TRANSFORMA INSIGHTS

# White Paper

Brought to you by: Transforma Insights
Sponsored by: floLIVE


# BEYOND THE CAMPUS: WHY MOBILE PRIVATE NETWORKS NEED A GLOBAL APPROACH

February 2022

# 1 EXECUTIVE SUMMARY

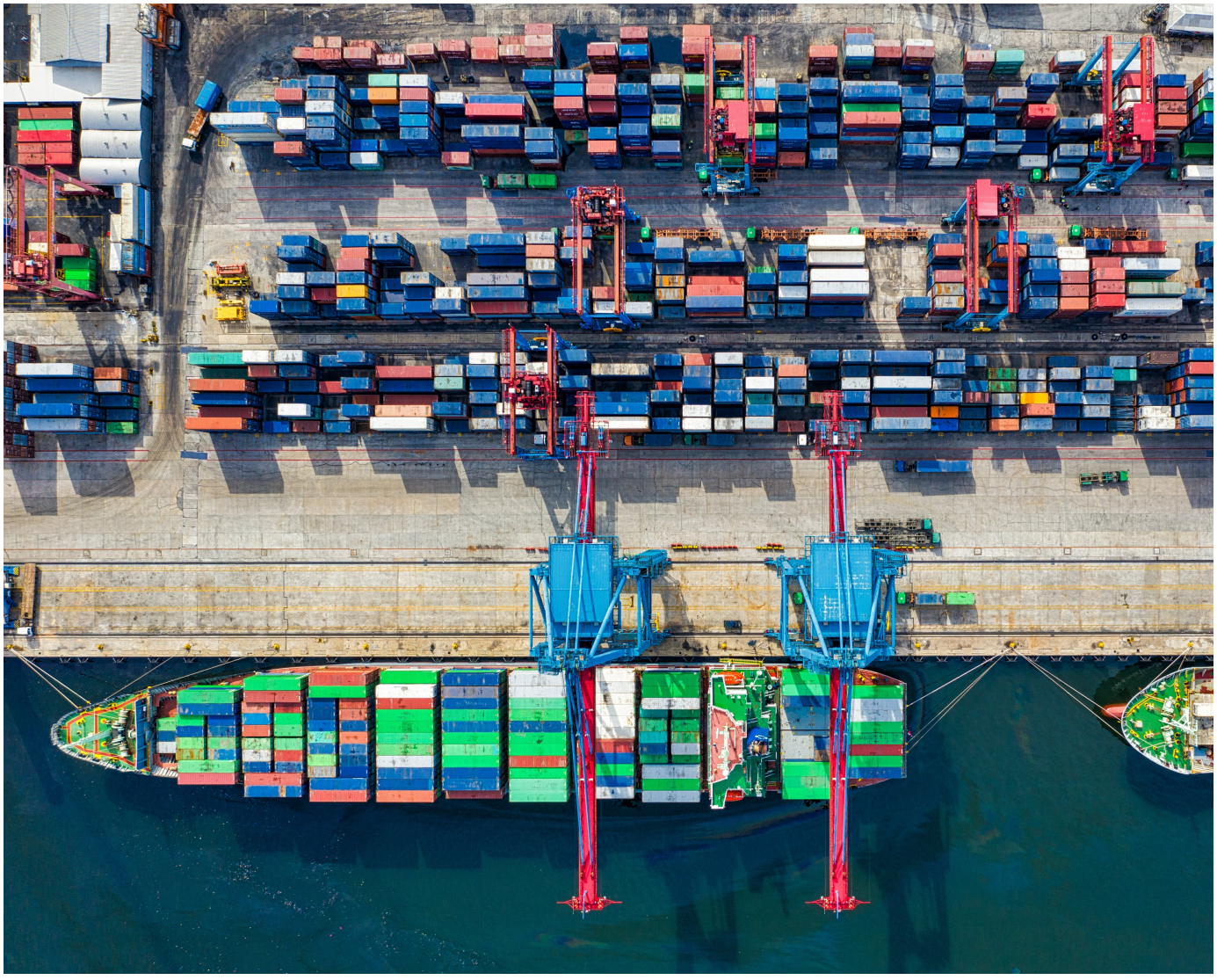
The concept of Mobile Private Networks (MPNs) has grabbed the headlines in the last two years. Enterprises are recognising their value for connecting increasingly feature-rich and critical IoT systems, and technology vendors see them as a critical bridgehead in the adoption of 5G. The availability of spectrum also helps to facilitate adoption. The benefits of dedicated campus networks are numerous in terms of security, reliability, latency and control.

There is a tendency to consider the MPN as a stand-alone requirement for a single site dedicated network. The reality is much more complicated than that. Often the deployment of such a campus network will be part of a wider requirement for connecting devices in a country or around the world. Furthermore, even some campus deployments will use public networks for some or all of their connectivity. Whatever the deployment, there is a strong chance that a campus network deployment will in fact be part of a wider national or global deployment. Verticals such as logistics, energy and manufacturing have demonstrable need for connecting devices both on and off campus.

Transforma Insights believes that enterprises would benefit greatly from a 'holistic' approach to supporting campus and wide area connections, effectively supporting them using a global private network, utilising 5G network slices (where appropriate) and a private Packet Core (or slice of one).

What is also missing from delivering the global element today is Transport Layer Orchestration (TLO) i.e. ensuring that devices are deployed and managed, and data delivered, in a compliant, secure and efficient manner regardless of where the device is deployed.

In this White Paper we examine in brief what MPNs are and why they are being deployed today. We then move on to looking at how the more holistic approach is required and in which particular sectors there is a need for the national and global complements to the campus network. Subsequent sections examine the TLO capabilities required from service providers wanting to deliver global private networks, the seven advantages of using a holistic approach, and which of the plethora of different vendors of MPNs are best placed to supply the holistic private national and global networks.



# 2 WHAT IS A MOBILE PRIVATE NETWORK?

In the last two years there has been increasing interest in Mobile Private Networks (MPNs) from enterprises looking for greater control and security for their deployments, particularly in IoT. It has also been a top priority for infrastructure vendors and communications service providers, looking for new opportunities particularly associated with the nascent 5G technology.

The traditional definition of a Mobile Private Network (MPN) is a dedicated network using cellular technologies (LTE or 5G) installed and operated for the benefit of a specific enterprise client (or similar) in a particular limited geographical location, typically a campus or large building. These dedicated private networks are nothing new. WiFi, Zigbee, WirelessHART, LoRa and other technologies are almost exclusively deployed as private networks. What is new in the last three years is the increasing focus on using 3GPP cellular technologies, i.e. 4G and now increasingly 5G.

As well as providing wireless voice and broadband services, the latest generation of campus MPNs are heavily geared towards IoT applications, including sensors, machinery, augmented reality devices, autonomous vehicles and surveillance equipment. As an illustration, Corning has deployed a 5G campus network at its Hickory, North Carolina plant to support factory automation and quality assurance, and with a further aim of developing capabilities around autonomous guided vehicles, augmented reality and machine vision.

