CommsWire

Essential daily reading for the communications industry executive

An iTWire publication www.itwire.com Editor: Stan Beer Monday 15 April 2019

HUAWEI 5G BAN BREACHES WTO RULES: CHINA

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

CHINA TELLS AUSTRALIA THAT 5G BAN MAY BREACH WTO RULES

China has told Australia that its restrictions on 5G technology are discriminatory and likely to have broken global trade rules drafted by the World Trade Organisation.

The exchange, **reported** by ***Reuters***, took place at the WTO in Geneva on Friday, with Beijing's representative to the organisation's Council on Trade in Goods saying steps taken by countries to restrict 5G technology had a big effect on international trade.

The Chinese representative also said that such measures would not help in better cyber security but would only serve to isolate countries technologically.

Australia banned the use of equipment from Huawei Technologies in its 5G networks last August, citing risks to national security.

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 Washington 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 **indicated** that the initial refusal for telco Spark to use Huawei gear is not the end of the matter. That stance was **reiterated** by Prime Minister Jacinda Ardern during a one-day China visit in April. Huawei **sued the US** on 7 March, seeking to be reinstated as a telco supplier in the country.

In its statement issued in August, Canberra made no mention of either Huawei, or another Chinese firm, ZTE Corporation, whose products were subject to a similar ban.

The Chinese diplomat at the WTO said Australia had not made official any reasons for the ban, which seemed to have taken effect well before the law in question was promulgated on 18 September 2018.

“Country-specific and discriminatory restriction measures can not address the concerns on cyber security, nor make anyone safe, but only disrupt the global industrial chain, and make the country itself isolated from the application of better technology,” the Chinese representative told the meeting.

WTO rules prohibit any member country from discriminating against other members and preventing imports from any one country.

However, "national security" can be cited to obtain an exemption though this method of evading a rule was not practised as WTO officials feared it would become common practice.

A WTO ruling clarified that, apart from war and the arms business, national security meant “a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state".

Sam Varghese

GERMANY GIVES CLEAR INDICATION THAT NO BAN ON HUAWEI

Chinese telecommunications equipment vendor Huawei Technologies will not be shut out from Germany's 5G networks, with Berlin's telecommunications regulator signalling that the firm would not be kept out despite US pressure.

The president of the federal network agency, Bundesnetzagentur, Jochen Homann, **told** London's ***Financial Times*** that the position the agency took was that no supplier, including Huawei, should be specifically excluded.

Last month, it was **reported** that the American envoy to Germany, Richard Grenell, had written to German Economy Minister Peter Altmeier, saying that if any Chinese vendors were allowed to supply equipment for the 5G networks in Germany, then the US would cut down on its intelligence co-operation with Berlin.

Also in March, Germany **said** it had tightened security criteria for all vendors who supply telecommunications equipment to the country's telcos.

Equipment for all critical communications networks should be vetted by the country's cyber security watchdog, the Federal Office for Information Security (BSI), and undergo security checks by a BSI-approved testing body, the Bundesnetzagentur said.

Though the US has been repeating claims that Huawei's technology poses a security risk, Homann said the Bundesnetzagentur had yet to see any evidence to back up these claims.

“The Bundesnetzagentur has not received any concrete indications against Huawei. Nor are we aware of any other body in Germany that has received any reliable indications," he said.

In February, it was **reported** that a small group of German ministries had reached preliminary agreement on Huawei, with a decision to snub the US.

The auction of 5G spectrum in Germany began in March and four operators are **competing** for licences – Deutsche Telekom, Vodafone, Telefónica and Drillisch.

Another factor mentioned by Homann was the fact that telcos were already using Huawei technology in their systems. Added to this, the fact that the Chinese behemoth held a large number of 5G patents would delay the roll out of 5G in Germany.

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

That stance was **reiterated** by New Zealand Prime Minister Jacinda Ardern during a one-day China visit in April. Huawei **sued the US** on 7 March, seeking to be reinstated as a telco supplier in the country.

Sam Varghese

HAWAIKI BROADENS US NETWORK WITH NEW POP IN SEATTLE

NZ cable operator Hawaiki Submarine Cable has extended its presence in the United States from Hillsboro, Oregon, to the Westin Building Exchange carrier data centre in Seattle to support its clients' capacity requirements between NZ, Australia, and the US.

