

PERSPECTIVE

# WHY PRIVATE 5G IS TAKING OFF IN THE DEFENSE AND PUBLIC SAFETY SECTORS

Ibraheem Kasujee

February 2024



# 1. Why are defense and public safety agencies adopting private networks?

Interest in private networks from the defense and public safety sector is not new but it is increasing. In December 2023, the US government called for the Department of Defense (DoD) to deploy private wireless networks on all DoD military sites.<sup>1</sup> Other defense organizations such as France's Ministry of Armed Forces, NATO and the Norwegian Armed Forces have also trialed private networks at military bases, and others will follow to take advantage of the benefits of private 5G.<sup>2</sup>

Private 5G networks are a good match for both defense and public safety sectors. Private networks can cover vast military bases, indoor sites such as aircraft hangars, or be deployed as portable networks on the battlefield. First responders and other organizations can also rapidly set up temporary private networks when there is an emergency or natural disaster and gain visibility in hard-to-reach locations. The Philippines Red Cross trialed the use of drones that were connected over a private LTE network to improve situational awareness in response to an earthquake or tsunami.

Defense and public safety agencies can leverage a technology that is getting mass market usage: Analysys Mason estimates that more than 60 000 private LTE/5G networks will be deployed by 2028.<sup>3</sup> The reason: Widespread adoption of private networks will reduce costs, increase device availability and improve market understanding of the benefits of private networks. The result is a connectivity solution that can provide superior performance to that of existing mass market solutions and at a lower cost than bespoke military solutions.

## The USD1 billion private 5G opportunity in the defense and public safety sectors<sup>3</sup>

### 1.1 Nine key connectivity requirements for defense and public safety

Any defense solution needs to be highly secure and controlled by the military, ruling out public mobile networks for most applications. The networks will support advanced applications such as drones, robotics and AR/VR, requiring high throughput and ultra-low latency. Connectivity needs to be highly reliable in a variety of environments, including large military bases or in mobile environments on the battlefield.

Public safety organizations also need a significant degree of flexibility. They require either permanent networks in areas where first responders know they will need extra capacity, or temporary networks that can be quickly deployed at the scene of natural disasters or emergencies (such as a major fire).

Private networks can meet the critical requirements of defense and public safety organizations and offer advantages over other technologies (Figure 2).

---

1 <https://federalnewsnetwork.com/defense-main/2023/12/military-installations-could-soon-get-private-wireless-networks/>

2 <https://5gobservatory.eu/telia-norway-demonstrates-5g-network-slicing-for-norwegian-armed-forces/>

3 Estimated based on data from Analysys Mason's private LTE/5G networks forecast: <https://www.analysismason.com/research/content/regional-forecasts-/private-5g-networks-forecast-rma17/>

Figure 1: Nine connectivity requirements in the defense and public safety sectors

#	Key requirement	Details	The advantage of private networks
1	Performance	Stable, reliable connectivity required.	Operate in locally allocated spectrum or dedicated spectrum, so unaffected by RF interference.
2	Wide-area coverage	Connectivity required over large, outdoor areas.	Can cover large areas with minimum infrastructure, due to high power and receive sensitivity. This could provide a significant cost saving compared to other technologies.
3	High-speed mobility	Need to connect mobile applications such as robotics and automated vehicles.	Can meet the throughput and latency requirements of mobile applications in both indoor and outdoor environments.
4	Security	Defense and public safety organizations need the highest level of security possible.	Dedicated networks are shielded from cyber-attacks targeting public networks. Federal organizations have full control over SIM encryptions and the ability to store them in federally secure domains.
5	Resiliency	Reliability is essential: even a temporary loss of connectivity could increase the risk of fatalities or injuries.	Strong resilience and network availability via SLAs as private networks are unaffected by network issues on public networks.
6	Control	Need to connect several, complex applications and need to monitor and optimize their performance.	Control over network functions to enables traffic prioritization and policy-driven performance (for example, ultra-low latency on mission-critical applications).
7	Equipment availability	May require equipment on a large scale and in a short timeframe.	Cellular connected devices used in private networks, such as push-to-talk devices, are readily available 'off the shelf'.
8	Future-proof solution	Need reliable, future-proofed technologies to replace existing technologies such as TETRA that are reaching end-of-life.	Long shelf-life with no deterioration in performance and will co-exist alongside other technologies such as Wi-Fi.
9	Develop new applications	Desire to develop new applications that have advanced connectivity requirements.	Can support new, advanced applications such as robotics, autonomous vehicles and AR/VR with greater reliability and flexibility than existing technologies.