A broad array of vendors offer campus MPNs, including mobile network operators such as Verizon and Vodafone, infrastructure vendors such as Ericsson and Nokia, and others such as Amazon Web Services, which launched its AWS Private 5G offering in late 2021.

The campus MPN comprises one or more access points, known as an eNodeB (in LTE networks) or gNB (in 5G networks), to which the device is connected using dedicated spectrum. The network access point is then connected to a private Packet Core, which authenticates devices, manages data traffic routing, and applies policy management. In some cases, the site will also have an edge server, running applications on the local site, allowing greater responsiveness for the on-site use case. The Packet Core can then be connected to the enterprise's servers, either dedicated or cloud-based, and/or the public internet.

In some cases, a private network may be delivered using public infrastructure, something which we examine in Section 4. In that case the device would be connected to a public eNodeB/gNB, using spectrum held by a mobile network operator. This could be delivered using a dedicated 'slice' of the network specifically allocated for the enterprise. That network is then typically connected to a public core, although could be managed using a separate private core that is interconnected with the public network.

# 3 WHY ARE CAMPUS NETWORKS SEEING DEPLOYMENT NOW?

Why are we seeing greater interest in the deployment of campus networks today? There are essential four reasons. Firstly, there is more demand for features that deliver greater functionality for IoT deployments, in a secure and easily managed way. There have also been two major developments on the supply side that have triggered greater demand: the arrival of 5G and the availability of spectrum. Finally, there is also a slightly more nebulous change which will also stimulate demand, that of network virtualisation and the disaggregation of the control layer from the network, enabling greater innovation in services. Each of these is explored in the sub-sections below.

## *3.1 Enterprise demand for IoT*

Using the Internet of Things is being seen increasingly as a key competitive differentiator across numerous sectors including agriculture, mining, manufacturing, distribution and retail. Over the last ten years there has been a steady increase in the demand for the IoT from enterprises. Use cases are becoming more well-established. Competitive pressure is forcing enterprises to look very closely at new ways to gain efficiencies, for instance through automation or digital twins. Transforma Insights has noted over the last two years an increasing interest in utilising IoT for more mission-critical use cases.

Recently we have seen increasing requirements for more on-shoring of production and more resilience in supply chains, at least in part due to the advent of COVID. Improving such capabilities will inevitably drive more reliance on automation in factories, distribution centres, ports and other enterprise sites, i.e. just the locations where private campus networks would be deployed.

As the value of IoT use cases becomes more established, attention inevitably turns to the networks being used to connect them. Increasingly bandwidth-intensive, low-latency, mission-critical applications demand a reassessment of which network technologies are utilised by the enterprise to support them.

## 3.2 Dedicated spectrum around the world has created a stimulus

One big driver for mobile private network adoption, beyond the availability of 5G, is the fact that many major markets have issued licenses for, or otherwise made available, spectrum specifically for private networks. Without such available spectrum, campus networks would need to rely on shared spectrum held by mobile network operators, which is unlikely to be available for the exclusive use of the enterprise.

The most prominent of the recent licence awards is the Citizens Broadband Radio Service (CBRS) spectrum in the United States. In 2020 the Federal Communications Commission opened up a frequency band from 3550MHz to 3700MHz, which had previously been held exclusively for use by the military and satellite ground stations. The new designation is that it is shared between three tiers of users: the former military and satellite incumbents which have priority across the full 150MHz band where they require it, Priority Access Licences (PALs) and Generally Authorized Access (GAA). Mobile, cable and satellite providers won the lion's share of licences. Enterprises focused on securing licences in very specific areas. John Deere, for instance, won licences covering its manufacturing and operations centres in Illinois and Iowa, while Chevron's wins were highly concentrated in the oil producing areas of West Texas, New Mexico, and the Gulf of Mexico.

In Europe, the prevailing trend is similar to that in the US, with licences in the range of 3-4GHz becoming available. In Germany in September 2020 74 "Lokale Netze" private 5G network licences were awarded in the 3.7-3.8GHz band. Those licence winners that were made public include manufacturers (e.g. Airbus, Mercedes Benz, ThyssenKrupp), systems integrators (e.g. Accenture and T-Systems), research institutes (e.g. Fraunhofer Institut) and telecommunications equipment vendors (e.g. Huawei). The regulator, BNetzA, also recently engaged in a further consultation process on the use of the 24.25-27.5GHz band and anticipates many more licensees for private networks. The UK regulator has made local spectrum licences available on a first-come-first-served basis (with cost-based fees applied) for four bands: 24.25-26.5GHz (indoor only), 3.8-4.2GHz, 2390-2400MHz (indoor only), and 2x3.3MHz duplex at 1800MHz. There are two forms of licence: low power (maximum 50 metre radius) and medium power (for rural areas). Licence holders will need to start transmitting within 6 months and be able to change frequency if required by Ofcom. Other European countries including Austria, Belgium, Finland, France, the Netherlands and Sweden have either made spectrum available already or are planning to do so.

Elsewhere in the world, China has somewhat bucked the trend in advanced markets by not yet making available spectrum for MPN, although the three mobile network operators have launched services. Japan's ministry of communications opened the application process in December 2019 and started awarding licences in 2020. Other countries that have awarded spectrum or are in the process of doing so include Australia, Brazil, Chile, Malaysia, and New Zealand.

## 3.3 The arrival of 5G

The benefit of operating a wireless network (e.g. WiFi) within a campus is self-evident, allowing for the networking of all of the various devices within the site. However, the last couple of years has seen a significant increase in interest in using cellular technologies to do this. Today the majority use 4G LTE, but the substantial take-off in the market will happen with 5G. While the benefits of using Mobile Private Networks are not dependent on using 5G, it's also true that 5G delivers a number of critical capabilities that can be particularly useful for enterprises. As such, 5G is a driver for MPN, but not a requirement.

There have been a lot of superlatives thrown around about 5G, up to and including it being the most important invention since electricity. Ignoring the hyperbole, the difference from previous mobile technology generations is three-fold:

- Increased bandwidth - Theoretically 5G offers speeds of up to 10Gbit/s but the experienced maximum speed by a single user is typically 100-200Mbit/s, about 5x higher than LTE. This opens up higher bandwidth applications such as online gaming, and augmented and virtual reality (AR/VR).
- Support for massive IoT deployments - 5G networks can manage up to one million devices per cell, clearing the way for much larger deployments of IoT.
- Lower latency across all applications - Historically, mobile networks never had latency much better than 50ms. 5G promises latency as low as 1ms, although in reality it will be more like 10ms for most communications, which is fast enough for any delay to be imperceptible.

Compared to legacy systems, 5G is leaps and bounds ahead, with faster speeds, lower latency, better reliability and the ability to support more devices. The range of applications that can be supported has expanded significantly.

