based spectrum management; radiofrequency spectrum; spectrum planning; spectrum economics.*

## Introduction

Spectrum Management is the combination of engineering, economic and allocative inputs resulting in a given use (or combined uses) of the radiofrequency spectrum (the spectrum) ([Kerans 2011](#)). Access to spectrum is vital for any service that cannot, or chooses not to be, tethered to a cable or optic fibre, and is the carriage medium for the exponentially growing mobile broadband industry. The rapid growth of mobile broadband, and the use of these systems to provide internet access where it previously could not be supplied, has been an enabler for a myriad of associated small industries; thus spectrum access is a true large-scale multi-faceted economic enabler.

The services that need to make use of the spectrum are many fold: they include the RADAR systems that monitor air traffic, the fixed links that pipe data to mobile base stations and are as diverse as deep space

communications systems and those that provide mobile communications to ships at sea in the High Frequency (HF) bands.

Mobile telephones have been with us since the early 80's, in Australia pushing aside aircraft navigation systems to access one of the first major spectrum band for GSM services. Recently the world's population has taken to mobile broadband in an unprecedented adoption of new technology. Mobile Broadband, the ability to access the internet and other services on a smartphone is reliant on spectrum – very large amounts of it – and regulators globally are faced with the problem of finding this spectrum in the increasingly crowded electromagnetic space.

Mobile broadband is estimated to contribute \$17.4 Billion (in 2010 dollars) to Australia's economy (Deloitte Access Economics 2010) and is totally reliant on access to suitable radiofrequency spectrum. Globally, Mobile Broadband is seen as a key enabler in developing countries, both access to spectrum and adherence to standards being key issues to ensure economies of scale in the production of user equipment.

[Turner \(2009\)](#) states that in some cases project members hold the view “There is no point planning...”; which historically has been the view of many in the spectrum planning field.

However access to spectrum is becoming fraught with difficulty. More and more systems are becoming available, each requiring access to spectrum. This is occurring at a time when public demand for mobile broadband is growing exponentially. This demand for spectrum is displacing incumbent systems, many of which collectively have a high sunk value and corresponding high economic value to various elements of society.

The cost of moving systems currently dependent on spectrum to a more appropriate medium is also a barrier. One example is television broadcasting. In most cases a combination of fibre to the home (or FttH) combined with satellite retransmission where FttH is uneconomical is a viable delivery solution. This would free up much valuable UHF spectrum for mobile broadband. However the cost to re-engineer broadcasting is prohibitive unless different allocation models are explored.

In real terms the cost of a spectrum refarming project requiring four planners with an appropriate travel budget over three years would be \$2.1 million (based on total staff cost of \$150,000 per annum plus \$100,000 overheads per annum) however such a project has the ability to disrupt \$300 million of existing infrastructure but on the other hand return \$600 million ([Plum Consulting 2012](#)) to government in auction returns for the spectrum. In addition to real returns the economic stimulus can be measure in terms of \$ Billions.

In Australia refarming of this spectrum for mobile broadband could potentially also result in a \$4 Billion additional economic activity (based on [Deloitte Access Economics 2010](#)).

Spectrum is an intangible finite inexhaustible resource. Simply put it doesn't exist. What is licensed or allocated is the right to create an electromagnetic disturbance within a given frequency range. The power to regulate spectrum in Australia is given in law by the (Australian) *Radiocommunications Act* 1992.

The regulation of spectrum requires change as technologies progress. In the current decade there is a strong demand for access to spectrum to provide mobile broadband data. To provide access to this spectrum the ACMA must undertake 'refarming' exercises which in the lower bands favoured for mobile broadband always require the re-planning of the technical characteristics of the allocation and the clearance of incumbent services.

## Spectrum Management

In the Australian context, Spectrum Management is the science of moving spectrum to its highest value use in accordance with the ACMA Principles for Spectrum Management (ACMA Principles) ([ACMA 2009](#)). In undertaking this task and projects relating to it the ACMA contributes to the Australian economy in general and the communications economy specifically.

Regionally coordinated spectrum planning has delivered many wins. Recognising that harmonisation brings with it economies of scale and ease of roaming, the Asia Pacific Telecommunity (APT) has developed a plan for the 700 MHz band that is now recognised as being superior to the US alternative. This band plan, developed through exhaustive regional cooperation, has now been adopted by many Administrations both in the Asia Pacific region but also in Latin America, with many African nations seriously considering its adoption.

The implementation of the plan however will be different in almost every case. One common theme will be complexity, both political and from an engineering perspective, as broadcasting services are cleared and relocated and the plan implemented. This process would benefit from a structured yet flexible project management methodology.

Figure 1 is a flowchart of a 'typical' spectrum planning project process. Projects may differ in complexity or the number of consultations undertaken. However as a general representation the flowchart is useful in understanding the process.

Figure 1 also only represents the externally facing facets of the project; internal processes are not represented but in the case of internal consultations have been previously described.

Not described is the environmental scan and engineering work which initially results in choosing the band under review, but in effect prejudices the outcome as only bands suitable for the proposed new application will be chosen. The consultation however is not 'token'; many changes to plans have been made in the past and indeed some processes have been discontinued because the highest value use was found to be in the incumbent use.

Pertinent to the management of the project are the stakeholders. Some will be for the project, usually those who will gain from access to the spectrum. Some will be against the project, usually incumbent operators; most will be knowledgeable about the subject; and nearly all will be able to influence it politically or via the media.

It is not in the interests of incumbents likely to be moved from a band to cooperate in either domestic or international deliberations where their eventual loss of spectrum access is a likely outcome.

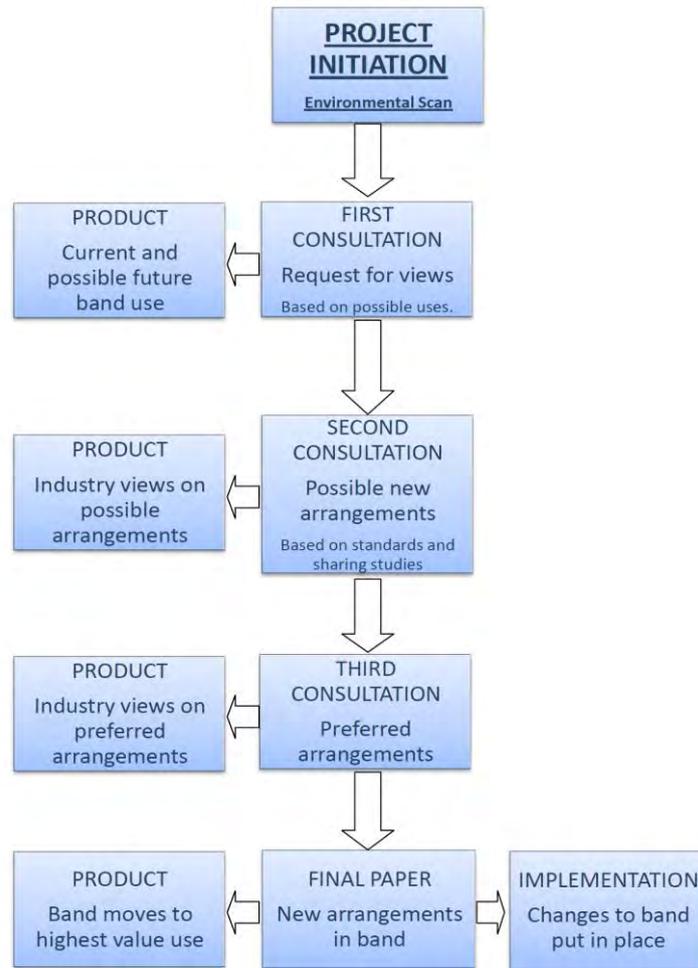


Figure 1. A Theoretical Spectrum Planning Process

## Stakeholder management

Turner (2009) gives a good background in stakeholder identification and management which is particularly relevant to spectrum management both externally and internally within the ACMA. Stakeholder management thus represents a key area that would obviously need to be comprehensively addressed in any spectrum management project, and thus within each individual spectrum planning project management plan.



Figure 2. ACMA Decision Making Hierarchy

## Project based spectrum management

Project Based Spectrum Management is a relatively new field. While various forms of project based management are used within the ACMA and undoubtedly within other spectrum management agencies there is no available literature on it.

Thus existing methodologies need to be examined, investigating their applicability to this reasonably well-known but undocumented field.

The literature search undertaken as a part of this project did identify a number of things: Firstly spectrum project management has strong similarities with software management. There is a product that is intangible, there are customers and clients, and it is hard to make everybody happy. Secondly the work is often undertaken by multiple teams consisting of technical experts, and thirdly software projects are often 'accepted' by non-technical managers.

In general modern software projects are managed using 'PRINCE2 Methodology' ([Office of Government Commerce 2009](#)). PRINCE2 meets many of the requirements for management of projects where the outputs are not tangible; in fact if the outputs of the spectrum planning process are treated as 'products' then most of the methodology seems to fit well.

