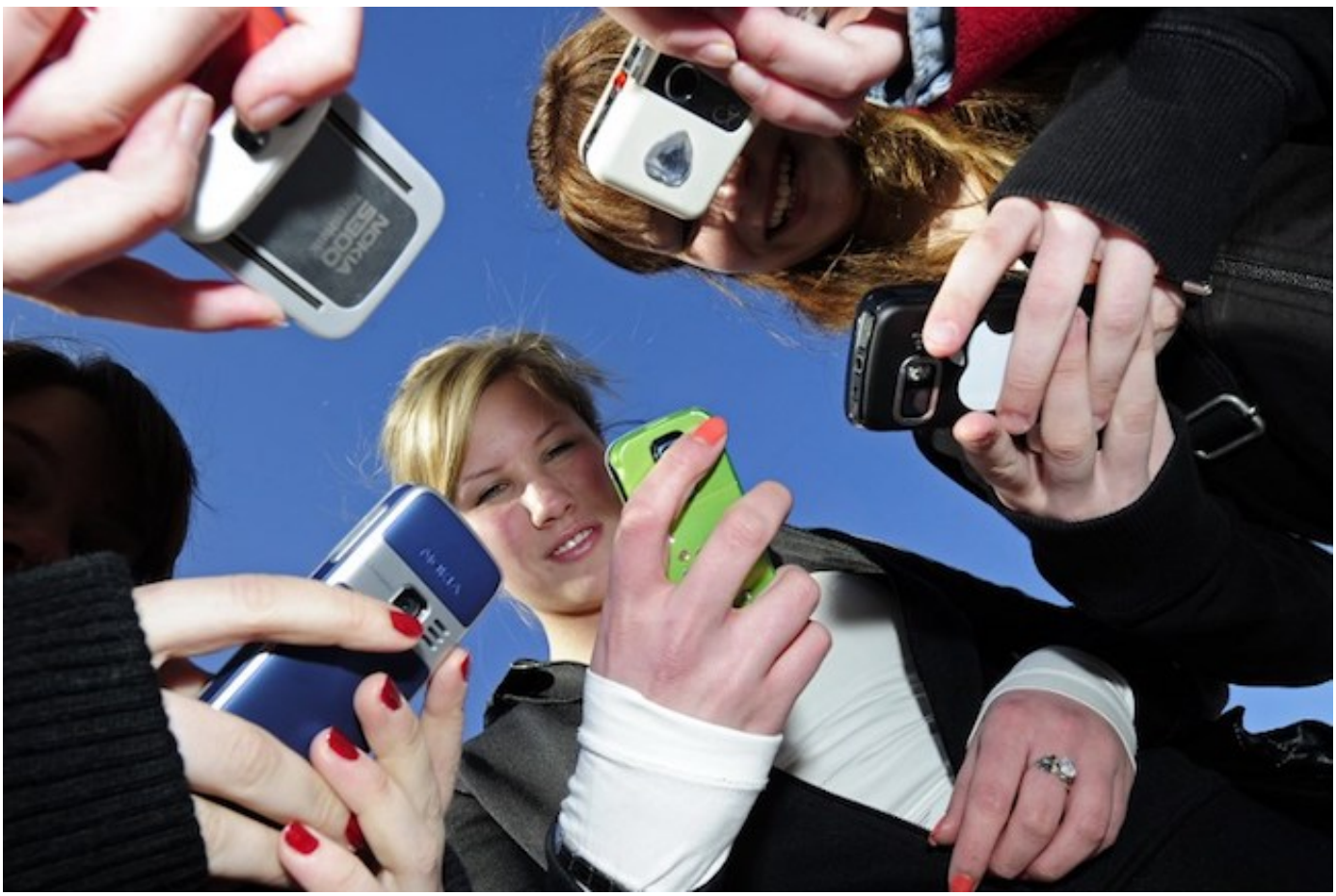
CommsWire

Essential daily reading for the communications industry executive

An iTWire publication www.itwire.com Editor: Stan Beer Wednesday 26 June 2019

VIC PUTS FOOT DOWN ON MOBILES IN SCHOOLS



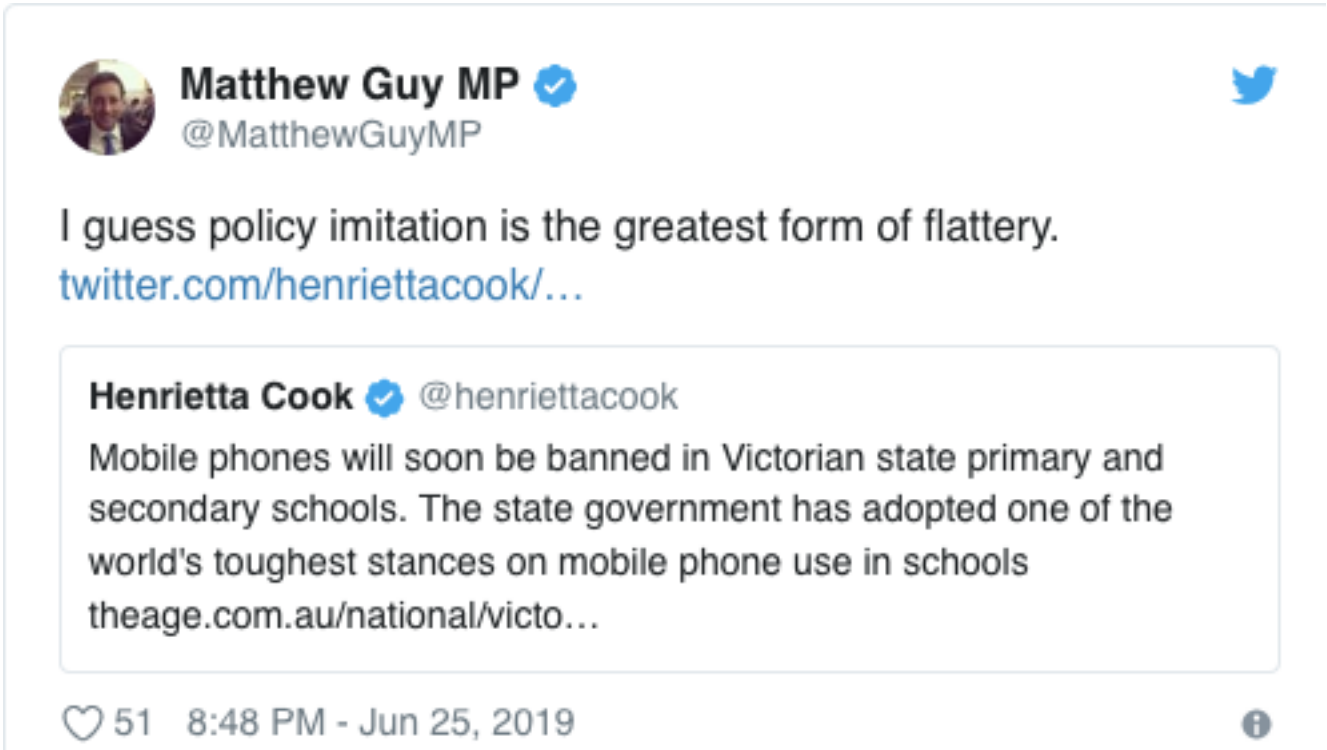
CommsWire (ISSN 2202-4549) is published by iTWire Pty Ltd. 18 Lansdown St, Hampton, Vic, 3188
CommsWire/Telecommunications Editor: Stan Beer
Staff writers: Peter Dinham, Alex Zaharov-Reutt, Sam Varghese. Columnist: John de Ridder
Advertising: CEO and Editor in Chief, Andrew Matler: andrew.matler@itwire.com • Tel: 0412 390 000

VICTORIA TO BAN MOBILE PHONES IN STATE SCHOOLS FROM 2020

The Victorian Government will ban the use of mobile phones during school hours in state schools from the beginning of the school year in 2020, with the state's Education Minister James Merlino saying the ban is aimed at stopping cyber-bullying.

Merlino is set to formally announce the policy on Wednesday, something the former Liberal National Government had promised to introduce in 2018.

The ABC **reported** that under the new rules, mobiles would have to be kept in lockers during school hours. The only exceptions would be if a student wanted to use a device for medical reasons or if a teacher allowed use for a specific classroom task.



