

PAMIR LLC

Meeting the challenge of China's growing 5G influence in developing economies

China's Belt and Road Initiative and its digital counterpart, the Digital Silk Road, threaten to displace US telecom and tech companies in developing economies in Africa, Latin America and the Middle East. How can US operators and network providers stand up to the challenge?

Mercy Kuo

PAMIR

Risk Data and Analysis to guide your decisions

Our analytical teams provide deep insight on geopolitical impact, risk landscape, and competitive strategies in foreign markets.

Pamir was founded in 2006 to help US corporations protect innovation, people and market share in foreign markets where there is no level playing field. Since then, we have served over 50 Fortune 500 companies in Agriculture, Aerospace, Automation, Biomedicine, Chemicals, Energy, Financial Services, Advanced Materials, Pharmaceuticals and Semiconductors.



Pamir Consulting LLC

8045 Leesburg Pike, Suite 220,
Vienna, Virginia
USA | 22182

Office: +1 703 783 5020
Mobile: +1 231 360 3408
Email: info@pamirllc.com
Website: www.pamirllc.com

Copyright Pamir Consulting LLC 2023

This is a confidential business communication and may not be used or distributed other than for its intended purpose and with permission. This information is provided for background, and for lead information only, and is not, by itself, to be used as a legal basis against the subjects of the reports.

All due care is taken to ensure that the information contained in the report is accurate and true at the time of the report, but as always, may require additional, independent validation and verification.

The Digital Silk Road

For decades, the telecom sectors in the US and China have coevolved. However, deepening mistrust between the two nations, tensions around the global rise of Huawei, and China's push to become a global leader in digital technologies such as edge computing, smart cities, IoT, AI, blockchain, and 5G represent the beginnings of a likely bifurcation as each party develops policies that aim to decouple technology stacks, supply chains, and markets, and influence the setting of standards.

The drivers for China have been its Belt and Road Initiative (BRI) and its digital counterpart, the Digital Silk Road (DSR). The aim of DSR is to increase Chinese companies' participation in the global development of information and communication technologies and to increase its influence in setting global technology standards.

Beijing wants Chinese companies to be involved at all levels of digital infrastructure construction: fiber optic and mobile equipment infrastructure, carrier services, and over-the-top providers of applications services. Ultimately, China wants its technology and communications sector to become a "cyber superpower".

At first, the DSR appeared to be a relatively vague strategy, however it is now becoming a coherent and strategic approach that offers country and region-specific solutions, particularly in the race to 5G.

China takes the lead in 5G

In 2020, Beijing created the IMT-2020 5G Promotion Group, an all-government, all-industry alliance to capitalize on 5G opportunities. The group's membership includes leading vendors in the Chinese telecom ecosystem, major research institutes and universities, operators such as China Mobile, China Telecom, and China Unicom, infrastructure suppliers such as Huawei and ZTE, and mobile device makers such as Oppo, Xiaomi, and Vivo.

At the same time, Beijing developed a long-term framework to ensure that major Chinese technology companies are not held hostage to US technology policies. This includes asking home-based tech and comms companies to minimize their reliance on the US supply chain and to use as many Chinese components as possible in their 5G build-outs. This five-year initiative, known as the Secure and Controllable program, is aimed at reducing reliance on foreign, specifically US, hardware and software.

China already has a strong digital infrastructure presence in emerging economies in Africa, the Middle East, and parts of Eastern Europe, Latin America, and Southeast Asia, which need low-cost, high-quality technology to expand mobile networks and broadband coverage. Because Chinese telecoms companies are state-backed, they can keep their prices low, and tailor solutions for poorer nations.

Chinese telecom companies also have access to low-cost labor and, importantly, to preferential loans from Chinese government banks, which they can then lend to their own customers – essentially subsidizing poorer countries.

The Chinese 'blueprint' for Africa, Latin America and the Middle East

Chinese telecom companies have followed a standard blueprint in these regions – establish themselves as a key supplier in the early development of the market, i.e., 3G and 4G, and put themselves in an advantageous position when it comes to network upgrades, i.e., 5G and future 6G, which is already taking shape, at least from a functional perspective.