Spectrum planning is a step-wise process composed of iterative steps; each step informs the next and a true project path can never really be developed from the beginning. Thus some form of step-wise methodology is needed where multiple inputs can be used to inform the next stage.

A variant of PRINCE2 methodology proposed for IT projects is called ‘Step Wise Methodology’ ([Lu 2006](#)) and potentially provides a good path for the development of a PRINCE2 methodology to inform spectrum project management.

One paper on software project management seems particularly relevant to spectrum projects; Barry W. Boehm in a paper entitled ‘Theory-W Software Project Management: Principles and Examples’ ([Boehm 1989](#)) presents some principles directly applicable to spectrum project management (direct quotes in italics). The title *‘Theory-W: make everyone a winner’* opens the abstract, a principle perhaps opposite to the reality of most regulators which can best be described as ‘the role of the regulator is to make everybody equally unhappy’. In a process where one party covets that held by another and where a compromise is necessary it may be near to impossible to make everybody happy, but as a risk mitigation strategy and care in the development of a business case, it is a worthy goal.

Boehm also makes two ‘subsidiary’ statements: *‘Plan your flight and fly your plan’* and *‘manage your risks’*. Both of these ‘adages’ are excellent guidance for spectrum management. When a pilot ‘plans their flight and flies their plan’ there must always be room for flexibility when the weather fails to cooperate or quick action when an engine fails. The two statements also go hand in hand; a rigid flight plan will fail to manage risk. A rigid PMP will do likewise.

In PRINCE2 methodology ([Office of Government Commerce 2009](#): pp 32–33 and Fig 5.2) a breakdown of various corporate structures is given. This is valid for the ACMA and the methodology can be modified to directly represent the reporting lines of the ACMA and similar Australian statutory bodies. Figure 2 shows a simplification of the ACMA structure along with project and decision making responsibilities.

In Australia and for the case of spectrum management the true client is the Australian Government; however in creating a Statutory Authority the Minister for Broadband Communications and the Digital Economy has delegated the stewardship of that role to the ACMA Authority who therefore become the client.

The Authority currently has little input to the project other than final decision making and delegates responsibility to the Divisional General Manager via legally binding delegations. Thus the Divisional General Manager is for all intents and purposes the customer.

Turner provides excellent guidance on the identification of interested parties ([Turner 2009](#): pp 77-83). The ACMA organisation is what Turner calls a Coordinated Matrix ([Turner 2009](#): p 126 & Figure 6.2). Occasionally a ‘secondment matrix’ is used for major projects or where a project has failed. In general though Spectrum Management within the ACMA is a bureaucracy, spectrum planning is carried out by the engineers within the Spectrum Planning Branch, spectrum allocation within a Policy Branch and operational support, such as the mechanics of issuing an authorisation and interference investigations, within an Operations Branch.

## Identifying stakeholders

In a spectrum planning project as in construction or software projects, stakeholders are both internal and external. Because of the inherent differences between the two in a spectrum regulation environment these will be dealt with differently.

### Internal Stakeholders:

Internationally the ACMA is recognised as a strong organisation, a world leader in spectrum management with a very good team spirit. The ACMA is a public service organisation, a term often unfairly maligned, with this in mind a quote from then U.S President John F. Kennedy about the 1960s US public service remains true today:

*“You may have been told that government workers are clock-watchers; you will soon find that the vast majority of them are dedicated not to their paychecks but to the job to be done. You may have heard that government positions involve nothing but plodding routine tasks; you will see some of the most exciting, interesting work in the world being done here. You may have read that public servants are unimaginative, security seeking, uncreative, skilled only at the techniques of empire building; you will quickly discover that we have far more than our share of lively minds, endowed with vigor and courage.”* (Spelling and Grammar uncorrected US Style) ([Rosen 1983](#)).

Like any large bureaucracy the ACMA has internal politics – people who may gain from a project’s failure, and this must be acknowledged and managed as outlined in an article ‘Project Management: Still More Art Than Science’ by [Kate Belzer \(2001\)](#).

Thus internal stakeholders, whether for or against the project, must be identified and communication with them managed. To quote an ACMA project manager when asked about why an earlier project; acclaimed as a ‘jewel in the crown’ of the ACMA during planning, failed to progress during the implementation phase: “X and Y set me up. They didn’t want me running this so they didn’t do the licence conditions we needed to get the incumbents cleared” ([Gladman 2013](#)).

Useful guidance on the management of internal stakeholders can be found in the ‘Theory-W’ paper ([Boehm 1989](#)) in guidance to ‘*make everyone a winner*’. With internal stakeholders it is entirely possible to make everyone a winner and Boehm goes on to explain how (quotes in italics). In essence it involves carefully managed communications and some simple guidelines:

- 1) Separate the people from the problem.
- 2) Focus on interests, not positions.
- 3) Invent options for mutual gain.
- 4) Insist on using objective criteria.

Within a public service structure profit is not a motivator, but kudos and prestige are, for both managers and teams, and working this into the project outcomes in a shared way in line with the guidance above is most likely to result in success.

In addition to not identifying internal stakeholders, beyond identifying them in ‘contacts’ the PMP does not outline what role a stakeholder may have in the process. In order to apply these principles, people with an interest and influence need to be identified along with their motivations.

While the ‘difficult internal people’ should not be identified as such in a plan available to all, they should be identified as having an interest in the project and from that a communications strategy formed. Turner ([Turner 2009](#): Ch 4.2) provides excellent guidance on managing stakeholders which is pertinent to ACMA internal stakeholders. Again it rests on communications, but also when to communicate depending on each person’s commitment to the project.

## External stakeholders:

In a spectrum planning exercise external stakeholders fall into one of two categories: the incumbents who have an investment in the band under review and stand to lose if changes are made, and those vying for new services, usually telecommunications carriers and vendors, who stand to gain from an expanded market.

While Boehm’s guidance to ‘*make everyone a winner*’ may not be possible where a stakeholder will be disadvantaged by change there are methods to salve the pain, such as incentive auctions for spectrum, where the incumbent bids against the new entrant and if they lose, some of the money goes to the incumbent.

## Risk management

In spectrum planning work the risk may be multi-tiered. There is risk to the project, it might fail. There is risk to the ACMA’s reputation, it might be sullied. Finally there is risk to the Government, and if they perceive this then the risk to the ACMA’s existence becomes a reality. So in any risk strategy multiple tables will be needed and an aggregate score developed that correctly identifies the total risk and where it emanates from.

There are other risks to a spectrum planning project beyond stakeholder reaction. In brief these could include a lack of applicable equipment standards, loss of trained personnel, an incorrect cost benefit analysis or inappropriate input from other areas of government (see an article in *The Australian* Newspaper by [Bingemann \(2012\)](#), for example). Risks are multiple and multi-faceted in any spectrum project and must be properly identified and defined, and from this a risk management plan developed.

Both PRINCE2 and the PMBOK Guide ([Project Management Institute 2008](#)) give guidance on risk management. It is probably simpler to look at a single ‘standard’ and PRINCE2 seems to have the most applicability to spectrum projects. The PRINCE2 manual ([Office of Government Commerce 2009](#): p78) gives the following guidance on risk management (paraphrased quotes in italics).

- Establish Goals and Context
- Identify Risks
- Analyse Risks
- Evaluate Risks
- Determine the Treatments for the Risks
- Avoiding the risk by discontinuing the activity that generates it.
- Reducing the likelihood of the occurrence.
- Reducing the consequences of the occurrence.
- Transferring the risk.
- Retaining the risk.
- Monitor and Report on the effectiveness of Risk treatments

At first glance all are appropriate except perhaps ‘*transfer the risk*’. However even this could be given consideration. Should an external agency threaten the project by, for example providing poor advice to the Minister, then a strategy for informing the Minister that the ACMA does not agree would transfer the risk of project failure from the ACMA to the other agency. This should of course be thought of as a last resort; a comprehensive communications strategy with the Minister’s Office may be able to prevent such problems developing.

## Critical path analysis

In a fully developed set of deliverables in a spectrum project, some work packages will rely on the outcome of a previous process or product. In its initial stages a spectrum management project is sold as an ‘open’ consultation where all possibilities are considered. This of course is not the case; early work in an environmental scan, a cost benefit analysis and a determination of the need for spectrum for a certain application would have identified candidate bands. From these, and depending on the urgency of the need, bands that are easily converted are chosen. Thus, while the initial consultation may ask questions like: ‘*The ACMA seeks comment on the proposed objectives of the review*’ ([ACMA 2011](#)), the outcome, at least in part is predefined by the initial work.

Because a likely path is known, a critical path at least containing initial products and bodies of work can be developed with possible paths leading from it. From this review stages can be planned and the critical path updated with known information and reviewed.

An excellent guide to using a Critical Path Method in a complex project environment is presented by [Stelth and Roy \(2009\)](#). This paper analyses the application of critical path management throughout a changing and complex project. Hill, in ‘*The Complete Project Management Methodology and Toolkit*’ ([Hill 2009](#)) provides an initial methodology for developing the critical path. These references combined provide sufficient information for the development of a flexible CPA capable of meeting the needs of project managers during a constantly changing spectrum planning project.