There are specific benefits from using cellular (and particularly 5G) technologies compared with other private network technologies such as LoRa, Zigbee or

even WiFi 6. Compared with most technologies, 5G provides far superior bandwidth, security and reliability. Compared to WiFi 6 the distinction is less pronounced but 5G has some advantages. It is quite hard to compare the two technologies because much depends on which generation is being implemented, the amount of spectrum and a few other factors. Nevertheless, it is generally clear that cellular has the edge over WiFi in a few areas:

- Lower latency - A number of IoT applications, particularly related to industrial automation and autonomous vehicles, demand low latency. While WiFi 6 is an improvement on WiFi 5, its 20ms delay is significantly higher than 5G. When it comes to running low latency wireless applications, 5G is really the only option.
- Greater reliability - One of the other great selling points of 5G is its reliability. The over-riding reason for it being more reliable than WiFi 6 is more to do with the fact that it typically uses dedicated spectrum, whereas WiFi 6 uses licence exempt spectrum where there is a risk of other devices contending for bandwidth. This does not guarantee that 5G will always be more reliable, but it does represent a significant variation between the two.
- Consistent deployment environment - Rather than having devices connecting and handing over between WiFi 6 and 5G when roaming outside of the factory, using solely 5G means a much simpler device and connectivity management environment and more reliable handover between the two.

The big drawback for cellular compared to WiFi 6 today is in device costs. WiFi is significantly cheaper. WiFi also has the advantage of backward compatibility with all previous generations, which is not the case with cellular technologies, although 4G to 5G compatibility is good. There is also some debate about security, with WiFi6 generally being at a disadvantage, depending on how it is provisioned.

To a certain extent the creation of a contest between WiFi and 5G is spurious. The most likely scenario is that the two technologies will co-exist. Very few organisations that elect to implement a private 5G network will not also provide WiFi for that same site. The functionality means that they will be focused on different uses cases, but WiFi will almost always be deployed alongside any 5G deployments.

## *3.4 Greater service innovation on the newly disaggregated control layer*

In the report 'The move to 'Network New Normal': how 5G, edge computing and network disaggregation are creating radical disruption' (June 2020) we at Transforma Insights examined the impact of new technology developments on how telecommunications networks are run. One of the key areas was disaggregation and virtualisation. Historically the software and hardware elements of telecoms networks were very deeply integrated. However, recently, there have been initiatives to separate those elements, such as Software Defined Networking (SDN) and Network Function Virtualisation (NFV). Furthermore, one of the key principles of 5G is that the user plane and the control plane are separated.

The separation of a software control layer from a commoditised and generic set of telecoms network hardware is the epitome of Transforma Insights' concept of 'Separation-Innovation-Explosion'. The key idea is that separation of hardware from software/control layers is a fundamental requirement for, and stimulus of, a technology area seeing true deep-seated innovation. In most technologies that combine hardware and software, the heritage is for deep integration of the two, e.g. in automotive or industrial systems. However, when these two are separated, as we saw with personal computing decades ago, it stimulates radical innovation. Not having to build the hardware and the software together enables greater innovation in both.

When considered in the context of the operation of telecoms networks, the increasing separation of the control layer will create an explosion in the number and variety of networking services, and therefore a more diverse service providers better able to meet the needs of customers. For instance, new service providers are able to operate their own virtual packet core, delivering flexible new offerings, without needing to operate an access network. This applies equally in the MPN space as it does in wide area networks. It is perhaps unsurprising that the advent of this separation and virtualisation has been the trigger for the interest and involvement of the cloud hyperscalers, particularly AWS and Microsoft in this market.

In the long term, the specific features and functionality of 5G are likely to be less important to the development of new services than the liberation of software-oriented organisations to freely develop innovative new telecom services.

# 4 BEYOND THE CAMPUS TO THE 'HOLISTIC' PRIVATE NETWORK

The discussion of MPNs naturally focuses predominantly on campus networks, and these are certainly a critical new growth area. However, considering requirements for a single stand-alone campus network in isolation from an organisation's wider connectivity requirements is a mistake.

In most cases, an enterprise's requirement for connecting people, things and processes do not begin and end at the factory (or warehouse, port or hospital) gates. For this reason, we advocate considering the enterprise MPN requirements alongside its wider needs for secure, reliable and feature-rich end-to-end connectivity, covering campus networks, national private networks and global managed networks.

The flexibility that enterprises demand in the campus will equally apply to devices deployed nationally and globally.

## *4.1 National private networks*

It is important to note that the idea of dedicated network infrastructure located on the enterprise's site is just part of a continuum of connectivity options for delivering highly secure and reliable connectivity to meet the specific needs of the enterprise. For instance, Deutsche Telekom's approach to the MPN market, under the banner '5G Campus', is far from solely reliant on private infrastructure, consisting, as it does, of three options:

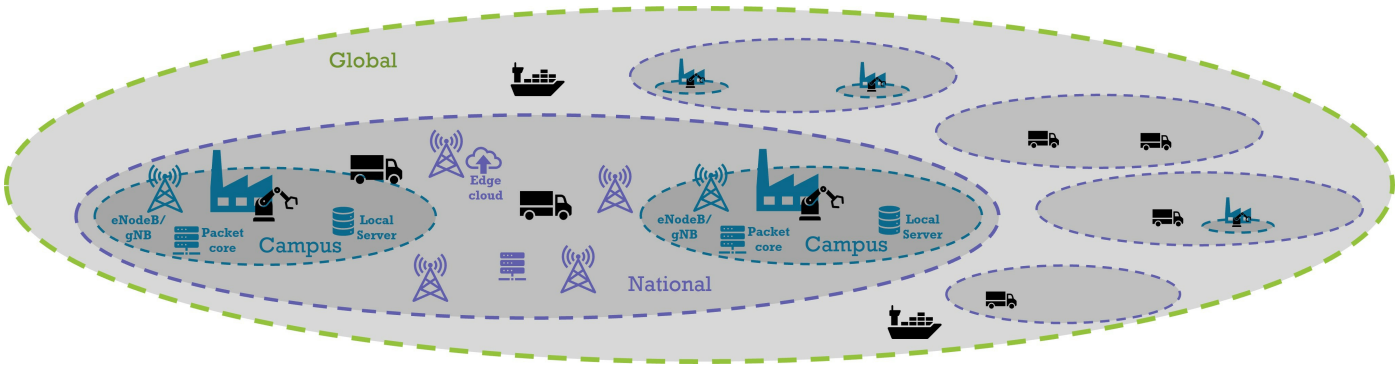
- Campus Network S - supported by installation of additional public RAN infrastructure.
- Campus Network M - supported via public networks but with a private network slice, VPN connection and traffic prioritisation.
- Campus Network L - dedicated access network and direct connection to local data centre.

It is noticeable that two of the three options do not involve a private infrastructure deployment but instead supports the campus connections through additional public RAN infrastructure. Using a dedicated campus network is just one option amongst many for addressing enterprise needs.

One of the most heralded attributes of 5G is the increased capability to offer 'network slices', i.e. a series of logically separate networks operating for particular clients on the same common public network infrastructure. The great benefits of the network slices are that they can be adapted to deliver connectivity capabilities to meet particular service levels. In some cases, it will be used as an alternative to a dedicated campus network; it is almost certain to be more cost-effective to deliver. In others it may be used as an on-ramp to a dedicated campus, i.e. testing the waters of how a network slice might deliver superior service before making the leap to deploying dedicated infrastructure. This is clearly at least part of the reason for Deutsche Telekom's product structure, above. In countries with no dedicated spectrum allocated for MPN it's likely that the public network is the only option.

