# 

# InmsVire

Essential daily reading for the communications industry executive

An iTWire publication www.itwire.com Editor: Stan Beer Wednesday 19 December 2018

## **TELCOS NOT READY TO DELIVER 5G SAYS REPORT**



*CommsWire* (ISSN 2202-4549) is published by iTWire Pty Ltd. 18 Lansdown St, Hampton, Vic, 3188 CommsWire/Telecommunications Editor: Stan Beer

Staff writers: Peter Dinham, Alex Zaharov-Reutt, Sam Varghese. Columnist: John de Ridder Advertising: CEO and Editor in Chief, Andrew Matler: andrew.matler@itwire.com • Tel: 0412 390 000

## DOUBT OVER WHETHER TELCOS ARE READY TO DELIVER 5G: REPORT

Sixty-six percent of organisations have plans to deploy 5G by 2020, but according to a new report users adopting 5G face the lack of readiness of telecommunications providers, with their 5G networks not available or capable enough for the needs of organisations.

According to the 5G use case and adoption <u>*report*</u> from global analyst firm Gartner, organisations expect 5G networks to mainly be used for Internet of Things (IoT) communications and video, with operational efficiency being the key driver.



"In terms of 5G adoption, end-user organisations have clear demands and expectations for 5G uses," said Sylvain Fabre, senior research director at Gartner.

"However, one major issue that 5G users face is the lack of readiness of telecommunications providers.

"Their 5G networks aren't available or capable enough for the needs of organisations."

Gartner also predicts that by 2022, half of the telecommunications providers that have completed commercial 5G deployments will fail to monetise their back-end technology infrastructure investments, due to systems not fully meeting 5G use requirements.

"Most telcos will only achieve a complete end-to-end 5G infrastructure on their public networks during the 2025-to-2030 time frame — as they focus on 5G radio first, then core slicing and edge computing," Fabre said.

"This is because telco 5G public network plans vary significantly in timing and scope. Telcos will initially focus on consumer broadband services, which may delay investments in edge computing and core slicing, which are much more relevant and valuable to 5G projects."

According to Gartner, to meet the demands of businesses, technology product managers planning 5G infrastructure solutions should focus on 5G networks that offer not only 5G radio, but also core slicing and edge computing infrastructure and services for private networks.

The analyst firm says telcos alone may not fully satisfy the short-to-midterm demands of organisations that are keen to deploy 5G quickly.

"Private networks for enterprises will be the most direct option for businesses that want to benefit from 5G capabilities early on," Fabre said.

"These networks may be offered not only by telcos, but also directly by infrastructure vendors — and not just by the traditional large vendors of infrastructure, but also by suppliers with cloud and software backgrounds."

Gartner maintains that to fully exploit 5G, a new network topology is required, including new network elements such as edge computing, core network slicing and radio network densification.

"In the short to medium term, organisations wanting to leverage 5G for uses such as IoT communications, video, control and automation, fixed wireless access and high-performance edge analytics cannot fully rely on 5G public infrastructure for delivery," Fabre cautioned.

Gartner says, however, that IoT communications remains the most popular target use for 5G, with 59% of organisations surveyed expecting 5G-capable networks to be widely used for this purpose.

The next most popular use is video, which was chosen by 53% of respondents.

"The figure for IoT communications is surprising, given that other proven and cost-effective alternatives, such as Narrowband IoT over 4G and low-power wide-area solutions, already exist for wireless IoT connectivity," Fabre says.

"However, 5G is uniquely positioned to deliver a high density of connected endpoints — up to 1 million sensors per square kilometre.

"Additionally, 5G will potentially suit other subcategories of IoT that require very low latency.

"With regard to video, uses will be varied. From video analytics to collaboration, 5G's speed and low latency will be well suited to supporting 4K and 8K HD video content."

#### Peter Dinham





## **TELSTRA TAKING EQUITY INVESTMENT IN SOUTHERN CROSS CABLE**

# Telstra is taking up an equity partnership in Southern Cross Cable Networks with an investment that gives it extra capacity in the trans-Pacific subsea cable.

Telstra joins existing shareholders in the cable company — Spark New Zealand, Singtel and Verizon Business — inking a terms of purchase agreement to acquire a 25% stake in SCCN and substantial capacity on both the existing network and the new Southern Cross NEXT subsea cable.



SCCN — which owns and operates the trans-Pacific Southern Cross Cable and has initiated work on the Southern Cross NEXT cable — says the share purchase and capacity purchase are inter-conditional, and both are subject to definitive documentation and relevant regulatory approvals.

Southern Cross NEXT will be a high capacity express route, providing data-centre connectivity between Sydney,

Auckland, and Los Angeles.

The cable is scheduled for completion by end-2020, and given its design and route, will be the lowest latency path from Australia and New Zealand to the United States.

The new 12,250 kilometre cable system has been developed as an extension of the existing Southern Cross eco-system.

SCCN says the cable will allow customers to leverage its extensive point-of-presence network and access infrastructure already in place.

It will also flexibly assign new and existing capacity across the three routes from Australia to the US, Australia to New Zealand and New Zealand to the US, maximising diversity and resiliency.