The potential for change during the term of a spectrum project is dependent on the initial cost benefit analysis. If the analysis suggests the benefits are close to the costs then the potential is high. On the other hand if the benefits far outweigh the costs, even with a reasonable allowance for uncertainty the potential for a change of direction is low.

Most bands where the costs and benefits were widely spaced in favour of change have already been refarmed; these were the 'low fruit' of spectrum management. The task now gets harder as the gap between cost and benefit narrows, thus the potential for a change in direction has increased and will continue to in the future.

In a paper on the integration of PRINCE2 and a methodology known as SCRUM ([Rankins & Kearns 2008](#)) describes how the two methods can be defined to commence a project before all requirements are known by being agile and open to change during the project. SCRUM is defined on Wikipedia:

**'Scrum** is an iterative and incremental *agile software development* framework for managing software projects and product or application development. Scrum focuses on project management institutions where it is difficult to plan ahead. Mechanisms of empirical process control, where *feedback loops* that constitute the core management technique are used as opposed to traditional *command-and-control* management' ([Wikipedia 2013](#)).

The combination of methods seems useful in the case of spectrum management projects and could be used to enhance a spectrum PMP.

## A new spectrum project model

Spectrum planning has been shown to be a complex process, one where stakeholder management is generally the key, and poor stakeholder management can result in project failure or damage to the ACMA's reputation. Beyond the importance of the project is the importance of the Australian economy, poor spectrum planning can have a serious detrimental effect on the wellbeing of all Australians: imagine living in a country without access to mobile data. So getting it right is paramount and to re-quote the famous adage: 'if you fail to plan you plan to fail'.

In this section recommendations are made for the transformation of spectrum planning project management into a professional activity that produces an economy stimulating resource and minimises the risk of failed outcomes.

To begin the recommendations resulting from this report a diagram of a more holistic, but generalised spectrum management project is presented. This is presented here so that it can be referred to in subsequent sections. The flowchart is by no means comprehensive; spectrum planning projects differ in many ways and only a thorough pre-analysis can possibly describe all necessary elements. Figure 3 is therefore presented here as guidance only, a basis or foundation on which to build a complete picture.

The second recommendation resulting from the development of a business case would be the target audience. The ACMA Authority currently spends time ‘editing’ and then approving consultation papers during the life of the project, finally approving the changes needed to implement the recommended outcome. Preparation for Authority is time consuming and uses resources that could be better used on the project itself. This report recommends that the business case be developed in a way as to allow the Authority to approve the project as a whole so that a single full-time Authority member can take oversight and that the project can then proceed to final recommendation without further Authority scrutiny.

Spectrum Planning Project management has been described in previous sections; while the project-based management of spectrum planning activities is an emerging field, the projects themselves are not dissimilar to other projects. The outputs from a spectrum planning project are discussion papers, decision papers and technical frameworks; these are tangible products similar to the code in a software project.

Figure 1 describes a very high level, or helicopter view of a spectrum planning project. Indeed this is the only level the final decision makers within the ACMA actually see. Figure 3 presents another generic flow chart of a spectrum planning project, this visualisation of a spectrum project where the activities of Figure 3 along with the preparation of technical frameworks are subsumed within a single work-unit “Commence Spectrum Planning Project”.

This flowchart may be useful when used to produce a thorough Project Management Plan (PMP) as it outlines each stage in each inter-related process providing a guide to ensure nothing is missed.

## Approval processes.

The first layer of the flowchart is the business planning process, culminating (hopefully) in the approval of the project. The process as shown is a recommendation; that is a business plan is prepared for each project and submitted to the ACMA Authority (or equivalent) for approval.

Following that, the ACMA Authority (or equivalent) is ‘kept informed’ to a level depending on the sensitivity of the project, this level being determined in the communications strategy, but does not make further approvals until the final recommendations are presented. This is not the method currently used and there may be resistance to this recommendation from managers or the Authority, as in the case of the latter it loosens their control and in the case of the former increases their responsibilities.

The recommendation has the benefit of seeking a single level of project approval, with review, removing the necessity for multiple papers with supporting documentation being submitted. On an average spectrum planning project this could save as much as 30% of the total work hours as well as some travel expenses for attendance at Authority meetings.

## The project management plan.

In Figure 3 the development of the PMP is shown as a single work unit. This is not the case – the actual PMP is a combination of all of the processes shown which result in the work unit ‘commence spectrum planning project’.

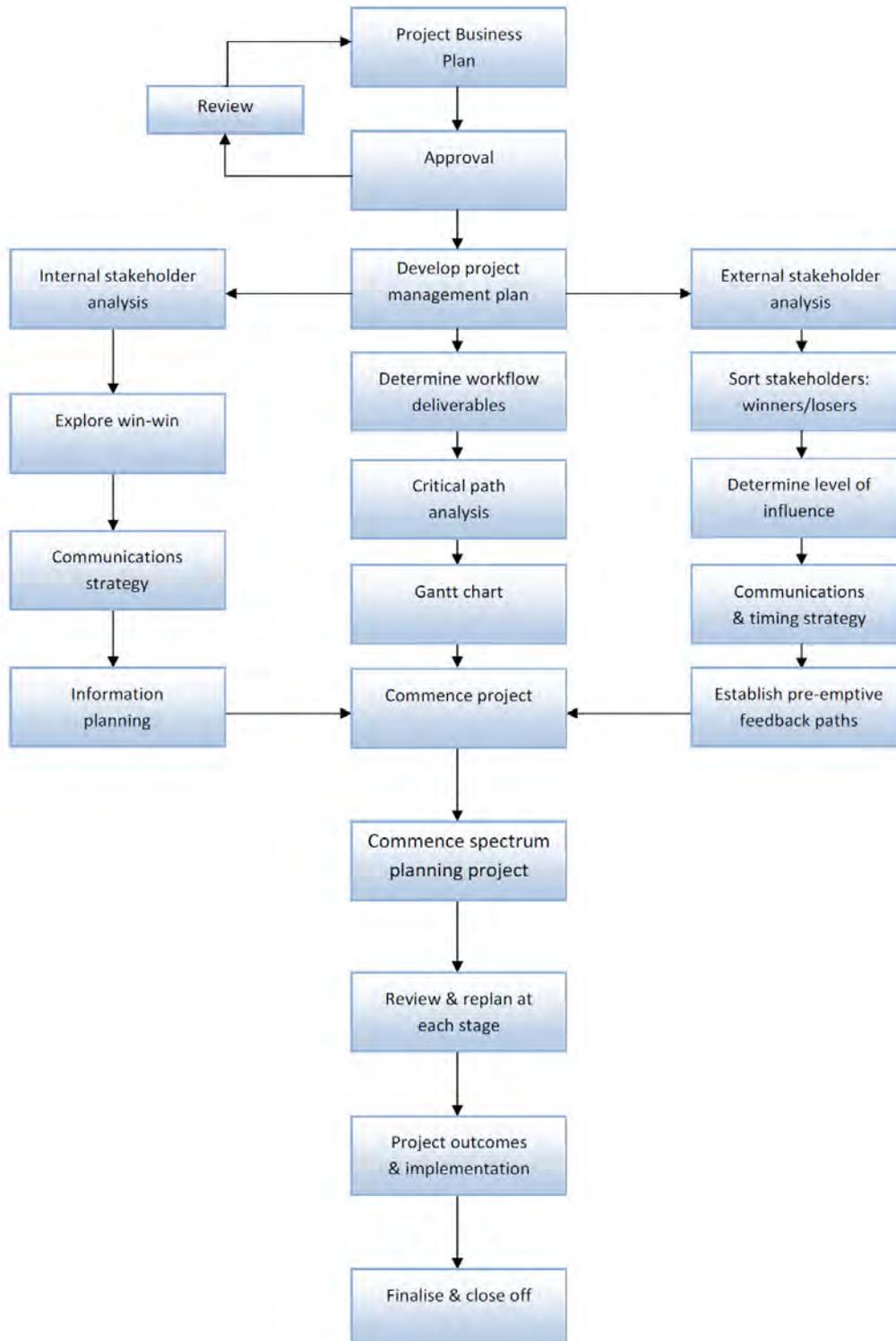


Figure 3. A new spectrum project model.

The importance of stakeholder identification, stakeholder sorting and a cross referenced communications plan has been discussed. These processes are depicted in each of the outriggers to the PMP development cycle. With internal stakeholders the philosophy of ‘make everyone a winner’ can be used and a strategy developed around that so as to eliminate or minimise disruption or the risk of failure caused by internal politics.

Making every external stakeholder a winner to the same extent is probably not possible in a spectrum planning project, however various methods have been described that may reduce the loss in the case of incumbents. The economic aspects of these should have been considered in the business planning stage, meaning the PMP development will have tighter guidance on what outcomes need to be planned for.

Using this information a communications strategy matrix can be developed outlining which external stakeholder is told what and when in the lead-up to a fully open public discussion process. By using time, message and strategy the impact of the main risk, political interference resulting from lobbying, can be minimised.

