CommsWire

Essential daily reading for the communications industry executive

An iTWire publication www.itwire.com Editor: Stan Beer Wednesday 20 March 2019

US AND UK AT LOGGERHEADS OVER HUAWEI 5G

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

US CLAIMS BRITISH TESTING OF HUAWEI GEAR INADEQUATE

US Government officials have warned that the way Britain is going about building its 5G networks could be a threat to its national security if it used equipment from Chinese telecommunications equipment vendor Huawei Technologies.

A report in London's ***Financial Times*** said senior American officials had criticised the UK's method of testing Huawei gear before it was used, claiming that it would be sufficient to avoid threats to the telecommunications system.

For nearly two years, the US has been pushing countries it considers allies to avoid using equipment from Chinese companies, Huawei foremost, in 5G networks.

But the US has produced no proof to back up its claims that these products could be used to spy for China.

Only Australia and New Zealand have fallen in line with Washington's dictates, but Wellington has now indicated that the initial refusal for telco Spark to use Huawei gear is not the end of the matter.

Huawei sued the US on 7 March, seeking to be reinstated as a telco supplier in the country.

The ***FT*** quoted one official as saying that Britain's testing method may have been sufficient in the past, but claimed that since 5G was based on software, changes could be effected by software updates after the equipment had been installed after testing.

This individual said: “One analogy that we can often use is, one minute you’re holding a 5G coffee cup that is transmitting back telemetric data on what the temperature is what the actual liquid is inside.

“And then the next moment that object can turn into something radically different.

“While a huge opportunity, it is also deeply concerning to us from the perspective of national security."

When the American official was asked about the UK National Cyber Security Centre which carries out tests on Huawei gear alongside employees of the company in a test centre built by the Chinese firm, he dismissed it as a "technical mandate".

And he added: “Ours is a much broader question about how trust is changing in the way in which 5G networks will work in the future.

“Right now, back doors exist by definition, that’s how the manufacturer runs the network.

“We understand that there are a number of different opinions about that. That’s the concern we have and we are making that very clear to our partners.”

Last month, as ***CommsWire*** **reported**, Ciaran Martin, the head of the NCSC, said that any likely risk posed by Huawei was manageable.

"Because of our 15 years of dealings with the company and 10 years of a formally agreed mitigation strategy which involves detailed provision of information, we have a wealth of understanding of the company," Martin said.

"We also have strict controls for how Huawei is deployed. It is not in any sensitive networks – including those of the government.

“Its kit is part of a balanced supply chain with other suppliers.

“Our regime is arguably the toughest and most rigorous oversight regime in the world for Huawei."

CommsWire has contacted Huawei for comment.

Sam Varghese

TELSTRA TURNS ON 5G AT ITS 10,000TH MOBILE NETWORK SITE

Telstra has turned on its 10,000th mobile network site, throwing the switch on a 5G site in the regional Australian city of Toowoomba.

Australia's largest telco says the new site in Toowoomba will not only provide better coverage to its customers in the area but is also a milestone achievement, representing a commitment to offer "connectivity to as many Australians as possible".

Telstra (then Telecom Australia) launched 1G in Sydney back in 1987 with just 14 base stations.

The telco says that today, its mobile network covers more than 2.5 million square kilometres – "vastly more than any other mobile network in Australia" – and offers coverage to 99.5% of the Australian population.

"Not only is our network getting bigger, it is getting faster and smarter.

"The new base station in Toowoomba includes the very latest technology as part of our 5G program," a Telstra spokesman said.

"Since passing 200 5G-enabled sites at the end of last year, our roll-out of 5G has continued in the major city CBDs with the plans to extend to a 2-kilometre radius of coverage from each city centre.

"Adelaide, Brisbane and Perth CBD roll-outs are already well progressed, as are Launceston and Hobart, and we are in the process of extending coverage in the CBDs of Sydney (including some coverage in Parramatta CBD) and Melbourne as we work towards the launch of our first 5G mobile devices.

"Toowoomba has been at the heart of this – as the first regional centre where we introduced 5G capability.

"Indeed, with more than 100 5G mobile sties now installed in Brisbane, the Gold Coast and Toowoomba – and with the region playing host to our 5G Innovation Centre (where a number of 5G world firsts were achieved) as well as our first 5G customer trial – Queensland could be considered the 5G capital of the world."

Peter Dinham

EXPLOITING NBN POTENTIAL CAN IMPROVE SITUATION: ECKERMANN

Writing down the value of the NBN to take the pressure off NBN Co trying to increase the ARPU and allowing more of the performance potential, that exists, to be made accessible, could improve the existing situation, networking veteran Robin Eckermann claims.

