Name of the Client: RtBrick
Publication: Voice&Data
Date: 24 July 2020
URL: https://www.voicendata.com/unlock-5g-broadband-networks-make-secure/
Page: 1 of 2

Unlock 5G and broadband networks to make them more secure

By Pravin S Bhandarkar Founder and CEO, RtBrick

The recent pandemic has illustrated just how reliant we are on our telecom's infrastructure. And the widely acknowledged source of that pandemic, China, continues to be a concern to that same infrastructure, but for an entirely different reason.

The risk posed by Chinese state influence over 5G and Internet technology is a matter of increasing debate amongst national security organizations around the world.

For example, the governments of Australia, New Zealand, Japan, Taiwan, and the U.S. have decided to completely ban the use of Huawei technology in their core network infrastructure, with the UK and others limiting its deployment.

The incumbent telecom provider in the Netherlands, KPN, has excluded the Chinese company from the core of its 5G network, for example. Many more countries are still to decide.

It doesn't seem long ago that the telecoms network market was almost exclusively in the hands of US and European suppliers. But when Chinese equipment arrived on the scene, it was adopted faster than many observers might have predicted.

It came with a clear proposition – it worked and it cost less. The cost advantage of having development and manufacturing in south-east Asia has been hard for western companies to match.

Despite government concerns about the security risks, it seems inevitable that telcos operating in a competitive market will always base commercial supply decisions on cost above national security (whether that risk is real or perceived). So, is there any way around this dilemma without heavy-handed legislation, that in turn threatens free-trade agreements and international co-operation? As

it happens, there is. And it is a by-product of a massive shift in networking technology known as *disaggregation*.

Unlike computing equipment, telecoms infrastructure has always been built using integrated systems, with both hardware and software locked together from the same supplier. Due to advances in the performance of standard off-the-shelf silicon, this is no longer necessary. Next-generation telecoms networks, such as Deutsche Telekom's new access network, are being built using disaggregated systems, with hardware and software from different vendors – much like we've been used to in cloud computing and IT infrastructure.

So, how does this help our security dilemma?

Well, the hardware used in these disaggregated systems – known as bare-metal-switches – can also be sourced from Asian manufacturers. Taiwanese supplied switches can match or even beat the cost points of the Chinese vendors. But the control of these systems is all done by the software. It's this software that turns a bare-metal-switch into an Internet gateway or a 5G core router, and where the security can be managed. And the choice of software provider is completely independent to the hardware. Operators are no longer locked-in to the same vendor for both.

So now an operator can take advantage of the Asian cost points for hardware, and select its software from a trusted country. The software is easy to change if the operator, or the national government, decides the security landscape has evolved, without the need to replace any physical equipment.

It turns out that network disaggregation could be the key to both unlocking – and securing – our

###