During this phase a multi-tiered risk management matrix should be developed which identifies all elements of risk to the project, to the ACMA and to Government. Most of the risk will pertain to a communications strategy but some may not. Until identified these risks cannot be mitigated.

## Monitoring the project.

The PMP, like a flight plan, needs to be flexible because ‘stuff happens’. The ‘review and re-plan’ work item in Figure 3 reflects this. When stuff does happen a review may be required and changes to the plan, timelines, staffing or budget necessitated. Stuff could also mean more briefings, additional consultation, more economic analysis or even discontinuing the project. The ability to incorporate these changes is an important aspect of the development of the PMP.

## Implementation.

A few ACMA planning projects have failed because the implementation process failed. The reasons for the failure have been touched on – good communications with internal stakeholders and a project based structure would have pre-empted them. So, assuming all managers and staff are on board, up to speed and ready because the inclusion and communications strategy has worked, implementation is simply the project moving away from the planners to operational staff but still within the core of the project.

## Close off.

There are very few lessons learned in spectrum planning processes because often the close off is not documented. This should become an integral part of any project so that those following can benefit. Beyond that criteria are needed to decide when a project ends. Following a reallocation the band may still be encumbered, so ‘all legacy systems cleared and the band reallocated’ could be a good start. However there

will always be residual encumbrances, so this is impractical. Exactly when it is beyond the scope of this report, but as a measurable it is important or projects may develop their own lives and unnecessarily consume resources and therefore it should be developed within the PMP.

## Overall recommendations.

The overarching recommendation of this paper is that spectrum regulators develop a spectrum planning project management methodology for each spectrum planning project, based on recognised methodology or combinations of methodologies such as PRINCE2 and PMBOK. This methodology should take into account the communications strategies necessary for managing a diverse group of stakeholders as outlined in the referenced literature.

The second recommendation is that project closure studies should be conducted for all major spectrum projects and the lessons learned made available through the literature, so that all regulators can learn and improve their respective methodologies.

## References

- Australian Communications and Media Authority (ACMA). 2009. *Principles for spectrum management* [online] Available at: <http://www.acma.gov.au/Industry/Spectrum/Spectrum-planning/About-spectrum-planning/principles-for-spectrum-management>
- Australian Communications and Media Authority (ACMA). 2011. *The 900 MHz band- Exploring new opportunities*, Available at: <http://www.acma.gov.au/theACMA/submissions-to-the-900-mhz-bandexploring-new-opportunities-ifc-142011>
- Belzer, K. 2001. 'Project Management: Still More Art Than Science', *PMForum Newsletter*, June 2001.
- Bingemann, M. 2012. 'Conroy's wireless spectrum reserve slammed as 'unworkable'', *The Australian* [online], 15 December, Available at <http://www.theaustralian.com.au/australian-it/telecommunications/conroys-wireless-spectrum-reserve-slammed-as-unworkable/story-fn4iyzsr-1226537177347> [Accessed: 15 Jan 2013].
- Boehm, B.W. 1989. 'Theory-W Software Project Management: Principles and Examples', *IEEE Transactions on Software Engineering*, Vol. 15, No. 7, pp. 902-916.
- Deloitte Access Economics. 2012. *Mobile Nation: The economic and social impacts of mobile technology*, Report for the Australian Mobile Telecommunications Association, Available at: <http://www.amta.org.au/pages/State.of.the.Industry.Reports>
- Gladman, K. 2013. ACMA Policy Officer. Interview January 2013
- Hill, G.M. 2009. *The complete project management methodology and toolkit*, CRC Press, United States.

- Lu, KM. 2006. 'A new stepwise project management method', *International Journal of Information Technology and Management*, Volume 5, Issue 2/3, June 2006, pp 212-225.
- Kerans, A. 2011. *Radio Spectrum Planning, Does it Matter in Industry?* Presentation to IEEE North Old Section November 2011, Available from author at [andrew.kerans@acma.gov.au](mailto:andrew.kerans@acma.gov.au)
- Office of Government Commerce. 2009. *Managing Successful Projects with PRINCE2 2009 Edition Manual*, 2009 Edition, The Stationery Office, Great Britain.
- Plum Consulting. 2012. *Valuation report for additional spectrum in the 700 MHz and 2.5 GHz bands*, Report for the ACMA, London (not publicly available).
- Project Management Institute. 2008. *A Guide to the Project Management Body of Knowledge: PMBOK Guide*, 4th Edition, Project Management Institute Inc., United States.
- Rankins, G. J; Kearns, M. (no relation to author). 2008. 'Integrating PRINCE2 and SCRUM for successful new product development', presented at the Australian Institute of project management National Conference, Canberra, ACT, Australia, 13-15 October.
- Rosen, B. 1983. 'Who Needs Bureaucrats?-In the National Interest', *The Bureaucrat-The Journal for Public Managers*, Vol. 12, No.1, pp. 41-42.
- Stelth, P; Roy, GL. 2009. 'Projects' Analysis through CPM (Critical Path Method)', *School of Doctoral Studies (European Union) Journal*, No. 1, July 2000, pp. 10-51.
- Turner, RJ. 2009. *The handbook of project based management*, 3rd edn, McGraw Hill, United States.
- Wikipedia.2013. [http://en.wikipedia.org/wiki/Scrum\\_\(software\\_development\)](http://en.wikipedia.org/wiki/Scrum_(software_development))

## The Victorian Time Signal Service

---

Simon Moorhead

Ericsson Australia & New Zealand

---

**Summary:** A 1945 technical paper from the Telecommunications Journal of Australia is revisited that describes the timing and signalling equipment used at the Melbourne Observatory between 1853 and 1945. The equipment was used to provide the Victorian Time Signal Service for over ninety years.

### Introduction

The measurement of time has a long history stretching back thousands of years. In most ancient civilisations the sun and the moon were observed to determine the time of day, the lunar cycle and the seasons. This led to astronomical observatories being the traditional sources of time measurement.

Fast forward to the Victorian gold rush: the Melbourne Observatory was established at Williamstown in 1853 to provide an astronomical capability for the new colony and a time ball tower for shipping ([Cannon 1945](#)). It was then moved to South Yarra in 1864 because of the deterioration of observing conditions at its previous site due to smoke and dust. The Observatory site still exists in South Yarra today and is managed by the Royal Botanic Gardens. ([RBG 2014](#))

The Observatory closed in 1945 due to encroaching light pollution from the city. ([Wikipedia 2014a](#)) The time signal service was transferred to the Postmaster General's Department (PMG) and the measurement equipment transferred to the PMG Research Laboratories. ([Melbourne Museum 2014a](#))

The TJA paper describes in detail the timing and signalling equipment in the observatory at the time of its closure in 1945, including the pendulum reference clocks and the transit telescope. The paper also discusses the electro-mechanical equipment used to insert the time signal pips into the time signals.

One could be forgiven for assuming the pendulum clocks would lack accuracy compared to today's quartz clocks. These pendulum clocks were actually designed by British railway engineer William Hamilton Shortt in collaboration with horologist Frank Hope-Jones, and manufactured by the Synchronome Co. Ltd. of London, UK. They were the most accurate pendulum clocks ever commercially produced, and became the highest standard for

timekeeping between the 1920s and the 1940s. Recent non-intrusive optical testing has verified their error rate to be only one second in 12 years. ([Wikipedia 2014b](#))

Naturally, special precautions were taken in 1945 to ensure the time references were not disturbed in the transfer from the Observatory to the PMG. The PMG also developed new electronic equipment (rather than mechanical mechanisms) to increase the reliability of the pendulum clock references and create the time signal pips.

The transfer of the time signal service to the PMG in 1945 was logical, given the PMG had the means to distribute time references throughout their national telephone network and via high frequency broadcast stations like VNG Lyndhurst in Victoria. Accurate time references have always been required by professionals such as surveyors, for pinpointing locations in remote Australia.

Eventually the quartz clock replaced the pendulum and later the atomic clock (either caesium or rubidium) replaced the quartz clock as the primary standard. Today, GPS is the most practicable time standard in locations with satellite visibility and is linked to US Naval Research Laboratory's atomic standards. The Precision Time Protocol (PTP), described in IEEE standard 1588, is used for Ethernet based time references and is linked to similar atomic standards. ([Wikipedia 2014c](#))

The oldest Shortt pendulum clock (Number 5) from the Melbourne Observatory was donated by the PMG to Museum Victoria in 1972. ([Melbourne Museum 2014b](#))

## References

Cannon, A.H. 1945. 'The Victorian Time Signal Service', *Telecommunications Journal of Australia*, June 1945, Vol. 5, No. 4, pp. 215-222.