Southern Cross NEXT is expected to cost around US\$300 million, and is designed to carry 72 terabits of traffic.

SCCN says this ensures it can cater for its customers' growing data requirements well into the future.

Services offered on the new system will be an extension and integration of the services offered across the current Southern Cross platform.

The construction will be funded by a combination of capacity payments, equity contributions and financing.

Southern Cross Cables president and chief executive Anthony Briscoe said: "Southern Cross has always been a provider of high-quality customer focused and resilient international capacity solutions, and the addition of the new Southern Cross NEXT route to the existing platform will provide existing and future customers with further resiliency and connectivity options between Australia/New Zealand and to the US via Los Angeles.

"We are delighted that Telstra has committed to the cable as an anchor customer, and more so that Telstra sees the value in our capability long-term and is set to take a stake in the company."

"Telstra has long been a key customer of Southern Cross and this investment will mean Telstra has an immediate ownership interest in the existing Southern Cross network, as well as in Southern Cross NEXT," said Telstra group executive for enterprise, Michael Ebeid.

"This route is extremely important to our business as US to Australia traffic accounts for more than 80% of all the internet traffic to Australia. Southern Cross builds on Telstra's existing footprint in Asia Pacific and creates a critical new path for 'Australia In' and 'Australia Out' connectivity."

Singtel vice-president, Carrier Services, Group Enterprise, Ooi Seng Keat, said: "The Southern Cross NEXT cable will be a new data superhighway expanding the existing Southern Cross network, enhancing network redundancy and providing the lowest latency route from Australia to the US.

"The new cable system enables Singtel Group and our Australian subsidiary Optus to meet customers' growing high performance data requirements for bandwidth-intensive applications such as unified communications, enterprise data exchange, internet TV and online gaming."

"This agreement is a major milestone in building what will be a valuable addition to the Southern Cross network, which provides critical connectivity between New Zealand, Australia, the Pacific Islands and the USA," said general manager of regulatory affairs for Spark, John Wesley-Smith.

"Southern Cross NEXT will ensure that Southern Cross can continue to provide high quality resilient connectivity to New Zealand, and serve our customers increasing demand for international capacity, for decades to come.

"We welcome Telstra as a prospective shareholder alongside us in Southern Cross."

SCCN says that with significant work already completed including pre-sales, marine survey, landing arrangements, Pacific Island agreements, detail design and the cable RFT, the NEXT project is well positioned to meet its target completion date of end 2020.

#### Peter Dinham



John de Ridder Telecommunications Economist

strategic management  $\bullet$  wholesale and retail pricing  $\bullet$  regulatory issues

click here to go to www.deridder.com.au

## T-MOBILE-SPRINT MERGER CLEARED AFTER HUAWEI EXCLUSION

T-Mobile US and Sprint have been given permission to go ahead with their proposed merger after national security reviews cleared the deal, which is now expected to be finalised in the first half of 2019.

The US Committee on Foreign Investment, the Justice Department, Department of Homeland Security and Defence Department all gave the green light for the two companies to merge, a statement from T-Mobile said.



The four agencies are together known as Team Telecom.

John Legere, chief executive of T-Mobile US, said: "We are pleased to achieve both of these important milestones in the journey to build the New T-Mobile.

"We are a step closer to offering customers a supercharged disruptor that will create jobs from day one and deliver a real

alternative to fixed broadband while delivering the first broad and deep nationwide 5G network for the United States.

"These approvals assure the strong partnership both companies have with the US Government will continue with the New T-Mobile.

"We look forward to continuing our discussions with the remaining regulatory agencies reviewing our transaction to share our story and subsequently achieve similar positive results."

The go-ahead for the merger of the third and fourth biggest mobile networks in the US was expected after <u>reports</u> that both Deutsche Telekom, the majority owner of T-Mobile, and Sprint's majority owner, Japanese firm SoftBank, had agreed to exclude Chinese telecommunications giant Huawei as a supplier.

The US has banned the use of Huawei equipment in its 5G networks, claiming that the company can be a conduit for spying by Beijing.

Huawei has repeatedly denied that it can be forced to indulge in espionage.

<u>Australia</u> and <u>New Zealand</u> have both followed the US lead and banned Huawei from roles in their respective 5G rollouts.

#### Sam Varghese

## THE PROBLEM WITH HUAWEI? IT JUST HAPPENS TO BE CHINESE

COMMENT: In the tradition of man bites dog, on Tuesday we had a genuine news story when Germany asked a rare question: where is evidence that Chinese telecoms equipment maker Huawei is using its products to spy on behalf of Beijing?

Given the hysteria that the US has generated around Huawei, that is the equivalent of questioning the law of gravity.

It is a given that Huawei is up to no good and Uncle Sam wants to help the rest of its rightthinking folks to hold out against nasty Chinese designs.

Journalists are happy to lend credence to this fable, swallowing tales from "official sources" with glee and regurgitating them verbatim in the publications for which they work.