The Hawaiki trans-Pacific cable, launched in July 2018, is a 15,000-km fibre optic deep-sea, carrier-neutral cable with a design capacity of 67Tbps.

It is the fastest and largest capacity link connecting Australia and New Zealand to Hawaii and mainland United States.

A statement from the company said Hawaiki selected the Westin Building Exchange as it had a large number of global carriers, simplified connectivity options and available cloud services that had been the hallmark of the original trans-Pacific, terabit fibre hub on the US West coast.

"Choosing the WBX in Seattle was a natural but strategic decision for us," said Hawaiki chief executive Remi Galasso.

"With over 250 carriers, cloud and content providers within their ecosystem, we could not have found a more ideal location."

Hawaiki has now expanded its reach in the US and provides PoP to PoP capacity between Sydney, Auckland and Seattle to its customers.

"At WBX, we are simplifying access to carriers, companies, clouds, countries and continents," said Michael Boyle, strategic planning director with WBX.

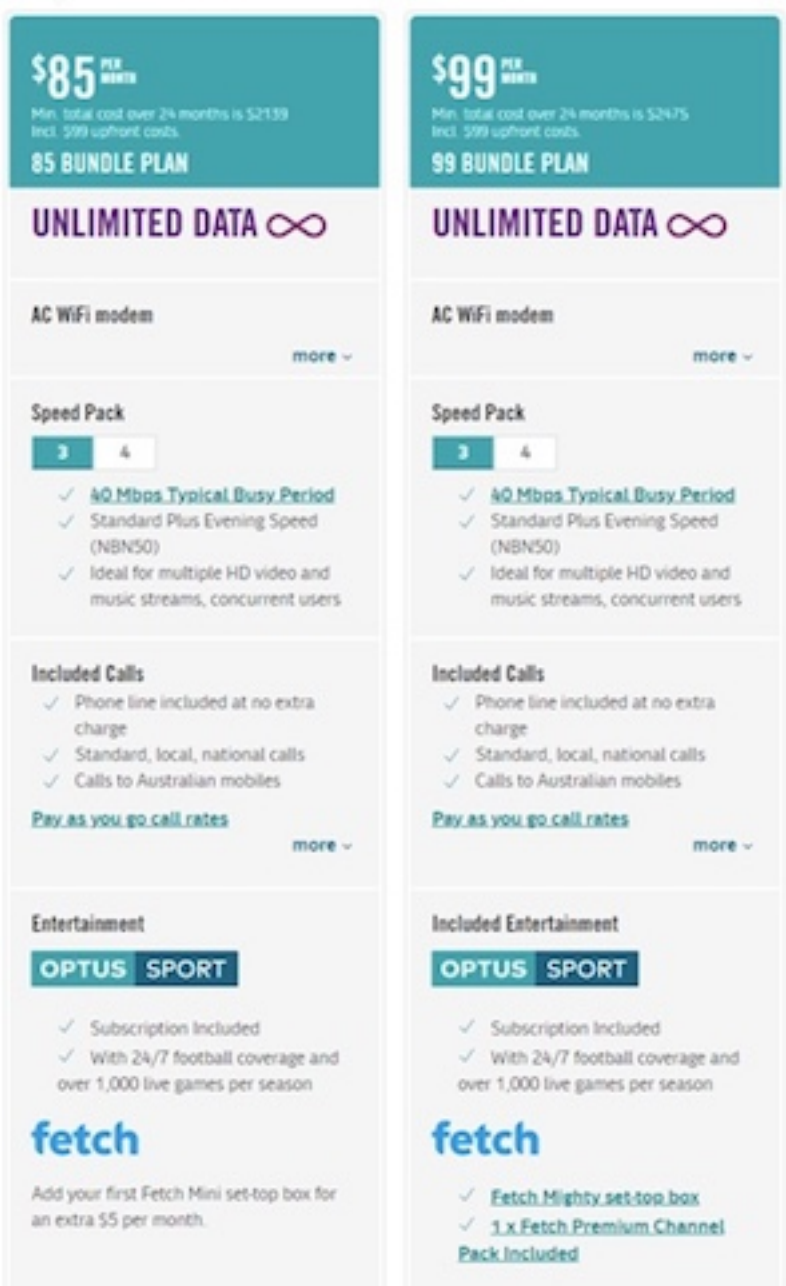
"The reason organisations like Hawaiki establish a presence with the Westin Building Exchange is due to the availability of multiple, cost-effective connectivity options and direct access to all major carriers and cloud providers, located in our building."