Melbourne Museum-1, 2014a 'Melbourne Observatory & Standard Time in Victoria' at <http://museumvictoria.com.au/collections/themes/1632/melbourne-observatory-standard-time-in-victoria>

Melbourne Museum-2, 2014b 'Free Pendulum Clock - William Shortt & Synchronome Co, London, No. 5, 1925' at <http://museumvictoria.com.au/collections/items/407878/free-pendulum-clock-william-shortt-synchronome-co-london-no-5-1925>

RBG, 2014. – Royal Botanic Gardens Melbourne 2014 'Melbourne Observatory' at <http://www.rbg.vic.gov.au/visit-melbourne/attractions/melbourne-observatory>

Wikipedia-1, 2014a. 'Melbourne Observatory', at [http://en.wikipedia.org/wiki/Melbourne\\_Observatory](http://en.wikipedia.org/wiki/Melbourne_Observatory)

Wikipedia -2, 2014b. 'Shortt-Synchronome clock', at [http://en.wikipedia.org/wiki/Shortt-Synchronome\\_clock](http://en.wikipedia.org/wiki/Shortt-Synchronome_clock)

Wikipedia-3, 2014c. 'Precision Time Protocol', at [http://en.wikipedia.org/wiki/Precision\\_Time\\_Protocol](http://en.wikipedia.org/wiki/Precision_Time_Protocol)

Lamb — The Dynamical Theory of Sound; Morse—Vibration and Sound.

(3) Mason—Electromechanical Transducers and Wave Filters.

(4) Shepardson—Telephone Apparatus, p. 55.

(5) Wentz and Thuras—Moving Coil Telephone Receivers and Microphones, Bell System Technical Journal, Oct., 1931, p. 565.

(6) Martin and Gray—Master Reference System for

Telephone Transmission, B.S.T.J., July, 1927.

(7) Wall—Applied Magnetism.

(8) Marsh—Alloys of Iron and Nickel, Vol. I.

(9) Ballantine—Receiver Testing with an Artificial Ear, Electronics, June, 1940.

(10) Fletcher—Speech and Hearing.

Reference indices in the appendices relate to the numbers against the items in the Bibliography.

## THE VICTORIAN TIME SIGNAL SERVICE

A. H. Cannon, B.E.E.

**Summary:** This article describes in some detail the time service given by, and the timing and signalling equipment used at, the Melbourne Observatory until its Time Department closed down on 19th June, 1945. This equipment is being taken over as a going concern by the Postmaster-General's Department to ensure continuity of the service. As soon as possible new equipment will be provided, using modern apparatus with which the operating staff of the Department is more familiar.

**Introduction:** The equipment used at the Melbourne Observatory to provide the Victorian Time Signal Service was built up over many years under the direction of four Government Astronomers, considerable development occurring during the period (from 1915 onwards) when the late Dr. J. M. Baldwin was in charge. With the retirement of Dr. Baldwin in September, 1943, from the State Government service, the responsibility for the Victorian Time Service was taken over by the Commonwealth Government and placed under the control of the Commonwealth Astronomer. In order to provide continuity of service, arrangements were made for the Observatory to carry on with Dr. Baldwin as Officer-in-Charge until a Victorian Time Signal Service could be provided which was based upon the determination of Fundamental Time at the Commonwealth Observatory at Mt. Stromlo, Canberra. Because of the clear atmospheric conditions usually existing at Canberra, and the staff and equipment already at the Observatory, Mt. Stromlo Observatory is well fitted to make Fundamental Time determinations, but it is not practicable for it to originate the actual time signals needed by the State of Victoria. Line rental charges indicated that this should be done by equipment located near the copper centre of Melbourne.

A number of factors led to the Postmaster-General's Department being requested to undertake, on behalf of the Commonwealth Observatory, the generation and distribution of Victorian Time Signals; these factors were the department's technical and distribution facilities, its existing interest in supplying time to the public, and the fact that as portion of its Frequency Standard technique, it had in operation synchronous clocks which were more precise than

any of the pendulum master clocks used by Australian Observatories.

The permanent equipment used to provide Time Signals will employ electronic and mechanical components with which operating staff of the Post-office can readily become familiar. However, as the provision of such equipment would take a considerable time, and as it was necessary to close down the Melbourne Observatory Time Service by the middle of 1945, it was decided to transfer the pendulum clocks time signal equipment from the Melbourne Observatory to the P.M.G. Research Laboratories and to operate the service from there as an interim measure, pending the provision of new equipment which would be operated by the department's State Administration.

This was done, and the first time signals from the Research Laboratories were transmitted at 2.48 p.m. on 19/6/45.

Consequently, this article deals with the equipment used at the Melbourne Observatory, together with mention of changes and additions made after installation of the first group of clocks at the Research Laboratories. The proposed new equipment will be the subject of a later article.

**Historical:** The Melbourne Observatory was first established at Williamstown, opening in July, 1853, with Mr. R. L. Ellery as Astronomer. Because of rapid deterioration in observing conditions (due to smoke and dust), the establishment was moved to its present site on a basalt hillock at South Yarra in 1864, and continued operations from there until June, 1945.

One of the first clocks obtained for the Williamstown Observatory came from England, and is still in service, being used now as the Mean Time "A" clock. Although showing wear in some parts, it still keeps time reasonably accurately, frequently showing changes of rate of less than one second per day.

Until recently the Observatory possessed, as its Master Clocks, two Shortt Free Pendulum Clocks: Shortt No. 5 obtained in 1925 (approx.), and Shortt No. 59, obtained in 1933 (approx.). Clocks of this type have given outstanding performances all over the world, and No. 5 and No. 59 were no exceptions, although No. 5 was noticeably the more stable of the two.

The other two important clocks used in the time service were the Signalling Clocks, known as the Normal Clock and the Seth Thomas Clock. The former was made at the Observatory soon after it was established at South Yarra, and

a "day" is the popular name for the time interval between two successive passages of the sun overhead. Because of various natural causes, of which the most prominent are the elliptical shape of the earth's orbit around the sun and the in-



Fig. 1.—The Observatory (Williamstown), 1862.

the latter was purchased from U.S.A. Both are giving good service still, but, of course, their second to second uniformity cannot be compared with that of modern high-grade synchronous electric clocks, such as are controlled by quartz crystal frequency standards.

For some years after 1853, time balls at Williamstown and in the city were the only way in which Observatory time was made public; then the Railways became the first "individual" subscriber to receive time signals, and rapidly the number of subscribers grew to include clock-making and business firms and Parliament House. At that time power for the electric signalling currents was obtained from large banks of wet Leclanché cells, each subscriber having his own battery at the Observatory.

Gradual progress added such improvements as a special transmitter for marine time signals and a special transmitter for radio time signals, although due to lack of funds the equipment was not modernised as much as desired.

**Fundamental Time Determination:** By definition, Time is measured in terms of the daily rotation of the earth about its North-South axis, and

inclination of the earth's North-South axis to the plane of this orbit, the actual length of a solar day varies throughout the year. Consequently, our normal timekeeping is based upon the Mean Solar Day, which is an average taken over a whole year. To increase the accuracy of time determinations, the passage of stars overhead is substituted for the passage of the sun, and, as the movements of these bodies have been observed for many years, their apparent positions are known to a high degree of accuracy. Actually, as the accuracy of time-measuring devices—clocks—is improved, it becomes possible to calculate the apparent positions of these bodies more precisely and so prepare the way for still more accurate determinations of fundamental time.

The Troughton and Simms telescope used at the Melbourne Observatory is typical of high-grade astronomical practice, and is specially constructed to facilitate the observation of celestial bodies for precise time determinations and other measurements. It is known as a reversible transit telescope, and is constructed so that, as it swings to sight different stars, its line of sight

moves in a plane which runs North and South, and is perpendicular to the earth's surface; this permits simple checks to determine any small deviation of the actual direction of the telescope from its correct position, and so makes possible the co-ordination of observations on successive nights.



Fig. 2.—The Melbourne Observatory, South Yarra.

**Solar and Sidereal Time:** Suppose for the moment that we have an accurate clock, capable of ticking at the same rate for a long time. Then if we recorded, from day to day, the times indicated by the clock, when the Sun and also some selected star crossed the North-South plane, perpendicular to the earth's surface, in our locality, we would find that the length of time between successive crossings of the Sun was slightly longer than that between successive crossings of the star. The actual amount is approximately 4 minutes, and after counting 365 solar days, we would find that we had counted 366 star, or sidereal, days, and had returned to our original position.

A clock constructed so that its full cycle (of 24 hours) is equal to the time between two successive passages of the selected star, is called a sidereal (star) clock; the master clocks used by Observatories are usually arranged to keep sidereal time because this is the time used in precision time determinations.

The signalling clocks (e.g., those used to provide time signals for use outside the Observatory) are adjusted to keep Mean Solar Time as accurately as possible, and are usually automatically controlled by the Master Clocks, at infrequent intervals (say, every five or ten minutes). This reduction in the work which the Master Clock has to do considerably improves the time-keeping accuracy.

#### DETAILS OF THE VICTORIAN TIME SERVICE

**General:** As stated above, this service was provided for many years from the Observatory in

South Yarra. Star observations there were made with the eight-inch reversible transit telescope, and were used to check the two Shortt Master Clocks. Associated with each Master Clock was a complete chain of working clocks in order to provide an operating and a stand-by system. These latter clocks were all of the weight-driven, pendulum type, with dead beat escapements. In the following discussion mention will only be made of the working group of clocks.