Merlino was quoted as saying: "This is for all state schools, government primary and secondary schools. We can't impose such a ban on our non-government sector [such as] Catholic and independent schools."

Victoria is a year behind NSW where the state government introduced a ban from 2019.

NSW Premier Gladys Berejiklian and Education Minister Rob Stokes said the followed an expert review showing rising cases of online bullying, inappropriate sharing of explicit images, predatory behaviour from strangers and unnecessary distraction for students.

Well-known child psychologist Dr Michael Carr-Gregg led the survey, which received about 14,000 responses and 80 submissions.

The UK introduced **partial bans** in 2007. France **introduced** a full ban in September 2018.

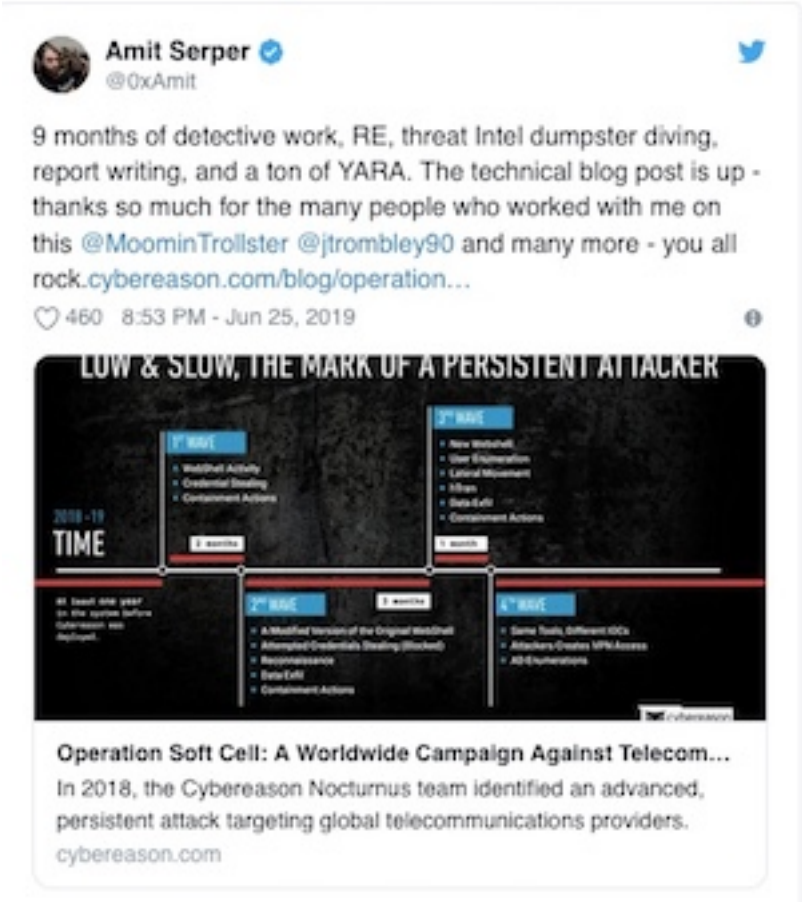
Sam Varghese

'NO IOCS OR VICTIM ACCOUNTS': EXPERT QUERIES APT10 COVERAGE

A well-known researcher from security outfit Chronicle Security has questioned tech and mainstream media blanket coverage to research by the US/Israeli firm Cybereason, which detailed intrusions into a number of telecoms firms by a Chinese group known as APT10.

Juan Andres Guerrero-Saade, who formerly worked with Kaspersky, said in a tweet that additionally the APT10 group had already been publicly written about by BAE, PwC, Kaspersky, FireEye and CrowdStrike.

"With such a broad claim, who would publish a story unsubstantiated by IoCs (indicators of compromise) nor victim accounts?" he asked.



He added a conciliatory note to Amit Serper of Cybereason, one of the researchers involved in the APT10 findings.

"No offence to Cybereason or @0xAmit," Guerrero-Saade wrote.

"Just wish the reporters had sprung for greater context or verification."

Serper responded by saying that the company had various restrictions put in place that prevented it from providing IoCs.

"We have all sorts of restrictions that keep us from publishing any IoCs since this is a targeted attack and a very sensitive issue that's being investigated," he wrote in a tweet.