Most enterprises will have a requirement for connectivity beyond the campus. Many of the use cases

**Campus, national and global networks**
[Source: Transforma Insights, 2022]



that will benefit from an on-site private network, either delivered using dedicated infrastructure or not, will also have a requirement for connectivity beyond the site, for instance for the transportation of stock or product to and from factories. And, furthermore, the service levels that will be desired to be applied on the campus, e.g. for latency, bandwidth or reliability, could well also extend to the whole country, or at least part of it. Stimulated by experience of superior capabilities within a campus, enterprises are also likely to demand the equivalent on the wide area network.

It is incorrect to think of these capabilities as campus extensions. In many cases, as noted above, the first iterations will use the wide area network rather than a dedicated one. There are also many distributed IoT deployments for which using a dedicated campus network is not a viable option, but which would nevertheless benefit from superior grades of service in terms of guaranteed bandwidth and latency and improved security. Examples include autonomous vehicles, Intelligent Transport Systems and smart grid.

It would also be incorrect to think of this as being tied solely to the provision of network slices. The ability to deliver 'private' secure connectivity over the national public networks is also a sliding scale. Many connectivity providers can offer IP VPNs, private APNs and other similar features. Beyond this can be layered on additional functionality. Ultimately the richest set of capabilities for off-campus devices will be delivered using network slices and a private core network.

National private networks can be strongly complementary to campus networks, or can be an alternative to them for connecting specific sites, or can be a valuable option for enterprises where a dedicated network would not be a feasible option. However they are delivered they reflect an increasing demand for more highly managed connectivity.

## *4.2 Global managed networks*

A further extension of the demand for managed connectivity applies for global deployments. Many IoT deployments have global requirements, for instance involving multi-country supply chains, or deployment of connected products and services around the world. This adds further layers of complexity to how such deployments need to be managed, compared to the national networks. There are issues of compliance, policy management, data routing and more.

Furthermore, the idea of using the wide area network as a complement to campus networks applies equally with multi-country deployments. Enterprises may well have campus networks rolled out in factories or distribution centres in various parts of the world and require multi-country wide area connectivity to fill in the gaps. Having some degree of consistency between those campus and national deployments will make the process run much more seamlessly for application roll-out, device management, connectivity management, and troubleshooting.

In order to guarantee control over these global deployments for things like policy management, compliance and local breakout requires a dedicated private core network capability. Connectivity providers today almost universally offer a set of connectivity management and device management features allowing the enterprise customer some degree of management over its IoT devices, e.g. for activation, billing, firmware upgrades and so forth. However, these are not sufficient to meet the demands for security, compliance and flexibility of critical deployments. What is required is a richer orchestration layer, supported by a dedicated core network, or slice of one. The characteristics of this orchestration layer are discussed in Section 6.

# 5 WHERE WILL CAMPUS NETWORKS BE DEPLOYED?

There are a number of scenarios where we can envisage enterprises wishing to make use of the associated capabilities for IoT. Manufacturing, transportation, logistics, agriculture and energy are amongst the most obvious. We have already seen early adoption in a number of places, as illustrated by these examples:

- The Factory 56 initiative which covers Mercedes Benz's 20,000 square meter Sindelfingen plant. The focus is on assembly line and process automation.
- China's Shandong Energy Group deployed China's first private 5G network in October 2020 for its subsidiary Baodian Coal Mines using equipment from Beidou Tiandi, another subsidiary specialising in smart mining. The network will be used for controlling mining equipment.
- A major Mediterranean port is using 4G today with future expansion to 5G. This is a compelling use case, involving tracking and managing 14,000 Twenty Foot Equivalent Units (TEUs) per day using over 100 cranes and over 200 trucks and trains.
- Vienna Airport has deployed a campus network, which delivers broadband connectivity for passengers as well as supporting devices such as luggage scanners, handling equipment and employee productivity devices.
- West China Second University Hospital in Sichuan has deployed a 5G network for hospital management, AR, CCTV and personal assistance robots.

The above examples represent a good cross-section of the deployments of campus networks to-date. Mostly they are deployed by market-leading organisations with a strong technology heritage. The Figure on the next page lists the sites where we expect to see the most campus networks. The deployment of campus networks also needs to be considered in the context of a wider national or global deployment, as discussed in Section 4. In the Figure we also include the associated requirements for each vertical to have national and global private networks as an adjunct to the campus deployments.

**Requirements for campus, national and global private networks**
[Source: Transforma Insights, 2022]

| Sector | Campus | National | Global |
|---|---|---|---|
| Industrial plants/ factories | Tens of thousands of sites globally ranging from highly sophisticated (e.g. auto manufacturing) to less complex such as food production. | Clients may have multiple sites and often with requirements for integration with supply chains. | Clients may have multiple sites and often with requirements for integration with supply chains. |
| Ports | Several hundred significant ports worldwide with substantial demand for efficiency savings from campus networks. | Requirement for integration of port operations with immediate incoming and outgoing transportation. | Some requirement for integration of port operations with global supply chains. |
| Oil refineries | Highly complex and critical processes. Between 500 and 1,000 sites worldwide. | Integration with national distribution. | Multiple sites worldwide. |
| Mines | Typically remote and with poor wide area network coverage. Often complex systems and demand for process automation. Tens of thousands of sites worldwide. | Some requirement for wide area connectivity for transportation of mined goods. | Mining companies will typically have multiple global sites with requirement for common approach. |
| Smart grids | Tens of thousands of power plants and distribution sites running complex critical systems often requiring low latency communications. | Requirement by utilities for monitoring of the wider smart grid infrastructure. Particularly taking advantage of low latency of 5G. | Some limited application in cross-border power distribution. |
| Airports | Very complex systems. Several thousand, but with only around 1,000 significant commercial airports. | Typically airports are very large sites with some connectivity provided by wide area networks. | Minimal requirement |
| Sports stadiums | Less than 1,000 significantly sized stadia around the world. Demand based on providing capacity rather than particularly sophisticated services. | Minimal requirement | Minimal requirement |
| Conference centres | As with sports stadiums, this is typically about providing additional secure capacity. Also around 1,000 likely sites worldwide. | Minimal requirement | Minimal requirement |
| Hospitals | Tens of thousands of sites. Complex systems with moderate levels of automation. | Integration with blue light services and between multiple sites. | Minimal requirement |
| Logistics distribution centres | Thousands of centres with very high levels of automation. | Significant requirement for integration with national supply chain and across multiple sites. | Significant requirement for integration with international supply chain and across multiple sites. |
| Malls and retail parks | Thousands of significant sites but typically provision for regular voice and data services. | Minimal requirement | Minimal requirement |
| Agriculture | Millions of possible deployments with highly distributed applications and generally poor coverage from mobile networks. | Typically very large sites with some connectivity provided by wide area networks. Also requirement for integration with supply chains. | Minimal requirement |
| Smart cities | A number of cities are deploying their own private 5G networks to support public services. | Smart city deployments will generally rely on public network infrastructure. | Minimal requirement |
| Remote workers | Minimal requirement for dedicated infrastructure for distributed workers. | Extending the enterprise perimeter for managed access to connectivity. Particularly relevant for secure home working. | Many implementations will involve global employees. |

# 6 ORCHESTRATING NATIONAL AND GLOBAL PRIVATE NETWORKS

As outlined in previous sections, the delivery of MPNs will often be tied up with provision of national and/or global connectivity to complement the campus network. Many IoT deployments will, of course, demand only wide area connectivity. For either of these scenarios, particularly those involving multi-country deployments, there is an increasing requirement for what we term 'transport layer orchestration' (TLO), i.e. ensuring that devices are deployed and managed, and data delivered, in a compliant, secure and efficient manner.