**Types of Time Signals:** Four different types of signals were provided:

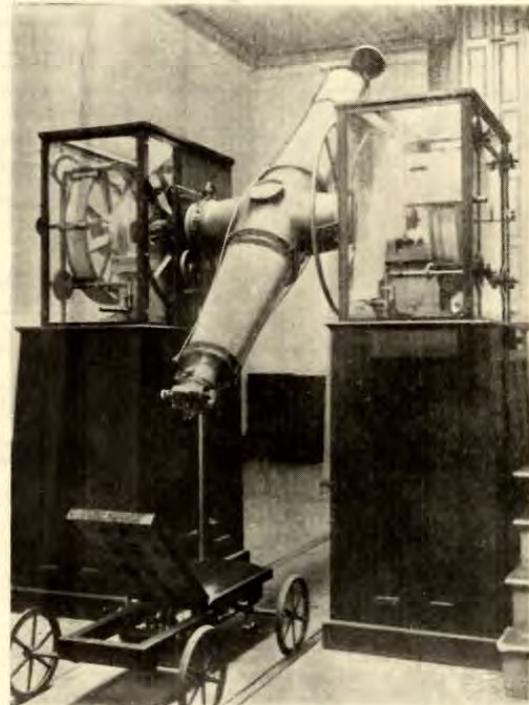


Fig. 3.—The Transit Telescope (the Observatory, Melbourne).

(1) The "XNG," or International Marine navigation time signal. This signal lasted for three minutes, ending precisely at the hour; during the 57th minute a series of "X" morse code signals, for identification, were generated, followed by six timing pips, the last pip of which occurred at the end of the minute; during the 58th and 59th minutes similar signals occurred, except that "N" signals and then "G" signals replaced the "X" signals of the 57th minute.

(2) The "6 pips" broadcast time signal, at the end of each hour, which consisted of a warning pip at 40 seconds, another at 50 seconds, and six timing pips at the end of the 55th, 56th,

57th, 58th, 59th and 60th seconds (the last pip again marking the exact hour).

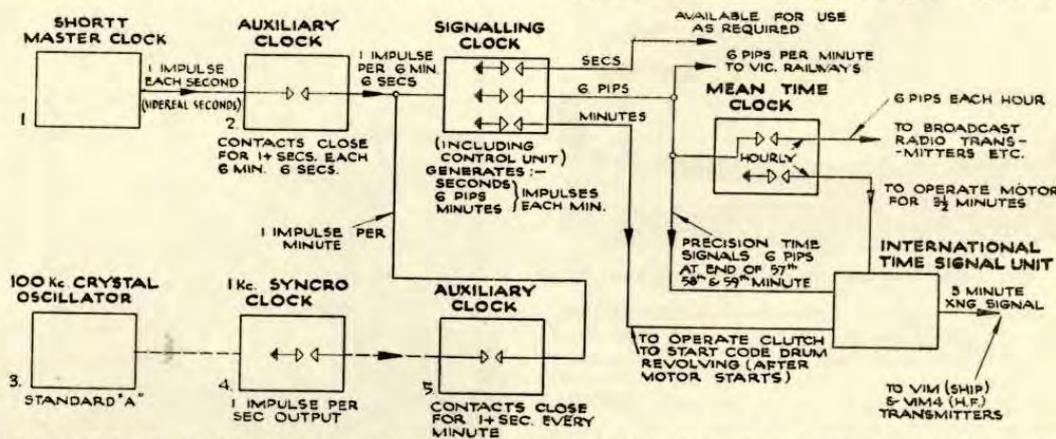
(3) The "6 pips" signal of (2), repeated once per minute; these signals were used for precision civil timekeeping by the Railways Department, and by some watchmakers.

(4) Pips each second, excepting an omission for identification on the 3rd second; these were used by the Postmaster-General's Department to assist checking the Primary Frequency Standard.

**Time Signal Generation Equipment:** Four clocks were used to provide these signals:

charged batteries, and a plug type single line switchboard was used for testing and for routine comparisons of the various clocks. The main auxiliary equipment consisted of a single pen, weight driven drum chronograph, a high-speed tape chronograph and electronic switch, an accurate chronometer, and a radio receiver. The drum chronograph was fitted with a special governor, giving a pen speed of approximately  $\frac{3}{4}$  inch per minute, and was used for most of the inter-comparisons of observatory clocks and radio time signals.

Clock and other relays were generally of low



Units 1 and 2 were at the Observatory. They are now replaced by Units 3, 4 and 5 at P.M.G. Research Laboratories. Fig. 4.—Temporary Time Signal Service Block Schematic of Time-Generation Equipment.

(1) The "Shortt" Master Clock; this consisted of two separate units—the "Free Pendulum" and the "Slave Pendulum."

(2) The Signalling Clock, which generated all the actual time signals (e.g., those near the end of the hour) as required for the "XNG" signal and the 6 pips broadcast signal, and also performed certain auxiliary operations.

(3) The Mean Time Clock, which selected certain of the time signals (e.g., those near the end of the hour) as required for the "XNG" signal and the 6 pips broadcast signal, and also performed certain auxiliary operations.

(4) The Auxiliary Clock, which selected the time interval between two consecutive corrections of the Signalling Clock by the Master Clock.

The Master Clock kept Sidereal Time, the Signalling Clock and the Mean Time Clock kept Mean Solar Time, and the Auxiliary Clock ran at a rate approximating Mean Solar Time, but adjusted to perform its correction function correctly.

In addition, a motor driven drum carrying raised projections on its surface, corresponding to the code XNG, and fitted with numerous auxiliary switches and relays, was used to generate the identification portion of the navigation signals.

**Miscellaneous Equipment:** Power was supplied by two sets of six volt 60 amp hour trickle

resistance, drawing currents of the order of half an ampere, resulting in operating times estimated as a few milliseconds.

**DETAILED DESCRIPTION OF EQUIPMENT**

**Shortt Master Clock:** The aim of the designer, in a clock of this nature, is to make the pull of gravity the sole factor affecting its swing. Disturbing factors are of two kinds—those which are, to some extent, necessary, e.g., the driving force necessary to keep the pendulum swinging, and those which are unnecessary, e.g., changes of temperature.

The outstanding feature of the Shortt "Free Pendulum" Master Clock is the ingenious way in which the Free Pendulum driving impulse is initiated; this is done by the use of another Pendulum, the slave, so that the master, or free, pendulum is only interfered with very slightly. As well as this all possible refinements are incorporated in the master pendulum.

In detail, the master clock is composed of two separate clocks, known as the Free Pendulum Clock and the Slave Clock. Both keep very closely in step, and are adjusted to keep (usually) sidereal time. The Free Pendulum is usually mounted on rock in a location free from vibration and from earth movements which

might affect the value of the constant of gravitation. Although the pendulum is temperature compensated, some care is taken to keep the

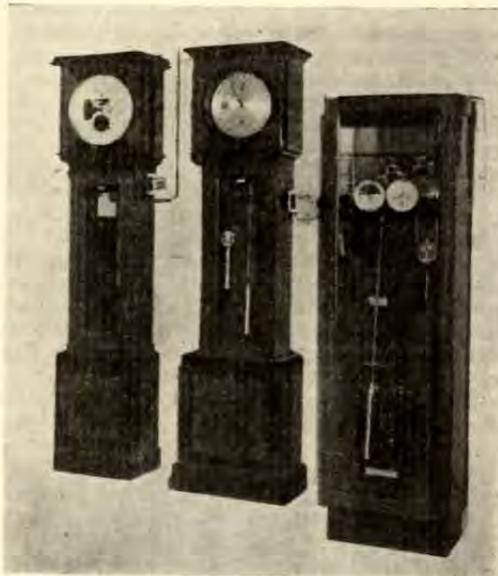


Fig. 5.—Time Signal Clocks, P.M.G. Research Laboratories. Left to right: Mean Time Clock, Auxiliary Clock, Signalling Clock.

room, or vault, temperature as steady as possible. The pendulum itself swings in a constant pressure cylinder, the air pressure in which is adjusted to be only a few cm. of mercury, as this gives the best balance between certain residual effects. Because of the low pressure only a small driving force is required, and the mechanism is arranged so that this is given relatively seldom and in a gradual manner, at the centre of the swing of the pendulum, so as to cause a minimum of interference with the evenness of its oscillation. This is the only unavoidable disturbance which the Free Pendulum suffers because the work of counting the time duration between successive applications of the driving force, and of tripping the mechanism to apply the driving force, is done by the Slave Pendulum.

The Free Pendulum is driven by a small weight applied by the jewel R on the wheel J attached to the pendulum rod; as R drops it first pushes the free pendulum sideways in the direction of its motion at that instant, and then drops clear of the inclined surface to trip a catch which closes a contact in the electrical circuit used to transmit a synchronising impulse to the Slave pendulum. Normally, each second synchronising impulse speeds up the Slave, which would otherwise run slow, so that on the average the Slave keeps correct time. The Slave

counts seconds to determine when the jewel driving the Free Pendulum shall be released again, and also supplies the outside time signals (via other clocks, of course). The Slave is a robust, high-quality clock self-driven by the small roller which runs down the inclined plane on the arm attached to the pendulum rod. It is usually mounted in an easily accessible location, and its routine maintenance requires the control of its own rate (i.e., between successive synchronising impulses from the free pendulum), by the adjustment of small weights on its bob, so that consecutive synchronising impulses alternatively miss and act on it.