In essence, China is making low-return investments initially with the aim of winning larger projects further down the line as economies develop. Often there is also a strategic goal in mind, such as access to the large lithium reserves in Chile and Argentina. In turn, it is increasing its influence over telecom standards across the globe.

A further incentive for poorer countries is that state-backed Chinese telecom companies often build local research and training centers to provide an educational and vocational boost to the local population. As a result, private Western telecom and tech companies are struggling to match China's state-backed proposition.

However, a growing number of countries are becoming concerned that Chinese-built 5G infrastructure, and proprietary technology standards, could increase the risk of espionage and surveillance, boost China's influence on local state politics, enable the censorship of content through filtering, or allow the storage of local data on Chinese servers.

Some of these concerns have already been borne out. For example, in 2020 a report provided to the Australian government revealed that a Huawei-built data center in Papua New Guinea (PNG) exposed PNG government files due to outdated encryption software and insufficient firewall settings.

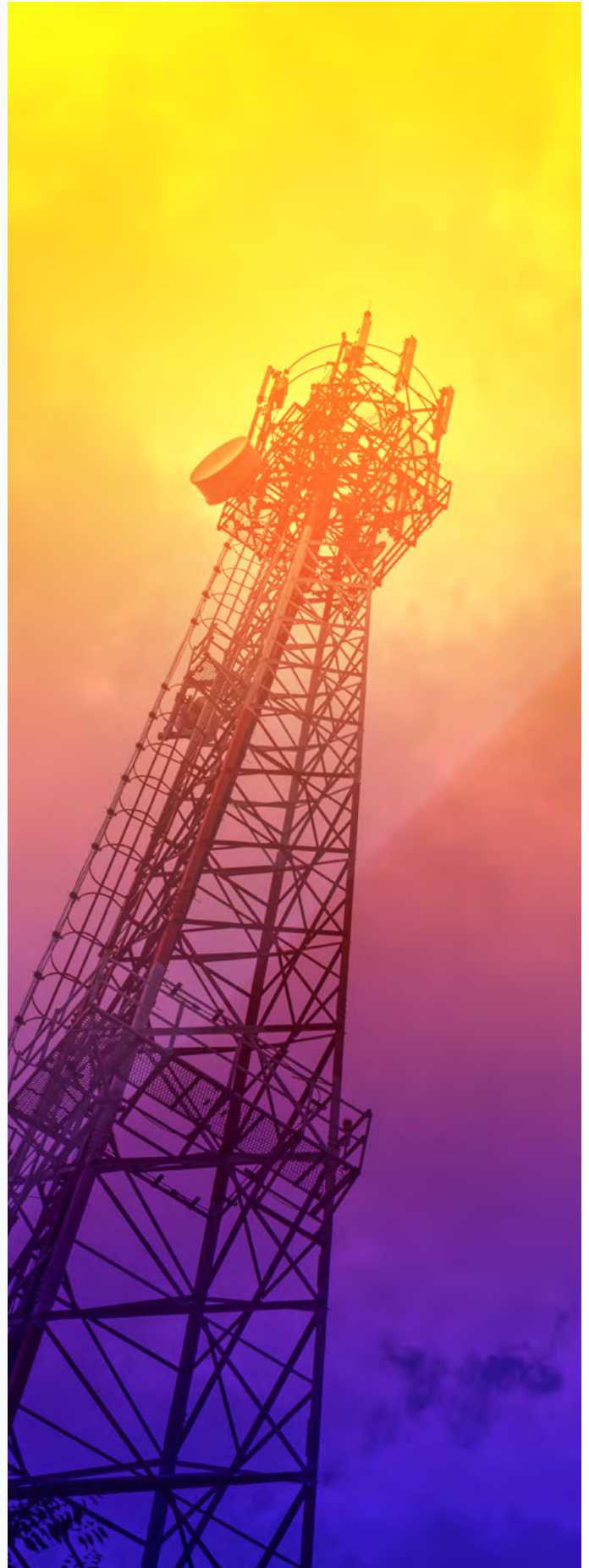
While, in 2018, French newspaper Le Monde reported that employees at the African Union headquarters found that the servers in a new conference center were sending content to Shanghai every evening, and that the building was planted with listening devices.