## 1.2 Critical use cases in defense

Defense organizations need flexible connectivity options that cover a range of scenarios: permanent connectivity in large military bases, aircraft hangars and warehouses, and temporary connectivity on battlefields. Private networks can provide solutions that cover all of these sites and address the following use cases.

- **Facility modernization.** Military organizations need permanent networks on military bases and logistics sites that will be used for many different applications. Private networks can augment Wi-Fi and support military applications such as the following.

- **Voice and video communications.** Military organizations may be using an assortment of land mobile radio (LMR) or proprietary radio technologies for communication. Private networks can provide a unified solution to connect mission-critical-push-to-talk (MCPTT) and push-to-video devices with greater capacity, security and reliability than ageing LMR technologies.
- **Equipment and vehicles.** Military equipment and vehicles can be connected to monitor their location and for predictive maintenance to identify issues before the equipment breaks down.
- **Surveillance.** Private 5G can connect security cameras, alarms and drones. 5G can meet the bandwidth and latency requirements for live video streaming or the upload of large quantities of video data captured from military vehicles. For instance, a private LTE and 5G network was deployed at Fort Cason, USA to enable the upload of vehicle data from the Army's Mountain Express Automated Shuttle.<sup>4</sup>
- **IoT sensors.** Weather and air-quality sensors can be used to monitor conditions on bases and tracking devices can provide geospatial information.
- **Logistics optimization.** Non-tactical sites such as warehouses and aircraft hangars are also candidates for private networks. Private 5G is more effective in covering large, indoor areas than other technologies. It can support applications such as robotics, inventory management and equipment and vehicle tracking. A private 5G network was deployed at a warehouse operated by the Marine Corps Logistics Base Albany. The private network connected autonomous forklifts, robots and guided vehicles, with sub 15 millisecond latency, and used scanners and trackers to create an inventory and asset management system.<sup>5</sup>
- **Tactical, rapid deployable networks.** Private networks can keep battlefield units connected. The connectivity requirements differ from a military base as connectivity is required on an ad-hoc basis and may need to be deployed quickly at short notice. Portable private networks solutions can be deployed on battlefields with network equipment carried in a box or backpack that can be easily transported. Battlefield applications that can be supported by private networks include the following.
  - **Communication.** MCPTT devices are a critical part of the tactical battle. Private 5G can support voice, video and data communications and integrate with existing LMR technologies. VoLTE or VoNR can provide reliable voice communication and devices can be configured to optimize quality-of-service (for example, prioritizing video-streaming devices). Private networks can also support dynamic, federated communications to link up and separate MCPTT groups of disparate military units. For example, The French Ministry of the Interior is using private LTE to establish communication for SWAT teams.<sup>6</sup>
  - **Device tracking.** Tracking devices can transmit data from personnel and vehicles in real-time to geospatial models, and equipment connected to monitor their position and performance.
- **Emerging applications.** Technological evolution is critical for the military. Private 5G networks can support emerging applications with advanced connectivity requirements, including the following.

---

<sup>4</sup> <https://www.us-ignite.org/news/us-ignite-begins-deployment-of-dedicated-cbrs-network-for-iot-research-at-fort-carson/>

<sup>5</sup> <https://info.kpmg.us/news-perspectives/industry-insights-research/kpmg-smart-warehouse-department-defense.html>

<sup>6</sup> <https://athonet.com/athonet-selected-to-supply-lte-tactical-networks-solutions-to-the-french-ministry-of-the-interior-moi-for-pcstorm-lot-1/>

- **Robotics and autonomous vehicles.** Robots and autonomous vehicles require high throughput and ultra-low latency, both of which can be supported by private 5G. The Portuguese Navy used a private 5G network to provide secure connectivity as part of Exercise REMPUS 2023, an event which tested robotics and unmanned maritime systems.<sup>7</sup>
- **Drones.** Drones require constant, secure connectivity, which private 5G can deliver. Drones can carry payloads such as cameras for surveillance and LIDAR for mapping purposes.
- **AR/VR.** AR and VR is used extensively by the military (for example, for training purposes). Private 5G can provide high throughput – both downlink and uplink – and a reliable connection to ensure quality-of-service.

### 1.3 Critical use cases in public safety

Private networks can provide crucial support for first responders or organizations addressing sites of natural disasters. These include private networks set up in areas of high demand, such as large cities, or temporary networks deployed at emergency or natural disaster sites. Private slices over public networks can also provide on-demand connectivity at short notice. Applications on these private networks include the following.