Sam Varghese

OPTUS LAUNCHES NBN PLANS AHEAD OF 'NEW CUSTOMER INITIATIVES'

Optus has launched three new NBN plans detailing promises of more speed for selected home users, and with unlimited data for "data hungry" streamers.

Optus' new offerings include two new NBN broadband bundle plans, which include a phone line at no extra charge for $85/mthi and $99/mth and a broadband only plan for $85/mth.



The plans have unlimited data on Optus' Speed Pack 3, which Optus says delivers 40Mbps typical evening speed (7-11pm) across its new NBN plans.

Optus Head of Product, Shawn Van Graan said, "We are unveiling our new NBN plans, offering customers fast NBN speeds, with some great features that are perfect for families and data-hungry streamers."

"As part of these plans, customers will receive an Optus Sport subscription and those who sign up to the $99/mth bundle plan (Min total cost $2475) will also receive a Fetch Mighty set top box and one premium channel pack.

"All standard, local and national calls, plus calls to Australian mobiles will be included as part of our two broadband bundle plans."

"The three new plans will offer customers the option to sign up to a month to month contract, giving them the peace of mind to leave their plan at any time if they are not satisfied with the speed or service.

"These plans will be enhanced by some exciting new Optus NBN customer service initiatives, which ensure customers experience a smooth transition to the NBN. We will be announcing these details soon," Van Graan said.

Peter Dinham

ASD: 'SOPHISTICATED, STATE ACTOR' BEHIND PARLIAMENT ATTACK

The Australian Signals Directorate has ascertained that hackers who breached the networks of the Australian Parliament and those of the three main political parties are nation-state actors, but says it cannot name the country involved in a public forum.

ASD director-general, Mike Burgess, told the Senate Foreign Affairs, Defence and Trade Legislation Committee on 5 April that the attackers had exfiltrated a small amount of data.

Asked whether the ASD had identified whether it was a state actor, Burgess said: "The level of sophistication here leads us to believe it has to be a state actor.

“That's our assessment.

“Of course, that could still be just a very, very clever individual, but we think that's highly unlikely."

He said the question of calling out any country for the attack was a matter for the government, once the ASD had presented its assessment.

In response to a question as to whether any confidential correspondence or information had been compromised, Burgess said: "There was a small amount of data taken; none of that was deemed sensitive, but the assessment of that is a matter for the parliament themselves."

The intrusion was **made public** on 8 February.

On 24 March, the ASD **told** ***CommsWire*** in response to queries that the investigation was still ongoing.

Burgess told the parliamentary panel that the damage assessment from the intrusion had been completed and the intruder or intruders had been fully evicted.

Questioned about whether any country would be called out for being behind the attack, Burgess replied: "Attribution is a really difficult thing, so tying it down to a particular country, a particular organisation, and perhaps particular individuals, is a piece of work that takes considerable time.

“Even if we got to that point, whether that got called out or not is a matter for other organisations — the government — not for the Australian Signals Directorate.

"I would say, though, that if you do get to the point of knowing who it is, sometimes you have an option of calling it out, and the Australian Government has taken action previously to call out state actors for known problems – that's an intent to call out inappropriate behaviour.

"Sometimes, however, there might be other reasons why you don't call it out, but I'll end with attribution: to get to the point where you could prove it in a court of law is terribly difficult."

There were competing claims at the time of the breach, with some organisations, like the ABC, **blaming** China, while Resecurity, a security outfit in the US, blamed Iran.

Resecurity said an Iranian-linked entity had been responsible for the network attack, adding that it had informed the ASD about its findings and claiming the agency had **confirmed** this attribution.

But the credentials of Resecurity **came under question** shortly thereafter, with journalists and technical researchers both citing what they saw as irregularities about its approach. The firm had also blamed Iran for a network attack on multinational software company, **Citrix Systems**.

Sam Varghese