“China already has a strong digital infrastructure presence in emerging economies in Africa, the Middle East, and parts of Eastern Europe, Latin America, and Southeast Asia, which need low-cost, high-quality technology to expand mobile networks and broadband coverage. Because Chinese telecoms companies are state-backed, they can keep their prices low, and tailor solutions for poorer nations.”

As has been well documented, fears that security holes in Huawei equipment could be used for spying have led to the Chinese vendor being effectively banned from some Western countries' core 5G networks. The US has banned Huawei outright, while eight other countries – Belgium, Croatia, Finland, Greece, Norway, Portugal, Singapore, and Spain – have effectively banned Huawei from the 5G core network by contracting Nokia or Ericsson to build their networks. Canada banned both Huawei and ZTE from its 5G networks in May 2022.

The UK government, meanwhile, fearing that ripping out Huawei equipment would cause network blackouts and cost billions has served legal documents to UK operators stating that there must be no trace of Huawei equipment in any UK network by 2027. Operators have also been advised that Huawei not account for more than 35 percent of any 5G radio access network (RAN) by July 2023, but any operator using Huawei equipment in the 5G core by January 2023 will face punishment. The specific concerns were outlined in a clear policy directive from the National Cyber Security Council, which also identified which network functions are impacted.

US telecom companies face a real challenge competing with China in developing economies, but security concerns could also offer a platform on which to build. There are other weaknesses to the “Team China” approach too. For example, Malaysia and Myanmar recently declared their concern over perceived Chinese threats to their sovereignty and growing levels of debt to Chinese banks. Likewise, India recently proclaimed its concern over Chinese-built infrastructure and data security.





Open RAN: More than the sum of its parts?

Raising awareness around Chinese 5G security concerns might provide a “foot in the door” in developing economies. Then, US telecom companies need a compelling sales pitch, which could be focused on innovation, a positive vision, openness, and transparency.

The Open RAN project, for example, is an initiative that allows network operators to mix and match different components from different vendors in an open, standardized manner. Open RAN Policy Coalition members consist of 51 European, Indian, and US operators, and network equipment and silicon manufacturers, including Cisco, AWS, Google, Intel, Juniper, Microsoft, Vodafone, Verizon, and many others.

Open RAN is aimed at broadening the telecoms vendor ecosystem to provide a more diverse pool of vendors. In turn, this is intended to create a more resilient supply chain, drive innovation, reduce costs, and lower barriers to entry for specialist companies. The concept is that by using the best possible component at every point in the network the whole adds up to more than the sum of its parts.

An open network with equipment and software from multiple vendors can also provide greater visibility into network interfaces and allow security analytics to be distributed throughout the network, thus enhancing security. In an open environment, security patches can also be more easily applied with less impact on the entire network.

US companies cannot compete with Beijing's investments in Chinese telecom and tech companies, and their subsidies for global south economies. So, instead of going head-to-head with Chinese companies, US institutions should look to partner with domestic and European-based telecom and tech companies as well as those in like-minded nations to promote a vision based on innovation, security, and openness.

Conclusion - building a diversified telecoms supply chain

Building an extended, diversified supply chain, such as that being created by initiatives such as Open RAN, could provide resilience, lower barriers to entry, reduce costs, and help to develop best-in-class, innovative components.

In terms of a compelling vision, US tech companies might also specialize in certain aspects of the digital infrastructure, for example, by offering secure, innovative, environmentally friendly, accredited solutions for smart cities, ports, or factories. Likewise, 5G-enabled network slicing provides organizations with specific capacity, scalability, and security capabilities.

US telecom companies should focus on building a robust, diversified supply chain with US, European, and other like-minded partners with an emphasis on innovation, transparency, standardization, and security – creating an ecosystem that provides true choice to operators – covering all high-risk points identified. It is also important to focus on early involvement in movements towards 6G. Building such a compelling vision could help to counteract China's current influence in the global south.

“US telecom companies should focus on building a robust, diversified supply chain with US, European, and other like-minded partners with an emphasis on innovation, transparency, standardization, and security”



Address

8045 Leesburg Pike,
Suite 220,
Vienna, Virginia
USA | 22182

Phone

Office: +1 703 783 5020
Mobile: +1 231 360 3408

Online

Email: info@pamirllc.com
Website: www.pamirllc.com