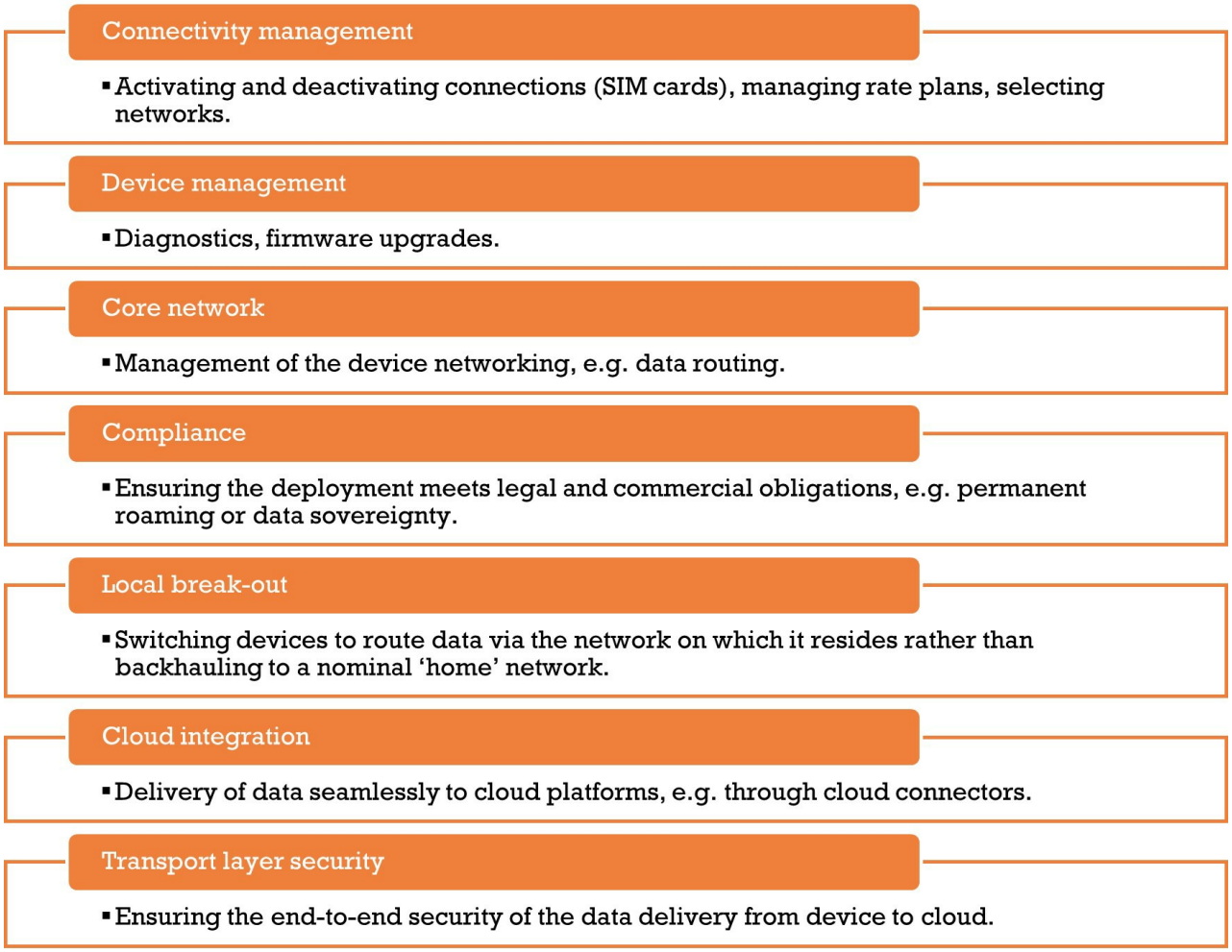
There is a wide range of features and functionality implicit in the provision of wide area IoT connectivity, either national or global. Most connectivity providers offer SIM cards that can connect anywhere in the world. Similarly, the majority already provide some element of connectivity and device management, e.g. activation, tariff selection or firmware updates. Most do not provide the appropriate level of orchestration at the transport layer, i.e. the end-to-end delivery of data, to ensure that data is managed in the appropriate way, or the localisation elements that are increasingly required.

A full set of IoT orchestration capabilities are set out in the Figure below.

The effective delivery of multi-country IoT solutions depends on being able to deliver these elements.

It should be noted with regard to all of these elements that there are implicit advantages to supporting a full deployment across multiple RANs and/or MPNs in a consistent way. For instance using a single core network (or multiple consistently deployed and integrated core networks) to deliver superior and consistent control and management.

**Transport Layer Orchestration functions**
[Source: Transforma Insights, 2022]



# 7 THE SEVEN ADVANTAGES OF A HOLISTIC APPROACH TO PRIVATE NETWORKS

There are numerous advantages to using mobile private networks both in the form of dedicated campus networks as well as national and global capabilities. Transforma Insights identifies 7 key advantages to adopting a holistic approach to managing campus and national/global connections in a holistic manner:

1. Control - The enterprise will always have the greatest degree of control over the network that it operates itself, in order to ensure the security, performance, policy management and other requirements. The campus network is the optimum example, but applying as much of the same logic to national and global network deployments as possible is sensible.

2. Security - A dedicated network gives optimum security. This applies to campus networks, network slices, and dedicated Packet Core. All provide superior security compared to a public network.

3. Performance - A Campus network, optimised for the requirements of the enterprise, will almost certainly deliver superior performance (e.g. latency and speed) than a public network. This means a richer array of applications can be supported.

4. Consistency of deployment - Having a holistic approach to campus and national/global deployments pays dividends. As well as having a single point of contact for all connectivity requirements, the enterprise also has seamless handover between on-site and off-site connectivity. Consistent deployments will also save time and effort in deployment, integration and troubleshooting.

5. Scalability - A consistently deployed technology makes it much easier to scale. An enterprise could start with a single site using public RAN and migrate relatively painlessly to multiple sites, dedicated campus networks and national/global connectivity for non-campus devices. Ideally this would be centrally managed across all deployments.

6. Cost savings - The ability to choose between private campus networks and private national network allows the enterprise some flexibility to find the cheapest connectivity option. Sometimes a private RAN will be cheaper. Sometimes public RAN will be cheaper.