"Rest assured that the relevant people have the IoCs.

“Wish I could share them, but I can't."

And he added: "I fought hard to be able to share IoCs and I lost.

“I wish I could get into the 'why' but I can't.

“For those reasons exactly.

“You can take my word for it or not, I'll respect you either way."

In **its research**, released on Tuesday US time, researchers Mor Levi, Assaf Dahan and Serper wrote that the operation, which they dubbed Operation Soft Cell, had been active since at least 2012 and was aimed at obtaining CDR data (call logs, cell tower locations etc).

The blog post detailing Cybereason's findings said the campaign, given the name Operation Soft Cell, had targeted 20 military officials, dissidents, spies and law enforcement officials all of whom were and took place in firms across Asia, Europe, Africa and the Middle East.

The release of the Cybereason research comes at a time when the US and China are locked in a trade war that has substantially elevated bilateral tensions.

Guerrero-Saade's scepticism is not without reason, as there have been at least two instances of so-called big technology yarns in the recent past turning out to be highly questionable.

Last year, the news agency Bloomberg published **claims** that security testing by Amazon in 2015 had revealed the existence of tiny chips that were not part of the original mainboard design.

It said that this led to an extensive investigation by US Government agencies which found servers built using these boards in data centres belonging to the Department of Defence, on warships, and for processing data being handled by CIA drones.

The story drew denials aplenty from the companies involved and also the government. No proof has ever been offered to back it up.

Again, in 2018, an Israeli outfit known as CTS Labs published **details** of a number of flaws in AMD processors after giving AMD just 24 hours to respond to their claims.

The firm set up a separate website for this, and the findings were accompanied by a white paper in which technical details had been redacted.

Soon after this, a company named Viceroy Research issued an analysis with the dramatic headline: "AMD – The Obituary". It appeared to be an effort to push down AMD's share price.

There was plenty of pushback at the time and the whole episode has now been more or less forgotten.

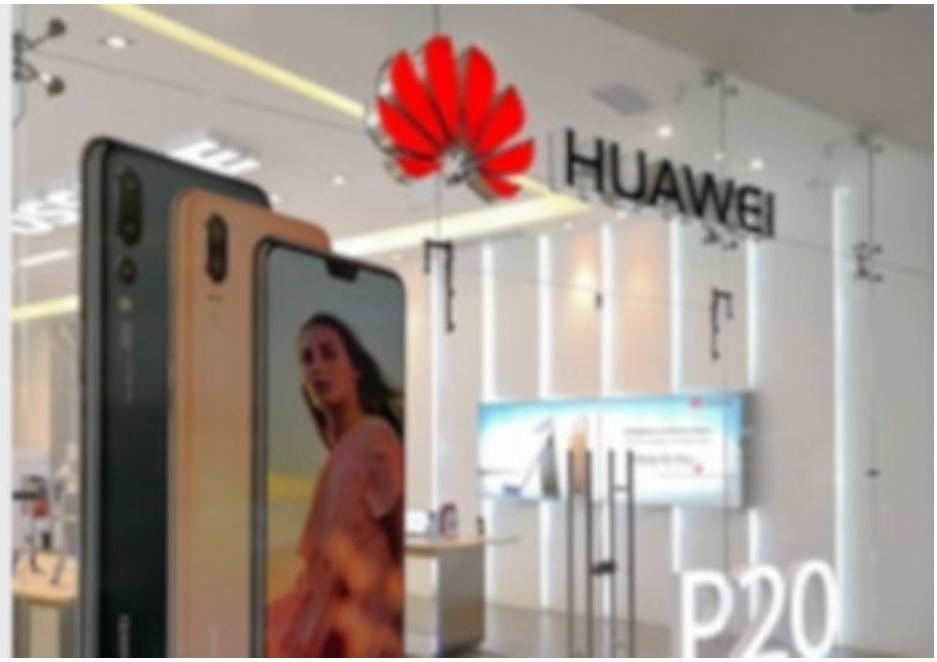
Sam Varghese

HUAWEI GEAR MORE VULNERABLE THAN THAT OF RIVALS: CLAIM

A hitherto unheard of company, Finite State, has claimed that telecommunications products made by Chinese equipment vendor Huawei Technologies are more likely to contain flaws that could be used for malicious activity than gear made by its rivals.