- **Telemedicine.** Private networks can link first responders to hospitals. Medical equipment can be deployed on temporary private networks to monitor the status and location of medical equipment and measure patients' vital signs. This data can also be synchronized with patient medical records to give clinicians instant insights into the patient's health and determine the best course of treatment. Ambulances can be equipped with video terminals connected to VR glasses to give clinicians a real-time view of patients' injuries, provide guidance to first responders and make an assessment before arriving at the hospital. Private 5G provides the high throughput and ultra-low latency needed to support these applications. This is especially useful in addressing sites of natural disasters where it may not be possible to take the patient to a hospital in time.
- **Drones.** Drones can be deployed to provide first responders with an initial 'bird's-eye view' of a scene such as a major fire. Drones can also help to survey areas unreachable by vehicles (for instance, following an earthquake).
- **Voice and video communications.** Private 5G's reliable and secure connectivity can offer extra capacity to support existing systems used by first responders such as TETRA or public cellular. First responders can be equipped with 5G connected push-to-talk devices and body-worn cameras to facilitate communication between first responders and monitor scenes.
- **Connected equipment and vehicles.** Private 5G networks can be deployed directly onto vehicles such as ambulances and fire engines. For instance, a national Fire Brigade is using a private 5G network mounted onto its fire engines to provide reliable connectivity as the vehicle moves between incident sites, including areas outside of public cellular networks.<sup>8</sup>

<sup>7</sup> <https://www.vodafone.com/news/technology/vodafone-provides-5g-world-largest-robotics-exercise>

<sup>8</sup> <https://athonet.com/use-cases/fire-brigade-deploys-private-5g-network-for-secure-communications/>

## 1.4 Private networks in action: a European defense agency

Athonet, a Hewlett Packard Enterprise acquisition, deployed a private LTE network for a European defense agency to cover an army shooting range in a remote area that is not covered by public cellular network. Its robust private LTE network is used for applications such as HD video cameras, VoLTE and MCPTT over ruggedized smartphones and real-time location tracking of people and vehicles on-site. In addition, the private network is connected to a centralized control room for surveillance and monitoring and voice and video communications with personnel in the field.

The benefits: the private network provides reliable connectivity in the absence of public cellular coverage with added flexibility to extend coverage via the portable manpack solution. Key outcomes include improved safety by enabling a 'man-down' alarm system, better visibility into all personnel and vehicles, improved communication between personnel in the field and central control room, and the ability to perform remote operations without being physically present on-site, reducing the need for travel.

## 2. About HPE

HPE's private mobile solutions help defense and public safety organizations to deploy mission-critical networks in even the most challenging environments. With market-leading technology based on Athonet, a Hewlett Packard Enterprise acquisition, HPE provides our customers with reliable and secure private mobile networks that can be deployed in minutes.

HPE has longstanding relationships with federal agencies globally, with robust supply chain capabilities to service the needs of federal entities, including federal contractors, systems integrators and distributors. We have deep experience enabling mission-critical enterprise IT networks and data centers from edge to cloud, including more than 500 000 customers who rely on HPE Aruba Networking infrastructure every day. We are also one of the world's leading telecoms suppliers, with a portfolio serving 300 service provider customers across 160 countries, connecting more than 1 billion subscriber devices.

To learn more about HPE's private 5G solutions, visit <https://www.hpe.com//networking/private-5g>

### 3. About the author



**Ibraheem Kasujee** (Senior Analyst) is a member of the *Operator Business Services and IoT* research team in London, and leads the *IoT Services* and *Private Networks* research programmes. He has written on topics including the private 5G opportunity and IoT eSIMs and iSIMs, and has conducted research on IoT verticals such as smart metering and smart buildings. Ibraheem holds a BSc in economics from the University of Warwick, and wrote his dissertation on the impact of technology on sleep.

---

**Analysys Mason Limited.** Registered in England and Wales with company number 05177472. Registered office: North West Wing Bush House, Aldwych, London, England, WC2B 4PJ.

This perspective was commissioned by HPE. Usage is subject to the disclaimer and copyright notice below. Analysys Mason does not endorse any of the vendor's products or services.

We have used reasonable care and skill to prepare this publication and are not responsible for any errors or omissions, or for the results obtained from the use of this publication. The opinions expressed are those of the authors only. All information is provided "as is", with no guarantee of completeness or accuracy, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will we be liable to you or any third party for any decision made or action taken in reliance on the information, including but not limited to investment decisions, or for any loss (including consequential, special or similar losses), even if advised of the possibility of such losses.

We reserve the rights to all intellectual property in this publication. This publication, or any part of it, may not be reproduced, redistributed or republished without our prior written consent, nor may any reference be made to Analysys Mason in a regulatory statement or prospectus on the basis of this publication without our prior written consent.

© Analysys Mason Limited and/or its group companies 2024.