7. Compliance - This topic is relevant particularly for global deployments where there will often be rules and regulations about IoT deployments, for instance prohibitions on permanent roaming for cellular connections, or data sovereignty rules related to how and where data is delivered. Keeping on top of compliance requirements can be a headache. Enterprises need a service provider that delivers compliance-as-a-service as part of its solution.

# 8 WHO IS BEST PLACED TO SUPPLY THE HOLISTIC PRIVATE NETWORK?

The essence of the Mobile Private Network is that it is owned directly by the enterprise which is using it. However, there are more participants in the provision of such capability that that would indicate. Very few enterprises will want to build and operate all aspects of their own network, something which is nigh-on impossible where it involves wide area connectivity.

For a start, just from the stand-point of a campus network, the enterprise will need network infrastructure, which means that either telecommunications infrastructure vendors such as Ericsson and Nokia, new entrant Open RAN vendors, or enterprise infrastructure vendors (e.g. Cisco and Juniper) will be required.

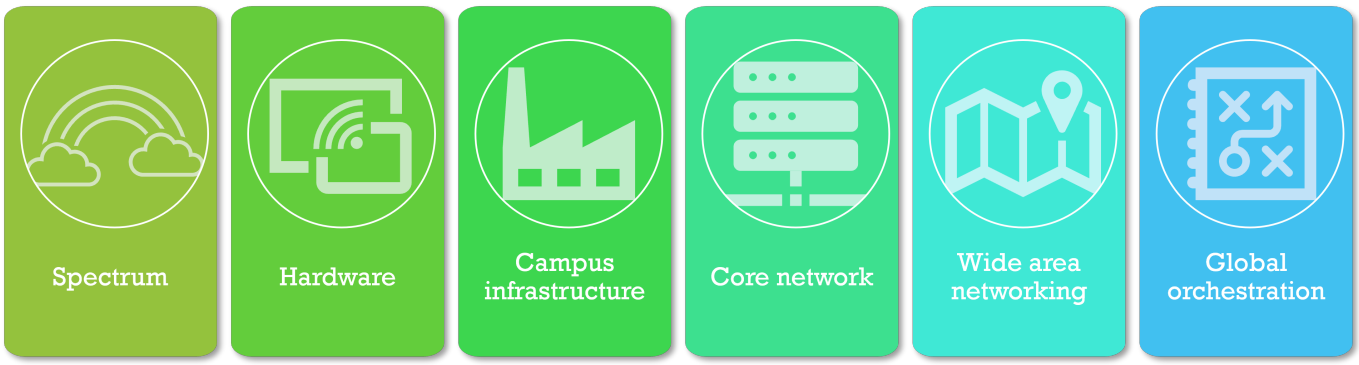
Furthermore, as highlighted in this report there is more to private networks than simply campus deployments. In many cases there will be a necessity to rely at least in part on wide area networks to support connectivity beyond the reach of the campus network coverage, which means mobile network operators or mobile virtual network operators (MVNOs) will also be required. There will also be a requirement for a core network, which may be provided by the traditional vendors, or possibly a new entrant, or delivered on a managed basis by a service provider.

Finally, we also need to consider that the MPN deployment will often take place in the context of delivering a wider range of services from systems integrator or specialist service provider focused on the particular vertical.

In this context of providing a more holistic private network capability spanning national and global deployments across both campus and wide area networks, who are the vendors that will likely be best placed to address the enterprise needs? Transforma Insights identifies the following, including their strengths and weaknesses:

- **The enterprise.** While the concept of the MPN is of being self-deployed, very few if any enterprises will actually deploy their own networks. Inevitably they will require infrastructure from some form of vendor, which the vendor may install for them. Or possibly they will buy infrastructure plus overlay services as a package. Some may hold spectrum, as with the CBRS auctions in the US, but that is only a small fraction of the required capabilities for deploying a network. For the national and global coverage which will, for many, be an integral part of their needs, there is no alternative but to find a partner to deliver a managed service.
- **Telecoms infrastructure vendors.** Clearly the manufacturers of cellular network equipment see MPNs as being an opportunity to sell more equipment. Most appealingly it is also an opportunity to sell to enterprises, rather than just to mobile network operators. Inevitably, as the organisations with the strongest heritage in supplying infrastructure, they will be at the forefront of selling equipment for campus-based MPNs. Ericsson, Huawei and Nokia have all been positioning themselves to take advantage of this opportunity. However, they generally lack much heritage in selling products and services to enterprises and they will also be somewhat unwilling to directly compete with their biggest customers (i.e. MNOs) for enterprise connectivity services. As a result, the vendors have focused a lot of attention on partnering with MNOs. For many of the same reasons they are also

**Elements required for Mobile Private Networks**
[Source: Transforma Insights, 2022]



generally not well placed to provide the wide area connectivity element. While they generally have strong capabilities, e.g. in the form of Ericsson's IoT Accelerator, or Nokia's WING platforms, these as tools that are supplied to MNOs and will constitute part of an MNO offering rather than a direct-to-enterprise capability.

- **Alternative network equipment vendors.** Beyond the traditional infrastructure vendors, there is also a group of smaller vendors which generally originated from selling 'small cell' hardware and many of whom have evolved towards supporting Open RAN . These include the likes of Airspan, Altiostar, Commscope and JMA Wireless. They also have offerings that are highly suited to campus-based MPNs. Many are active members of the CBRS Alliance. As with the major vendors, many also need to sell through partners although have in many cases already established those partnerships. None has any significant capability outside of campus hardware, making them poor candidates to address the national or global requirements outlined in this report.

- **Enterprise infrastructure vendors.** The provision of in-building or campus connectivity is not a new thing. Vendors such as Cambium Networks, Cisco, HPE and Juniper have been selling wireless networking equipment to enterprises for decades. While the main focus has been on WiFi, inevitably in the face of the growing interest in MPNs they have also turned their attention to cellular technologies. Cisco, for instance has its Premium Mobile Broadband (PMB) offering for private LTE networks. The big advantage for these types of vendors is that an MPN offering slots into an existing portfolio of enterprise services for which the vendor already has a channel to market. They also have a strong heritage in selling direct to enterprise. The limitations on enterprise infrastructure vendors are that their offerings are unlikely to be at the cutting edge of cellular technologies (i.e. mostly being focused on LTE, if anything) and that they also generally lack much capability to integrate a wide area connectivity offering into the campus MPN offer.

- **Mobile network operators.** Mobile network operators also have significant skin in the MPN game. Few markets have issued dedicated spectrum for MPN and where they have, MNOs have often been the biggest licence winners. MNOs are also well positioned to support the wide area networking element of a holistic MPN deployment, or use network slices as an 'on-ramp' to a full campus private network deployment. However, MNOs' offerings tend to focus on their own footprint, with few seeking to address a broader global opportunity, although we expect this to increase in future.

- **Cloud Core IoT Mobile Virtual Network Operators.** A large proportion of IoT connections today are supported by IoT MVNOs. This group of providers is particularly adept at supporting multi-country deployments based on relationships with multiple MNOs and deployment of rich orchestration features. Some have also added campus networks to their portfolio. Where consistency of deployment across campus networks and multi-country wide area deployments is necessary, MVNOs have a strong potential role to play. The critical thing for MVNOs is to have core network capabilities and all of the other orchestration features noted in Section 6 above. The limitation of the MVNO tends to be in scale and not owning the radio access network, although as noted in Section 3.4 the greatest innovation is today coming from control of the Packet Core rather than the RAN, and for global deployments no MNO has a global footprint.