Just a few days back, Australians Chris Uhlmann and Angus Grigg had <u>a dramatic yarn</u> about how spies from the Five Eyes — the US, the UK, Canada, Australia and New Zealand hatched a plot to prevent Huawei from selling equipment to anyone who would listen.

Buried within that tale was a reference that Huawei had copied in Australian Signals Directorate chief Mike Burgess on a tweet that it had demonstrated that separation between the 5G radio access network and its core was possible – something Burgess has <u>claimed</u> is not possible and the main reason why Huawei has been banned by Australia.

But then Uhlmann and Grigg are not concerned with <u>technical details</u> – anything that comes from a Western spy chief is acceptable. Burgess was quoted as replying with a tweet saying that he had yet to see such isolation in 5G technology.

He obviously knows more than <u>the 3GPP</u>, the organisation that is actually deciding the standards for 5G.

Anything that paints Huawei in a good light is Communist propaganda in the eyes of journalists such as these.

For all the talk of spying by Huawei, one has yet to see any evidence of such activity.

There have, however, been <u>backdoors disclosed</u> in equipment from global networking vendor Cisco, one which the company buried therein.

Yet there has never been any talk of banning Cisco equipment from the Internet.

There has also been a verified account of the American NSA spy agency **planting backdoors** in Cisco equipment when it was en route to certain customers.

But then Cisco is an American company. It ain't got no truck with those Communists.

So too is the NSA, which is as American as apple pie.

And you know that anything American cannot be involved in anything shady.

The argument one hears often is that under Chinese law, Beijing can ask any Chinese company to assist in the task of espionage.

But then nobody mentions that the situation in the US is the same – and, in fact, the NSA has already used the good offices of Messrs Google Verizon, Apple, Microsoft et al to spy on all and sundry.

After the Snowden revelations, this is no figment of one's imagination.

To digress a bit, Australian journalists are also prone to work themselves into a lather whenever they mention the fact that China has developed islands in the South China Sea as a military base.

But there is never a mention of the equally indisputable fact that the US has about 40 military bases in the Pacific, completely ring-fencing China.

Nope, American spying good. Chinese spying bad.

This morning, I was struck by some posts on an American website known as Slashdot.

Responding to a post about Huawei asking for proof to justify the US and other countries' claims that it is involved in spying, several people responded by saying that they would prefer to buy Huawei phones.

Crazy? No, their argument was that China could do nothing to them even if it were spying on them, whereas if they were spied on by the NSA and the CIA — through American devices — then they were indeed in danger.

The level of espionage carried out by the NSA and the CIA is far in excess of anything indulged in by China, Russia, Iran or North Korea – the four countries that are most often blamed for cyber intrusions.

But one never hears of any American cyber activity at all; when it comes to that, American journalists, for all their talk of democracy and a free press, become fiercely patriotic.

So I guess the mud being thrown at Huawei will continue, until the US is satisfied that it has saved its allies from the danger of Chinese spying.

People who look for logic in this nakedly political exercise are searching for pearls in mud.

#### Sam Varghese

## PRESSURE ON PIPE NETWORKS OVER TELECOMS CODE RULES

PIPE Networks, a subsidiary of telecom services provider TPG Telecom, has been ordered by the telecommunications regulator to comply with new rules for small mobile phone base stations following investigations finding the company had contravened code rules.

The Australian Communications and Media Authority has warned <u>Pipeworks</u> that if it fails to comply with its direction, it may issue an infringement notice or commence proceedings in the Federal Court.

The <u>ACMA's direction</u> follows two investigations where PIPE Networks was found to have contravened code rules:

- By failing to provide accurate and up-to-date information to a local council and residents during consultations on a proposed base station deployment
- By starting work before concluding consultation on the proposed deployment.



The Mobile Phone Base Station Deployment Industry Code aims to ensure mobile telcos consult with local councils and communities before deploying mobile phone infrastructure.

"It's important for telcos to keep affected communities in the loop and to consider their feedback when deploying new infrastructure", said ACMA chair Nerida O'Loughlin.

"We expect to see more and denser deployments of small cells as demand for mobile services increases and as 5G networks are built," O'Loughlin said.

The ACMA recently registered a revised version of the code which includes new, tailored consultation provisions dealing specifically with the deployment of small cells, and says these provisions are better suited to the rollout of small, rather than large infrastructure.

The new code also contains provisions that enable community consultations about mobile base stations to use digital communication channels, such as social media and email.

"The ACMA will closely monitor the deployment of small cells to ensure communities are consulted in line with the new version of the Code, and to identify any new concerns," O'Loughlin said.

#### Peter Dinham

### Not your copy of CommsWire? If so please join up!

All material on CommsWire is copyright and must not be reproduced or forwarded to others. If you have a trial subscription that you are finding valuable please subscnbe formally via subscriptions@itwire.com Subscriptions are very affordable for indivduals, corporate and small teams/SMB. Special deals and discounts for PR firms

For editorial, contact, Stan Beer, CommsWire Editor: 0418 516 720 | stan.beer@itwire.com To subscribe or advertise contact, Andrew Matler, CEO: 0412 390 000 | andrew.matler@itwire.com