The rivals in question are Juniper and Arista. Not, as one would think, Ericsson and Nokia.

This is from **a report** in ***The Wall Street Journal***. But some serious questions hang over it and it looks like the kind of propaganda that is common in US mainstream media when an agenda needs to be pushed.



At the moment it is the question of Huawei's security credentials; the next US-China summit is a few days away and every little bit of pressure helps.

On Tuesday, the US/Israel security firm Cybereason **claimed** that numerous telcos had been breached by a group known as APT10, which it said was tied to China. Cover of that report was **questioned** too.

Finite State is two years old. Its report — not even the title is cited — has only been shown to select entities.

The firm has no media contacts listed and has no way of being contacted apart from a web form meant for those who want to make business inquiries.

There is no phone number for the company on the site either.

The company's chief executive Matt Wyckhouse says in the ***WSJ*** report that the security report was done pro-bono and that the best way to inform policy makers of these issues is to make them public.

But the company's website has no copy of this "research" for public examination.

The report says Wyckhouse plans to publish it this week. That's akin to putting the cart before the horse, but I'll let it pass. And his aim? "We want 5G to be secure." Noble, indeed.

Certainly not to meant to drum up business by approaching the ***WSJ***, then.

The ***WSJ*** claims that "cyber security experts" from the company have made the claims and "top US officials" say they appear credible.

Those top officials are unnamed White House officials, Christopher Krebs of the US Department of Homeland Security, Michael Wessel of the US-China Economic and Security Review Commission, a committee that advises Congress, and Republican Representative Mike Gallagher.

That is indeed a non-partisan bunch who can be relied on to give an unbiased verdict.

It is not stated whether either of the ***WSJ*** reporters, whose bylines appear on this piece, has the technical qualifications to evaluate a report that makes the claims it does.

It was not shown to any third-party security expert either.

To quote the ***WSJ***: "Finite State said it used proprietary, automated systems to analyse more than 1.5 million unique files embedded within nearly 10,000 firmware images supporting 558 products within Huawei's enterprise-networking product lines."

What products we do not know.

To add to its credibility, the ***WSJ*** report says unnamed sources found that the Finite report "broadly aligned" with a report from the UK National Cyber Security Centre issued in March.

Exactly what "broadly aligned" means we are not told.

To refresh public memory, ***CommsWire*** **reported** that the British report in March found "concerning issues" in the company's approach to software development, significantly increasing risk to operators and needing ongoing management and mitigation.

But it said it was not part of its functions to advise UK telcos on their purchasing decisions and did not recommend a ban on the use of Huawei equipment.

The report was issued by the Huawei Cyber Security Evaluation Centre Oversight Board.

Huawei was asked about this Finite State report – but not provided a complete copy to make a judgement.

That, perhaps, says the most about this effort by the ***WSJ***.

Sam Varghese

US SUPPLIERS FIND WAYS TO EVADE BAN ON SELLING TO HUAWEI

At least two big American semiconductor manufacturers have used loopholes in the US ban on supplying parts to Chinese telecommunications equipment vendor Huawei Technologies and shipped goods to the company from units that operate outside the US.

The New York Times, citing anonymous sources, **reported** that Intel and Micron were among the American companies that had found ways to evade the ban, imposed on 16 May, beginning about three weeks back.

The Trump administration **placed** Huawei and 68 of its affiliates on its Entity List on 16 May, meaning that the company would have to seek permission to purchase any American components it needed to manufacture its products.

Micron chief executive Sanjay Mehrotra **told investors** during a conference call following announcement of the company's third quarter results on Tuesday that shipments of some products to Huawei had resumed in the last fortnight.

"To ensure compliance [with the US ban], Micron immediately suspended shipments to Huawei and began a review of Micron products sold to Huawei to determine whether they are subject to the imposed restrictions," he said.

"Through this review, we determined that we could lawfully resume shipping a subset of current products because they are not subject to Export Administration Regulations and Entity List restrictions.

“We have started shipping some orders of those products to Huawei in the last two weeks."

On 21 May, the US Commerce Department **eased** some of the restrictions until August, allowing Huawei to maintain and update existing networks and handsets.