- **Other Communications Service Providers (CSPs).** MNOs and MVNOs might seem the most obvious CSPs to venture into MPNs, but cable and fixed line operators have also been active in the space, as illustrated by the winners of the CBRS licences. Most will be at a disadvantage for a few reasons. They will almost always have a more limited footprint, being typically single country operators, they will lack the wide area cellular connectivity either national or global, and they will often have a limited enterprise customer base.

- **Systems integrators.** The provision of MPNs will often be part of a wider offering incorporating factory automation or augmented reality or any number of applications, particularly for IoT-related MPNs. As such, a significant proportion of MPNs will be implemented as part of a systems integrator's wider solution for its enterprise client. The likes of Accenture and T-Systems were amongst the winners of Lokale Netze licences in Germany, illustrating that they plan on integrating MPN into a wider set of offerings. They are also well able to partner with MNOs or use the enterprise's own spectrum. IBM, for instance, has integrated Vodafone's MPN capability into its own edge computing solutions focused on industrial clients. The big downside for Systems Integrators is cost: the solutions they deliver tend to be bespoke.

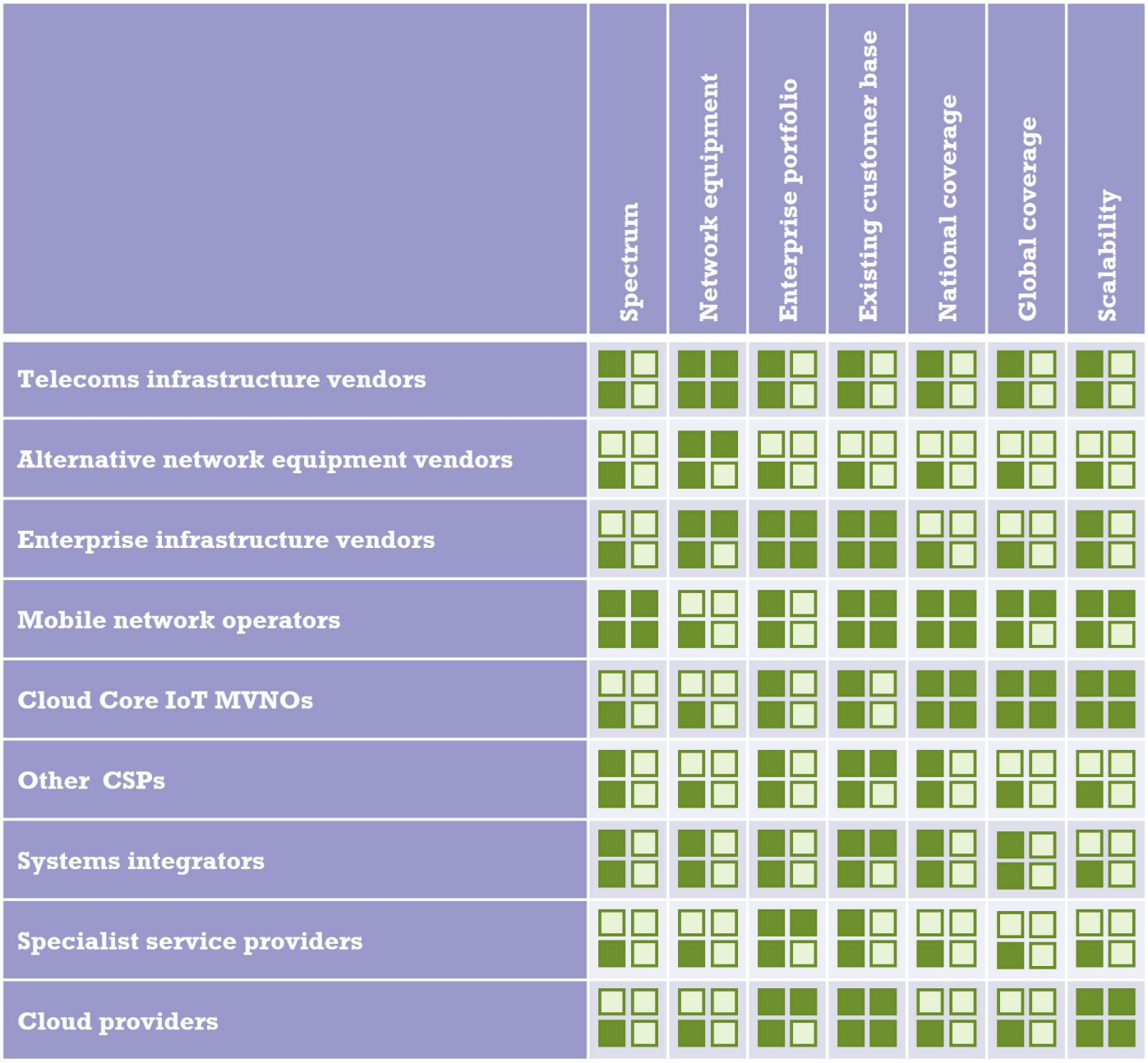
- **Specialist service providers.** There are already currently a set of companies, such as

Boingo Wireless or CityMesh which provide campus MPNs to enterprises. There are also specialists, focused on providing ICT solutions for particular verticals that may benefit from the addition of MPNs. This will be an interesting area to watch but will be almost exclusively limited to campus networks.

- **Cloud providers.** The cloud 'hyperscalers', most notably AWS and Microsoft, have been building MPN and wider core network capabilities. AWS launched its AWS Private 5G offering in late 2021 and also has its AWS IoT Core device gateway and AWS IoT Core for LoRaWAN products. In 2020 Microsoft acquired Affirmed Networks which provides virtual core network infrastructure, including virtual Evolved Packet Core (vEPC), mobile edge computing (MEC) and network slicing capabilities. It does not yet have a campus product.

In the chart below we present the Transforma Insights view on the relative capabilities of the various different providers of holistic MPNs, i.e. cutting across dedicated campus networks and the ability to support national and global wide area connectivity.

**Holistic MPN capabilities**
[Source: Transforma Insights, 2022]



flo. LIVE

# Is Private RAN Enough?

## Ushering in a New Era for Mobile Private Networks

**The world is changing, and it's time to start rethinking everything you think you know about mobile private networks.**

The classic campus network, where enterprises use a private core network and a private Radio Access Network, covers only a subset of today's enterprise use cases. Take Utilities companies for example. Imagine an electric company who wants to connect hundreds of thousands or even millions of household smart meters to its main operations center. It needs security, availability and control. However, this company is hardly going to deploy cellular antennas across the country to achieve private RAN, and will instead need to utilize a private core network alongside public RAN, without compromising on security, policy enforcement, and performance.