As the Free Pendulum is impulsed every 30 seconds, the Slave clock is only required to run so that its error is small over a time of 60 seconds, since after that time the synchronising impulse from the free pendulum will adjust the time error in the Slave by any amount necessary. So the ideal driving conditions for the free pendulum, of a uniform force applied for uniform times at uniform time intervals, are met almost perfectly.

Before the Shortt "Free" pendulum was invented the non-uniformity of driving conditions

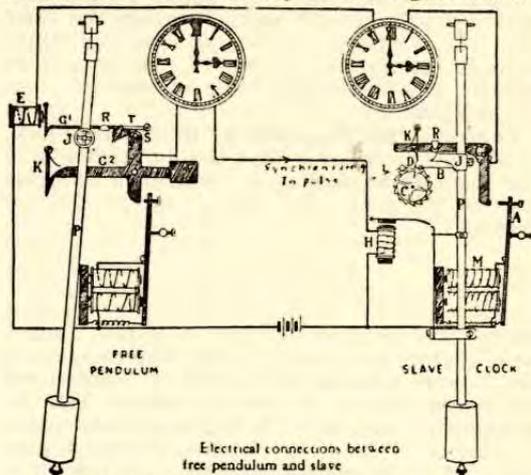


Fig. 6.—Shortt Free Pendulum Clock Electrical Connections.

was the major obstacle to more precise time-keeping. For many years after its introduction in 1921 the Shortt clock was unrivalled, and competitors and technique were so backward that it was hard to analyse its imperfections. With the advent of more precise "Crystal Clocks," which form portion of Frequency Standards, a more accurate clock and means for measuring short period (second to second or day to day) irregularities of the Shortt have become available, and work is going on in England, at least, to improve the Shortt clock still further. As it is possible that this will result in a considerable increase in accuracy, and because of

the simplicity (and hence reliability) of the pendulum clock, this work is of some importance. However, further discussion of this point is outside the scope of this paper.

Because the Free Pendulum is constructed to be independent, as far as possible, of outside forces, difficulty is usually experienced in changing its rate occasionally to compensate for the slight amount of ageing which occurs. This was done, in the case of the Victorian Observatory, by a small permanent magnet, under the bottom of the evacuated case, which interacted with the steel pendulum rod; the range of control was approximately one second per day.

**The Signalling Clock:** This was a high-grade pendulum clock, weight-driven through a dead beat escapement; it was adjusted to keep Mean Solar Time, and generated the actual time signals. It was controlled by the Shortt Master Clock, the correction impulses occurring each six minutes six seconds (Solar).

All the time signalling was done by arms carrying electrical contacts, which were operated by teeth on wheels mounted on the shaft rotating once per minute. There were three of these wheels, and they were cut to give, respectively, signals at each second (except the third after the minute, which was omitted for identification), at 40, 50, 55, 56, 57, 58, 59 and 60 seconds, and at the third second only (i.e., one signal a minute).

**Control of the Signalling by the Master Clock:** It will be remembered that the duration (T) of one complete oscillation of a pendulum swinging free of all controlling forces except that of gravity is

$$T = 2\pi \sqrt{\frac{L}{g}}$$

where, if T is in seconds and L is feet, then g is in ft./sec./sec. and is = 32 (approx.). L is the distance between the point of suspension and the centre of mass of the pendulum. This indicates that variation of L will be a ready means of varying T, and, in practice, coarse adjustments of T are made by screwing the bob up or down the pendulum rod, and fine adjustments by adding weights on the top of the bob; as this latter step effectively raises the centre of mass of the pendulum and so decreases L, any added weight will decrease the length of the period of oscillation and so make the clock run fast.

At the Melbourne Observatory, control of the signalling clock, by the master clock, was obtained by the use of mechanism which caused a small weight to be put on or lifted off a tray attached securely to the pendulum rod. The clock was adjusted by varying the small weights on the top of the pendulum bob so that, with the control weight off, it ran slow by approximately  $\frac{3}{4}$  second a day, and the size of the weight was chosen to make it gain approxi-

mately  $\frac{3}{4}$  second a day when the weight was on. With these adjustments made correctly, the control weight was, over a period of, say, 61 minutes, down in the tray for as long as it was lifted up out of the tray, and with corrections made each six minutes, approximately, the clock would usually gain, or lose, approximately three milliseconds, before the position of the control weight was altered.

**Mean Time Clock:** As well as providing signals for the XNG unit as described later, this clock was used to eliminate, for broadcast transmitters, 59 of the 60 "six pip" signals generated each hour by the signalling clock. As the signals to be transmitted occurred on the 40th, 50th, and then 55th to 60th seconds, the Mean Time clock contacts concerned were closed from 45 seconds before the hour to 15 seconds (approximately) after. These requirements specify the timekeeping precision required of the Mean Time Clock; to provide a factor of safety, time errors of more than five seconds are not permissible, and, as the rate of the clock is usually better

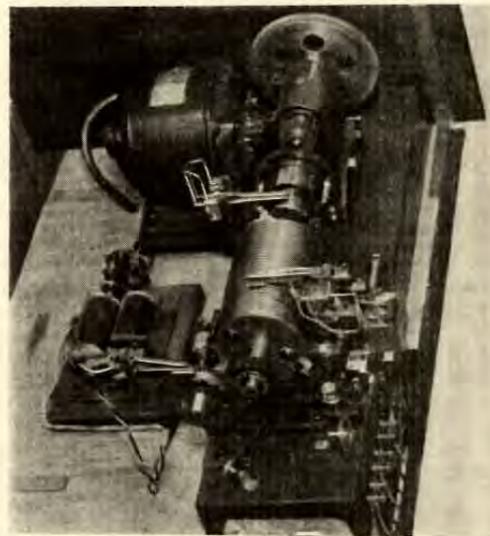


Fig. 7.—International Time Signal or XNG Unit (looking down), P.M.G. Research Laboratories.

than one second per day, a reasonable margin is available for long week-ends, holidays, etc.

**Auxiliary Clock:** This clock carried one pair of make contacts which were closed each six minutes six seconds for approximately one and a quarter seconds, during which time a control impulse from the master clock was permitted to pass to the correction unit of the signalling clock.

**XNG Transmitter:** This unit, under the control of the signalling clock, generated the identification portion of the XNG signal; the time sig-

nal portion of the XNG signal (viz., the six pips at the end of each minute) was transmitted direct from the signalling clock to obtain the highest possible accuracy.

Driven by a synchronous motor through a magnetic clutch, was the programme drum (approximately 6in. long and 3½in. diameter) which carried the XNG signals in the form of raised projections on its cylindrical surface; as required at the start of a run, a pair of electrical contact carrying arms were released by an electro-magnet to cause one end of the lower arm to trail on the drum surface so that it was raised by each projection sufficiently to close the two contacts. A deep spiral thread (6 turns per inch) was cut into the surface of the drum, running in between the signalling projections, and into this was fitted a hardened steel tongue which was fastened on to the base of a carriage which carried the two contact arms mentioned above; consequently, when the drum rotated, the contact making arms were moved parallel to the main axis of the drum, so that the arms passed over each signalling projection in turn. On this contact arm carriage was also mounted, at the forward end, a trip mechanism to open the circuit of the magnetic clutch when the contact arms reached the end of the XNG programme; while at the rear end of the contact arm carriage was a spring-loaded projection which, when the carriage had almost completed its return stroke, caused a spring steel finger to swing out and, by engaging a projection on the rear end of the programme drum, stop its revolution without excessive shock.

The full programme lasted practically three minutes, and near the end of each minute the time signal output of the unit was switched from the drum contact arms to take the six pips from the output of the signalling clock by a cam operated from main drum drive shaft.

The induction motor was started at 3 minutes 14 seconds before the hour, and stopped 15 seconds after the hour by relays controlled from an hourly contact (lasting for three and a half minutes) on the Mean Time Clock; while the magnetic clutch was started at 2 minutes 57 seconds before the hour by the minute signal on the signalling clock. Use of the correct minute signal was ensured by keeping its circuit open until the Mean Time Clock hourly signal occurred. The first minute impulse after this circuit became closed locked up the trip mechanism carried at the forward end of the programme arm carriage and so closed the magnetic clutch circuit and held it closed until the trip mechanism was unlocked mechanically by the drum after the programme had been concluded.

As stated above, drive on the forward transmitting portion of the cycle was by electric motor; at the end of the forward portion of the cycle the clutch was de-energised, allowing the drum to be rotated in the opposite direction

back to its start position by a torque provided by a weight-loaded cord which had been wound up while time signals were being transmitted. This reverse rotation of the programme drum also returned the contact arm carriage, which was gravity-loaded to assist this movement.