Eckermann, an adjunct professor at Canberra University and one of the people behind the TransACT network, told *CommsWire* in response to queries that any write-down would need a restructuring of the wholesale pricing model as well.

"For example, [there could be] elimination of the artificial CVC bottleneck on performance, establishment of 50Mbps as the minimum speed and, perhaps, introduction of traffic quotas on low-priced 'entry-level' plans to ensure that high-speed fixed broadband is available to most Australians," he said.

The first step, Eckermann pointed out, needed no re-engineering, but rather the ministerial pen. "The network revenue foregone would be more than offset by the broader socio-economic and environmental benefits to Australia across every sector (health, education etc)," he said.

"The subsequent focus should be on upgrading the weakest areas of the network, starting with the lowest-performing fibre-to-the-node areas to (at least) fibre-to-the-distribution-point. This will take time and will be costly, and it would best be undertaken in a calm and considered manner, insulated from the political point-scoring that sadly characterises the history of the NBN to date."

In the case of FttDP, the length of copper that forms the last bit of the connection is typically less than 40 metres. In the case of FttN, the lead-in copper cable can be even a kilometre.

Said Eckermann: "Contrary to the views of some, the NBN is not a 'train wreck'. It is not 'unusable' – just ask the many Australians already using it quite happily. However, changes are needed going forward if the original vision and associated benefits are ever to be fully realised."

He refused to back the opinions of "experts who attribute all NBN problems to the adoption of additional last-mile technologies - notably FttN. In my view, their positions are more ideologically and politically-based than well-founded in facts or real-world experience. Their extreme and emotional claims contribute little to navigating a sound way forward with the NBN".

Eckermann said there was not a soul who would deny that FttP offered the ultimate in fixed-broadband connectivity. But, he added, the high cost of taking new cabling into homes was generally under-estimated.

"Costs are what they are, and arguments that they should be reducing at a faster rate are less convincing than real-world data," he said.

"FttN can deliver 100Mbps performance for users located sufficiently close to the node, but according to NBN Co, about a third of the lines are not capable of 50 Mbps. In due course, these areas of the network will need upgrading – and the cost will undoubtedly be greater than if fibre had been taken deeper into the network from the outset."

He took aim at recent claims over speed on the Australian network saying, "Most recently, NBN detractors seized upon Australia’s lagging national average fixed broadband download speedtest result as 'proof' of the shortcomings of FttN".

"The logic was sadly flawed! The speedtest results are based on a broad sample and, as of the latest weekly progress report, less than five million NBN services had been activated against an eventual population of some 12 million premises due to have access to the network. The figure is, therefore, not a meaningful reflection of NBN performance."

Eckermann said in looking just at the NBN, the end-user’s self-selection of the lower 12Mbps and 25Mbps speed tiers was inevitably going to drag down average performance.

"It is true that a small proportion of FttN users may be selecting these speeds because their lines are not capable of higher speeds," he said.

However, this does not account for the vastly larger number of users who have access to higher speeds (including users on FttP connections) but who are still choosing 12Mbps or 25 Mbps services! It is hard to escape the conclusion that pricing and affordability isn’t a factor in their choices."

He said, in his opinion it was possible to estimate an average download speedtest result on the NBN by taking a weighted average across the different speed tiers (12/25/50/100 Mbps) – "the result is around 35Mbps. However, using information disclosed by NBN Co on the performance of FttN lines, it is also possible to estimate the average download speedtest result that would be achieved if all lines across all technologies were allowed to run at their full potential. The result is about double!"

Eckermann also took aim at another claim: that NBN Co would fail to achieve its revenue targets because of adopting the multi-technology mix "and, in particular, that bogeyman of technologies, FttN".

"Presumably the inference is that there is overwhelming demand for speeds that only FttP can deliver – so NBN Co is missing the opportunity to sell heaps more high-speed services at premium prices. The fact that so many people who already have access to such speeds are still opting for 12/25 or 50Mbps highlights the invalidity of this claim."

Sam Varghese

ONLY POLITICIANS EXEMPTED FROM ENCRYPTION LAW THEY PASSED

The Federal Government's encryption law spreads its net far and wide in society, but exempts one class of person — politicians — from its tentacles, according to an analysis of the law by lawyer and consultant Matthew Shearing.