Other examples where distributed IoT impacts the type of infrastructure necessary include logistics use cases. Imagine a smart warehouse or a connected logistics center owned by a large retailer or brand. They might have a private network with a private core and private RAN in their warehouses or manufacturing plants, but will need to utilize public RAN to track pallets and shipments on the move. While the private network in their factories will enable low latency applications like machinery or connected assets, once drivers are on the road, they need to be able to benefit from public RAN.

Even outside of Logistics or Utilities use cases, many enterprises may opt out of deploying private RAN, even when they want to simply cover connectivity over multiple sites or locations, simply due to the costs, complexities and compliance mandates of accessing radio spectrum from the government, which differs from one region to another. For many enterprises, private RAN should be an option reserved for areas where there is no public cellular coverage, or where low latency is critical.

## You might ask, doesn't relying on public RAN for private networks cause challenges for the business?

The truth is, a lot of the value of MPNs for enterprise requirements comes from the core network. With a robust core network, enterprises can ensure:

### Performance

If low latency is a requirement for specific areas, private RAN will be unnecessary across the board. Instead, use private RAN where it's important, and rely on public RAN elsewhere.

### Policy enforcement

At the core network level, policy enforcement can be very powerful, deciding what the device can do in terms of data, SMS, voice, roaming, and more.

### Resource allocation

Automatically via the core network, users can determine the bandwidth that's available and how to allocate resources to the relevant devices to ensure top quality performance and availability.

As enterprise use cases increasingly need a mix of private and public RAN, at floLIVE we believe that a hybrid solution is the key. A robust private core that can provide all the benefits listed above and more, and then the flexibility to choose private RAN or public RAN, depending on the business requirement.

This can only be achieved with the support of companies who can deploy, configure and operate the private core, but who can also integrate with various public RANs through a vast IMSI library of local operator partnerships. A connectivity partner should also be able to provide additional services related to the handover between public and private RAN. For any business use case, whether it has low latency requirements and needs private RAN with private core, or whether private core and public RAN is necessary for distributed IoT use cases, or any combination - a company who owns the whole technology stack will be best placed to offer agility, flexibility, and quick time to value.

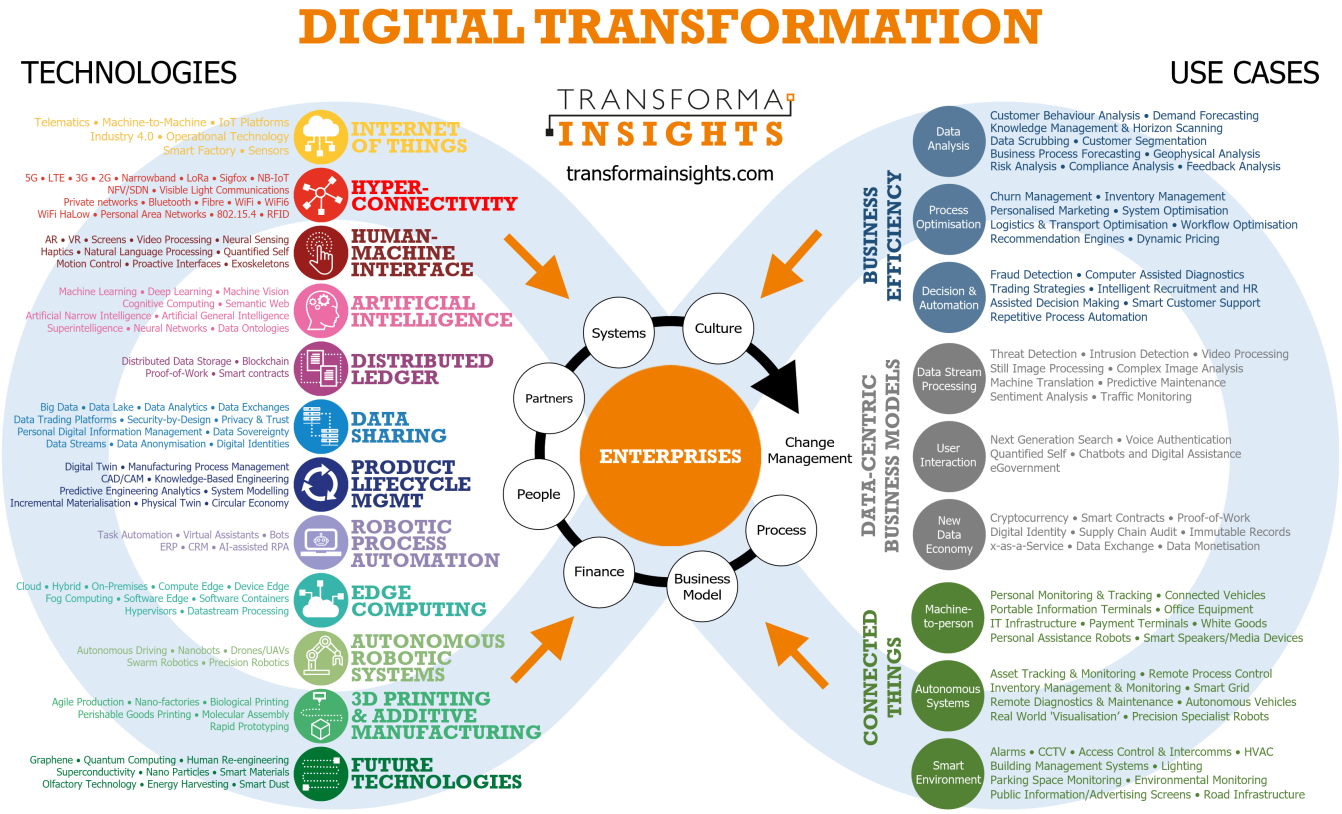
## Who could meet this need in the market?

At first glance, mobile operators are well positioned to provide the coverage needed for these use cases, and can also offer the failover between private and public networks. However, they can't offer the technology for policy enforcement, billing, or resource allocation. Mobile operators will also be challenged providing a solution beyond their native footprint. Thus, if the company's network requirements span across multiple regions, no single mobile operator will be able to natively support that need.

There are technology vendors and other providers who are entering this space to offer the technology to deploy and operate the core network functionality, but they aren't able to provide the public connectivity service for new distributed, regional or even global use cases. Even where they create MNO relationships to access connectivity - their technology lags behind or becomes expensive and complex to implement. Moreover, many of these technology providers offer to sell and deploy the network solution, but leave the ongoing management hassle to the enterprise IT to manage. In many cases these enterprise IT departments are less familiar with the operation of Cellular Technology.

**At floLIVE, we bring the two sides of the coin together, the technology and the service. Our partnerships with mobile operators globally allow us to offer public RAN anywhere in the world, and our core network capabilities are second to none. On top of that, we provide a fully managed service to run and operate the cellular network for our customers, whether it uses Private RAN, Public RAN or a combination of the two.**

**This means today's businesses can have all the control they need to ensure best quality of service, airtight security, and unparalleled performance, when they need private RAN and private core infrastructure in the way of a "traditional" mobile private network, but with equal capabilities for more modern business requirements for globally distributed availability and control.**




TRANSFORMA INSIGHTS

transformainsights.com

enquiries@transformainsights.com

TransformaTweet