**Switching Facilities:** In order to permit the maximum use of clocks in the reserve group comprehensive arrangements were made to switch in practically any clock of the reserve group, in place of its corresponding member of the working group. At the same time arrangements were provided to enable the various clocks to be readily inter-compared, using a tape or drum chronograph.

**Overall Accuracy of the Equipment:** The main factors controlling this, under normal operating conditions, were the deviation of the master clock from its predicted value (obtained by extrapolation based on star observations) and the irregularities in the spacing of the teeth of the transmitting wheels on the seconds shaft.

Star observations were normally attempted each night, but owing to Melbourne weather conditions periods of up to a week between satisfactory observations were common. On many occasions the master clocks would keep time to within, say, 10 milliseconds, over this period, but on other occasions errors of as much as 50 milliseconds were noted. The position was further complicated by the inaccuracy of the star observations (the probable error was usually about 25 milliseconds); this made several consecutive star observations necessary before the master clock error could be determined reliably. In addition, the spacing of the teeth in the seconds wheels could cause errors of 10 or 20 milliseconds.

Consequently the estimated probable error lay between 20 milliseconds (when conditions were stable) to possibly 60 or 70 milliseconds when conditions were bad. Over the last few years this latter figure was considerably reduced to, say, 20 or 30 milliseconds by the use of the Post-office Crystal Clock (Frequency Standard) as a third master clock.

**Modifications Made When Installing the Time Signalling Equipment at the Research Laboratories:** Continuity of operations during the change from Observatory to Post-office operation was obtained by installing the clock group, which had been in reserve at the Observatory, in the Research Laboratories. The master clock of this group was not available, having on August, 1944, been sent to Mt. Stromlo Observatory. At the Research Laboratories, the function of this clock was performed by a synchronous clock driven from one of the crystal oscillators of the Primary Frequency Standard. This gives a greater accuracy and flexibility, at the cost of greater fault liability. This greater fault liability will shortly be practically eliminated by the insertion of a stable pendulum clock between the

synchronous clock and the signalling clock to carry on as a master clock if the synchronous clock stops. Because the crystal master clock keeps Mean Solar time certain auxiliary equipment was modified to enable the original control system of the Signalling clocks to be maintained.

Some increase in the reliability of the control of the Signalling clock (which had been giving erratic trouble at the Observatory) was obtained by increasing the control weight and also shortening the time between comparisons of the Master and Signalling clocks.

Better use of cable pairs was made by installing splitting relays (for the hourly six pips signal) at City West Exchange.

**Use of Frequency Standard Equipment with the Pendulum Clock Units:** Although all details of this aspect have not been finalized, the following notes are included as a matter of interest:

At present the main units of the Frequency Standard are two 100 kC quartz oscillators ("A" and "B"); held as a stand-by is the previous Frequency Standard, a 1000 c.p.s. Valve Maintained Tuning Fork.

Timing of all three units is effected (using divide by ten multi-vibrators as necessary) by driving 1000 c.p.s. synchronous clocks from portion of the output of the unit concerned.

As well as indicating in a conventional way, hours, minutes and seconds, the one r.p.s. shafts of these clocks produce seconds impulses of high precision (erratic variations are of the order of one millisecond). The phase of these in seconds impulses can be precisely adjusted by moving the back (normally fixed) contact of the pair of seconds contacts, so that the contacts make earlier or later. Seconds Signals generated from a "Crystal" clock operated in this way (from Standard "A" at present) are transmitted twice daily over a normal telephone carrier circuit to Mt. Stromlo Observatory, Canberra. Comparison of these signals at the Observatory, with star observations and radio time signals provides the link between Time Signals generated in Melbourne and Fundamental Time, and also provides one means for calibrating the Frequency Standard.

The precision of this method of time keeping can be gauged from the fact that it is possible to predict ahead, on the basis of past behaviour against Observatory Time Signals, that "Frequency Standard" time after an interval of, say, one month, will be within 20 milliseconds of the corrected Observatory Time Signals at that date. (Corrections are usually not known till some weeks afterwards.)

Seconds impulses generated in this way are

converted into electrical power by the use of gas discharge tubes as impulse generators, and the pulses of power, after being lengthened, are fed into the Signalling Clock control circuit in place of signals previously generated by the Slave portion of the Shortt Master Clock.

The phase differences between series of second signals from various sources (e.g., time signals, synchronous or pendulum clocks) are determined in several ways, e.g., by the use of pen or spark tape chronographs, or by adjusting the phase of one series to cause it to coincide with the series of seconds impulses from another source. In the former case, measurements can be made with negligible delay and errors of less than two milliseconds; while in the latter case the delay is also small and the measurement inaccuracy can be made less than one millisecond. In this latter case, coincidence can be observed visually on a Cathode Ray Oscilloscope, or audibly by feeding the signals into a special Valve Oscillator/amplifier unit which drives a loud speaker; here coincidence is indicated aurally by a cancellation of one signal by the other, or by their super-position.

A purely electrical method of controlling a weight-driven pendulum is being developed to supersede the lifted-dropped weight method at present used on the signalling clock; such a development is necessary, because in the event of failure of the control signals the control weight remains dropped, thus giving the clock a large gaining rate. The unit being developed determines the phase of the pendulum clock seconds, relative to the control seconds, and converts this phase difference into a unidirectional magnetic force, which operates on a permanent magnet fastened to the bottom of the pendulum bob, and so causes what is, in effect, a change in the value of the constant of gravitation, as far as the period of the pendulum is concerned. This system of control is expected to be especially useful when applied to the Shortt Clock, where the master pendulum swings in an evacuated space, thus rendering impracticable control of its rate by the usual method of adding small weights to, or removing them from, the pendulum bob.

**Future Action:** It is proposed to instal new equipment, using electronic and telephone apparatus, at City West Exchange as soon as possible, so that the service can be handled by the department's normal operating staff.

**Acknowledgment:** The author's personal thanks are due to the late Dr. J. M. Baldwin and members of the Observatory staff; and to the officers concerned in the Research Laboratories, for their interest and enthusiasm.

## Big Data meets Big Fridge (a frolic)

---

Edouard Estaunié

West Melbourne Institute

---

**Summary:** This article offers a possibly optimistic view of the influence of the new anti-terror laws on the profitability of the telecommunications industry.

“Looking back, the 2010s were the decade in which Big Data took off and telco shares went through the roof.

“And with hindsight from year 2020, heh heh, we can see that the main cause was Big Government.

“It wasn’t just the endless traffic from the bots set up by all those charming politicians to erase their broken election promises in Wikipedia and the media websites, under their Right to be Forgotten laws. Or the counter-traffic from the bots set up by concerned members of the Historical Societies, to redeploy the video clips of the same polliès caught making those promises *in flagrante delicto*.

“Nor was it just the endless downloading of Hollywood and indy films dealing with imagined dystopias in the near future (*Matrix, The Road, Cloud Atlas, The Hunger Games, ...*), which resonated amongst first world citizens, so totally frustrated with living in supposed democracies that seemed to be trending towards police states.

“No, the major source of data traffic was the provenance of Big Spook – the government security agencies that blossomed under massive funding increases through the post-9/11 and counter-ISIS anti-terrorist legislation. Much like the CIA had grown huge and out of control during the Cold War – and again under Bush.

“In the early days, Big Spook was happy to connect to the telcos’ backbone routes, copying and recording zettabytes of traffic for their data-mining software.

“But once they got deeply interested in profiling potential terrorists, and kept persuading the polliès to broaden the definition of ‘terrorist’ so as to improve their performance results, the

passive detection of incriminating data via the Internet became ... inadequate. Especially when Electronic Frontier and other Internet libertarians began producing effective tunnelling software to evade Big Spook's best anti-encryption tools. Hah!

"To profile their suspects, Big Spook needed more data than the oceans of it being sucked out of the burgeoning public WiFi systems. It saw great potential in profiling personality types from eating and imbibing habits. Animal liberationists, for example, were almost universally vegans. Islamic jihadists would demand halal meat. Biker gangs would favour cocaine, ice and other drugs. And so on.

"From 2016 the remotely controlled fridge became a best seller amongst consumers, and simultaneously the target of Big Spook. To monitor the fridge contents it would need to mimic signal traffic from the owners' mobile devices, and divert the fridges' responses to its own portals. Easy peasy. As was hacking e-health records from a variety of sources (hospitals, GP surgeries), and lifting shopping records from retailers – a routine exercise. And snooping the web-cameras in home and office security systems: the biggest generator of 'black ops' traffic.

"To disguise its cowboy surveillance operations, Big Spook would set up and pay bogus accounts with major telcos. Big Spook of course has vast, secret budgets beyond any official oversight.

"And thus the projected traffic from the known Internet of Things has exceeded the analysts' forecasts, year after year.

"No-one has lost money investing in telco shares during the past decade, my friends."

## References

News.com.au. 2014. 'Anti-terror laws pass Senate, giving Australia's ASIO spies increased power and protection', 26 September 2014, at <http://www.news.com.au/national/antiterror-laws-pass-senate-giving-australias-asio-spies-increased-power-and-protection/story-fncynjr2-1227071099923>