

# Europe Struggles to Quit Chinese Telecom > Huawei and ZTE equipment remain despite security concerns

BY LUCAS LAURSEN

**I**n September, Huawei filed a complaint against Spain's rural 5G contracting process, because the tender made it too risky for bidders to include the Shenzhen, China, telecom giant's hardware. The filing is another step in the global telecom-equipment market leader's long, involuntary departure from Europe and other telecom-network markets around the world.

Huawei and ZTE, the other major Chinese-headquartered telecom supplier, are stuck between a law and a hard place. Two laws, actually: The equipment manufacturers are subject to a pair of laws in their home country that, if enforced, could require them to comply with security-related instructions from the Chinese government. On the other hand, other countries are writing stronger language into their telecom and security

regulations that limits the use of telecom equipment from suppliers subject to pressure like China's—although these regulations don't mention China directly.

In some countries, private companies are reading the writing on the wall: This past summer, a Spanish telecom operator, MasOrange, announced that it was voluntarily phasing out its use of Huawei and ZTE components in its networks over the next few years in favor of supplies from Stockholm-headquartered Ericsson.

Elsewhere, officials are dragging their heels. German officials met in July with domestic telecom operators to negotiate how fast to replace Chinese hardware. Many governments are requiring replacement only as network operators upgrade to 5G or, eventually, 6G to keep costs down. But that scheme provoked criticism from lawmakers who say

their governments are too complacent about China's control over their critical infrastructures.

"The Chinese can shut down or slow or meddle with the mobile network. It will devastate the European economy," says John Strand, the CEO and founder of telecommunications consultancy Strand Consult, in Copenhagen. Allowing the performance of telecom infrastructure to degrade over time or shutting infrastructure down altogether would be a major threat to any economy, and one that Huawei could hold over much of the world.

A July cybersecurity risk assessment by the European Commission concluded that installing too much Chinese-made equipment in the region's telecom infrastructure would be risky. The impact of any spying for a country like China the report calls "much harder to assess."

As a collective, the European Union agrees that it is risky to support critical telecommunications infrastructure, including 5G, with hardware from foreign equipment manufacturers. But the EU has lagged the United States in taking enforcement action. As of August 2024, only 11 of the EU's 27 countries had implemented explicit restrictions on Huawei or ZTE through legal powers, according to Euronews.

Some countries are taking the less confrontational approach of inserting language into their bidding processes that put so-called high-risk suppliers at a disadvantage, as in the Spanish rural 5G case. There, the tender terms require any winners to replace equipment from high-risk suppliers, even if the government makes the designation after installation. That happened in Portugal and Romania, where operators bet on Huawei equipment that those governments banned soon after, costing the operators significantly for removal and reinstallation.

Getting out ahead of such bans may be far cheaper: Strand estimates the one-time cost of ripping out existing Huawei radio access network (RAN) base stations and replacing them in Germany at only €29 per person. The cost was even lower in networks that had not yet installed as much Huawei 5G equipment: In 2019, Strand estimated that for Europe as a whole, it could be as low as €6.50 per person. ■



European Union nations—like Germany, where this Vodafone tower is located—are moving slowly when it comes to removing Chinese components from their cellular networks.