"This Bill (which is now law) has a number of small but powerful provisions tucked away in its 220 pages – but none might raise more eyebrows than the provision regarding members of Parliament," Shearing pointed out in his analysis which came to ***CommsWire's*** notice after ***InnovationAus*** editor James Riley mentioned it.

"While the rest of the Australia (and in many cases, the world) is subject to the new legislation, the only people who are expressly excluded from everything in the Bill are the very people who rushed it through Parliament in the first place – the politicians."

And in a sarcastic aside, he added: "It's not a big deal though – it's common knowledge that our politicians are the most trustworthy and transparent of anyone in our society.

"I, for one, am glad they have blanket immunity."

A great deal of Shearing's analysis of the bill covers well-worn paths.

The difference is, however, that he has used plain English unlike some pundits who have laid claim to tell people "everything you wanted to know about the Assistance and Access bill".

Shearing mentions the danger that the law poses to the technology industry in Australia many times.

"If I was advising an international company on this Bill, I'd say they must assume that any data originating in Australia is being routed via Australian intelligence servers," he wrote.

"I'd also say there's a the much higher chance that Australian software will be breached by hackers and malicious actors.

"I suspect many experts will recommend avoiding Australian software and staff altogether – which some organisations have already begun doing.

"This is tough, because most Australian companies probably haven’t been served with a notice yet.

"Business, however, is cold and pragmatic, and there’s little room for doubt when you’re talking about data security.

“It’s entirely possible that, when weighing options for service agreements or software development, one of the first questions asked will be 'Who has an Australian presence?'

"Much in the same way that low university grades are filtered out of job application processes early, being ‘Australian made‘ may get you automatically removed from shortlists quicker than you can say 'there should have been a referendum on this'.“

Also listed in his analysis are a number of measures that can be taken to minimise the impact of the law.

One that Shearing cites is, "Wherever possible, put measures in place to monitor your software for unauthorised alterations and suspicious activity from your employees.

"The Bill gives authorities the power to compel employees to make changes without the knowledge or involvement of anyone else in a company.

“If you’re unaware of the existence of a notice, you must treat any unauthorised alterations as a cyber attack and deal with it accordingly."

And his advice to international firms does not sound good for Australia.

"If you’re an international company, seriously consider if you still want to do business in Australia.

“You may save a lot of time and money by simply excluding Australia from your business until our government comes to their senses.

“How overseas companies will interact with this Bill (and what they can be forced to do) is still something that requires further thought and will probably form a Part 2 of this article."

An **inquiry** is now underway into the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 by the Parliamentary Joint Committee on Intelligence and Security.

The PJCIS is expected to submit a report to the Government by 3 April.

Sam Varghese

ERICSSON SELECTED BY TDC FOR DANISH NATIONAL 5G ROLLOUT

Swedish telecommunications equipment supplier Ericsson has been selected by Danish service provider TDC to roll out nationwide commercial 5G, as part of a major network overhaul, and to provide managed services through the Ericsson operations engine.

Ericsson says the collaboration also encompasses R&D innovation which will enable TDC to help mobile broadband subscribers, enterprises, industries, and society to capitalise on 5G, the Internet of Things, and Industry 4.0.

Ericsson will modernise TDC's entire radio access network network with the latest solutions from Ericsson Radio System, while TDC's core network will be modernised with Ericsson's dual-mode 5G Cloud Core solution.

The rollout of Ericsson 5G New Radio hardware and software products will begin in 2019 in line with 5G licensing obligations.

TDC will make 5G available to selected customers under pilot testing from mid-2019, with the actual 5G network rollout expected to be initiated in October – pending the anticipated approval and availability of licensed 5G spectrum.

TDC is targeting the end of 2020 to provide nationwide 5G coverage in Denmark.

The companies have also signed a five-year managed services contract, centred on the artificial intelligence- and automation-driven Ericsson Operations Engine, which will see Ericsson operate TDC's network from September 2019.

It encompasses network operations, field services, customer experience management, network planning and optimisation. TDC customers will benefit from network performance powered by Ericsson's global scale, processes, artificial intelligence and automation solutions.

Under the agreement, about 100 network operations professionals will be transferred to Ericsson.

Ericsson says the strengthening of the TDC-Ericsson partnership means TDC's subscribers will be among the first in Europe to benefit from new 5G-enabled enhanced mobile broadband experiences, including gaming, infotainment, streaming and interactive services.

TDC and Ericsson will also collaborate to drive joint 5G-enabled innovation activities, tapping Ericsson's global R&D ecosystem, including Ericsson's closest physical R&D facility in the Öresund region of Lund, Sweden.

Peter Dinham