To Protect Network Security, Regulate Software, Not Hardware

Worried about political opposition to buying from Huawei? Here's a short guide and a possible solution.

By Steven S. Ross / *Broadband Communities*

Huawei, the world's largest supplier of equipment for broadband networks, is under fire as a potential security risk. Governments in the United States, Australia, the United Kingdom and elsewhere have sounded their displeasure about using Huawei equipment. Germany has signaled approval, and many companies in other countries have shelved plans for Huawei purchases.

Is excluding Huawei fair? And if you are in the market for broadband equipment, what should you do?

Huawei is truly huge. Its annual revenues are about $100 billion, of which about half comes from consumer electronics and half from network gear. Of the network gear business, a quarter ($12 to $15 billion of about $50 billion) is from software sales and service contracts. With roughly $40 billion in network equipment sales, the company is about the size of all American suppliers combined.

These comparisons are tricky; like Cisco, Huawei has a supply chain with many third-party players. Many American firms specializing in access network products, such as Adtran and Calix, manufacture abroad – in China – but are turning themselves into software companies. Their network access equipment is becoming more and more commoditized, as is Huawei's.

Cisco, specializing in network core equipment, has its own custom chipsets. Huawei won't comment, but it seems to customize its core equipment more than its access equipment. Custom chipsets are tough to monitor for hidden functions.

Huawei has leveraged its volume in wireless and fiber, edge and core, to become a huge competitor in the emerging 5G market – a major reason for the extra scrutiny it's getting.

Huawei's growth accelerated around 2011 and faltered only in the past year or so as government opposition mounted worldwide. Growth started when Huawei solved nagging quality control problems and moved beyond copying established software. Holding Huawei circuit boards in hand, I was always impressed. They rarely had jumpers, which are a key indicator of bad design practice. Mechanically, they were first-rate, with quality connectors and brass and aluminum castings and extrusions. Through-board solder-and-cut mounts for chips on the boards were almost nonexistent. Chips that consumed much power were well sited on the boards to minimize local temperature hot spots.

However, Huawei boards often failed in the field anyway. Evidently, manufacturing defects at contract assembly plants were to blame. Huawei made good on solving its problems. It also took a few years to bring those issues under control, it seems. Revenues jumped. Competitors adjusted or died – or got deeper into trouble when they took shortcuts to compete. A competing Chinese vendor, ZTE, went through that experience. But it seems to have had even more support from the Chinese government than did Huawei. The Chinese military itself is a major owner of ZTE.

In short, Huawei has more than just low prices going for it.

One argument Huawei and its supporters make is that bad actors and the U.S. National Security Agency have had little difficulty penetrating modern networks, even with no involvement in equipment or software design. But penetration is far less an issue than, say, an entire carrier or an entire country's network going dead after a seemingly innocent software update.

That scenario is less plausible if all or almost all the action happens at the network edge. Malware would have to be inserted into millions of sites before being discovered. Wouldn't it be easier to simply knock out the constellation of GPS satellites upon whose timing signals so much of the internet depends? But some carriers and concerned countries already limit Huawei equipment to the edge and ban it from the core. These carriers say they can continue to do so, although 5G, in particular, blurs the distinction.

Another approach would be to allow Huawei to sell whatever equipment it wants but hand software off to multiple third parties. As network functions and software become more and more complex, that is not a trivial task – but it is not impossible, either. And although Huawei would potentially give up a quarter of its revenue to outside software vendors, it would collect licensing fees for little work.

This approach would complicate the work of hackers, who would have to attack multiple software families, even if most of them were related to open-source parents. And, of course, it would satisfy politicians in the United States and elsewhere as they seek to bring home some of the money spent in China. ❖

Contact the Hawk at steve@bbcmag.com.