Google **announced** on 20 May it was cutting off Huawei's access to future updates of Google's Android and Google Play Store.

Mehrotra added: "However, there is considerable ongoing uncertainty surrounding the Huawei situation, and we are unable to predict the volumes or time periods over which we’ll be able to ship products to Huawei.

"Micron will continue to comply with all government and legal requirements, just as we do in all our operations globally. Of course, we cannot predict whether additional government actions may further impact our ability to ship to Huawei."

The NYT report said goods made by US firms outside the country were not always considered American-made and suppliers were exploiting this loophole.

Last week, the Semiconductor Industry Association, a lobby group for companies in the sector, issued **a statement** about the Huawei ban.

"SIA companies are committed to rigorous compliance with US export control regulations," the organisation's president and chief executive, John Neuffer, said.

"As we have discussed with the US Government, it is now clear some items may be supplied to Huawei consistent with the Entity List and applicable regulations.

"Each company is impacted differently based on their specific products and supply chains, and each company must evaluate how best to conduct its business and remain in compliance.

"Over the longer term, SIA remains concerned restrictions on our ability to sell commercial products in major markets will erode the competitiveness of the US semiconductor industry.

“We continue to call on the US Government to help advance US semiconductor leadership as it works to preserve US national security.”

Also last week, a report **said** that American processor firms were lobbying the government to ease the ban on Huawei.

Qualcomm and Intel were among the companies said to be involved in the lobbying effort, the report said, adding that Intel and Xilinx had talked to the Commerce Department in May about the placement of Huawei on the Entity List.

Earlier this month, processor maker Broadcom **said** it expected to take a hit of US$2 billion in its full-year revenue due to the ban.

Huawei spent about US$70 billion on components worldwide in 2018 and about US$11 billion of that was spent with US companies.

A Huawei spokesperson told ***CommsWire*** the company was unable to make any further comment.

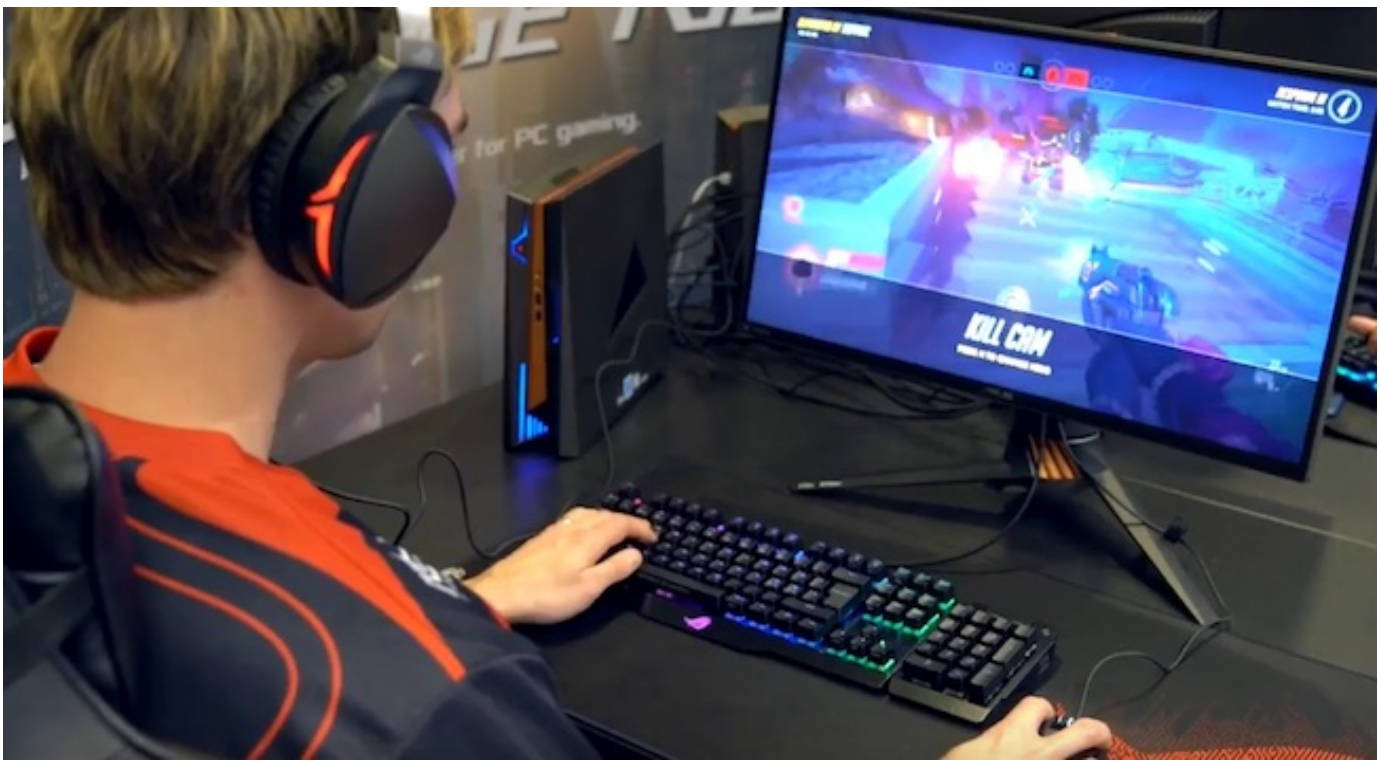
Sam Varghese

QUALCOMM, ZTE DEMONSTRATE 5G-POWERED CLOUD GAMING

Qualcomm Technologies and Chinese telecommunications equipment provider ZTE have demonstrated cloud gaming on a live 5G network utilising cloud gaming solutions from Tencent Instant Play on 5G smartphones from OnePlus, Vivo, Xiaomi and ZTE.

The demonstrations are taking place at MWC Shanghai, formerly known as Mobile World Congress Shanghai.

The display is aimed at demonstrating that console-quality mobile gaming experiences are achievable over live 5G networks and show the growth opportunity for the cloud-gaming ecosystem.



Qualcomm says the demonstrations will use China Telecom's live 5G network, ZTE's 5G NR commercial system infrastructure, and 5G commercial smartphones featuring its Snapdragon 855 mobile platform with the Snapdragon X50 5G modem with integrated RF transceiver and Qualcomm RF Front-End (RFFE) solutions.

Cloud gaming solutions provided by Tencent Instant Play leverage the cloud's capabilities for rendering and processing, while utilising high-speed 5G network to send users' commands to the cloud which streams back the rendered frames to local devices.

Qualcomm says this allows users instant access to graphically demanding games via 5G smartphones without the need to download and install on the devices, delivering a smooth "games on demand" experience.

“We believe that cloud gaming is one of the key trends in the future of the entertainment industry,” says Jian Wang, head of operations, Tencent Instant Play.

The arrival of 5G is expected to set off a new revolution in cloud gaming.”

“5G’s high speed and low latency make it an ideal connectivity fabric for cloud gaming which can support improved image quality, provide more fluent interactive experience, and effectively reduce the cost per user of services, thereby bringing high-quality gaming experiences to a wider range of users.

“We will continue to work on the enhanced cloud gaming experience based on various gaming scenarios and stay focused on innovative experience and high-quality content.”

Yanmin Bai, vice president, general manager of TDD & 5G products, ZTE said: “5G is here. As a global leader in edge-to-edge 5G solutions, ZTE has been working closely with operators and vertical sectors on exploring new 5G business models and use cases to achieve high network performance in those scenarios”.

“The power of these cooperative efforts is successfully displayed when the company and Qualcomm Technologies team up with multiple OEMs on 5G applications.

‘We will continue to work with our partners to contribute our parts to the 5G ecosystem and accelerate the industry’s maturity.”

Pomp Sheng, vice president, sales, Qualcomm Communication Technologies (Shenzhen) said, “China’s 5G era has officially begun, and it was accelerated from the original timeline thanks to the work of the whole mobile ecosystem”.

“With the readiness of 5G commercial networks, China is poised to have a fast large-scale 5G rollout.

“Within this year Chinese consumers will have access to numerous use cases and enhanced experiences, such as cloud gaming, powered by 5G and the Snapdragon 855 Mobile Platform.

“Qualcomm Technologies is committed to sharing opportunities with Chinese partners.

“And we are excited to be part of this extensive cooperation across operators, OEMs and content providers for facilitating the improved user mobile experience through 5G innovations.”

Peter Dinham