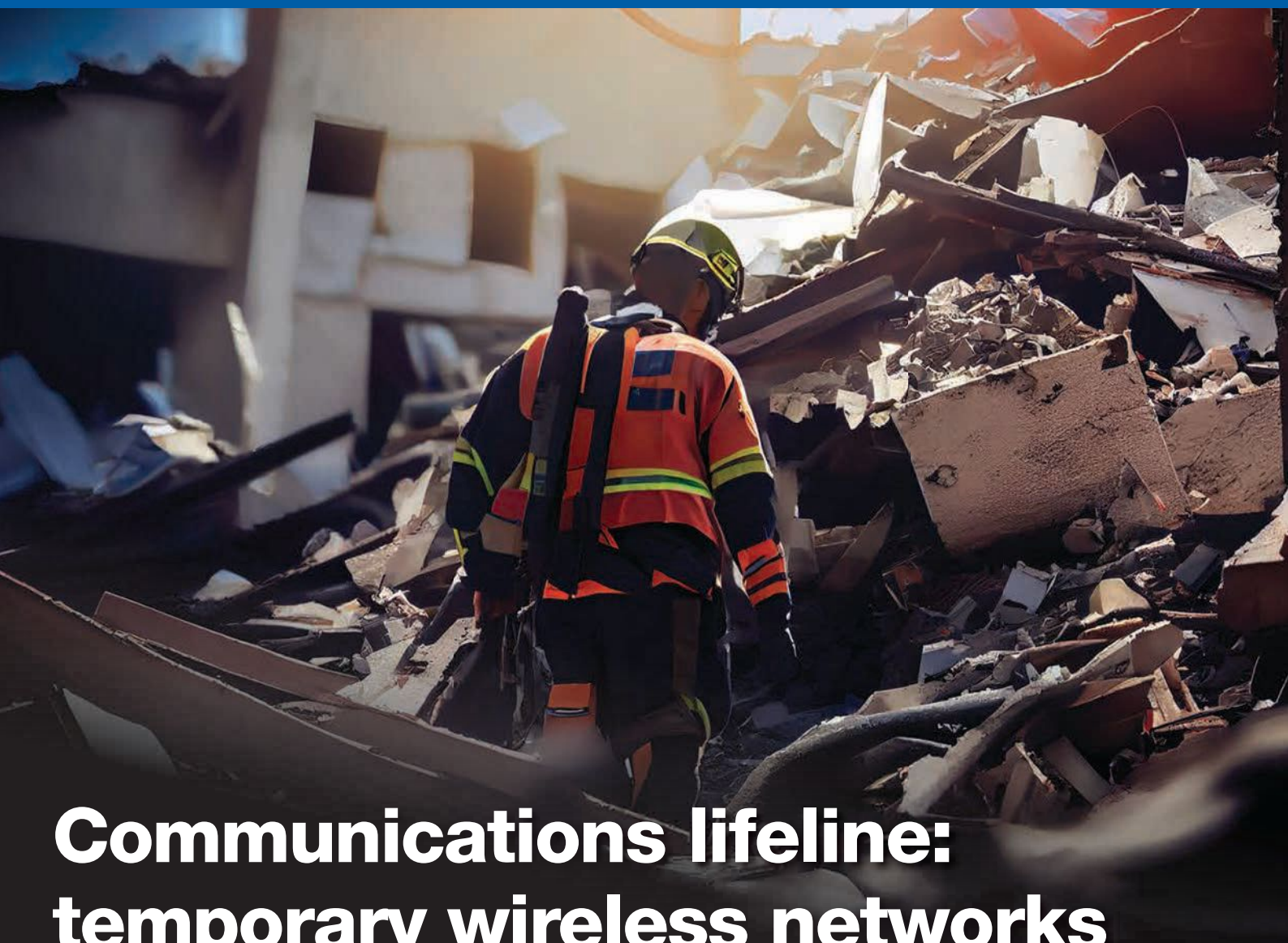
# CRITICAL COMMUNICATIONS TODAY

The global information resource for mission-critical communications

# Communications lifeline: temporary wireless networks in disaster zones




**November 2023**
*www.criticalcomms.com*
*@CritCommsToday*

SUPPORTED BY TCCA


# Meeting mission-critical needs of the future

- Designed for public safety
- Reliable access to push-to-talk over broadband with files, video, multimedia and location information
- Operate on 4G and 5G networks with quality of service for priority and preemption
- Improve situational awareness and operational efficiency

Airbus Agnet MCX, the next generation collaboration solution

**Read more**

Discover advanced solutions for reliable communication in a changing world

**Visit us at PMR Expo**
Hall 8.1 Stand: F010 G011

AIRBUS

CRITICAL COMMUNICATIONS TODAY

Editor: Philip Mason
philip.mason@markallengroup.com
Sales director: Jessica Szuts-Naranjo
jessica.naranjo@markallengroup.com
Senior sales manager: Sam Carter
sam.carter@markallengroup.com
Sales executive: Freddie Slendebroek
freddie.slendebroek@markallengroup.com
Graphic designer: Jamie Hodgskin
jamie.hodgskin@markallengroup.com

Circulation manager: Paul Creber
Sub-editor: Chris Young
Production director: Richard Hamshere
Managing director: Tim Willoughby
Chief executive officer: Ben Allen

Reader enquiry and subscription services:
Tel +44 1722 716997
(in the UK, 0800 137201)



MA Exhibitions
Part of Mark Allen

www.markallengroup.com

**Critical Communications Today** is published by:
MA Exhibitions Ltd, St Jude's Church, Dulwich Road, London, SE24 0PB, United Kingdom
Tel. +44 0207 738 5454
**Online edition:**
**www.criticalcomms.com**

**Twitter:** @CritCommsToday



**(Print) ISSN 2517-2719**
**(Online) ISSN 2045-8673**

**UK Personal subscription rates**

| | |
|---|---|
| Quarterly Direct Debit | £13.50 |
| Annual Direct Debit | £55 |
| Annual Credit Card | £58 |
| 2yr Annual Credit Card | £99 |
| 3yr Annual Credit Card | £139.50 |

Subscribe online:
www.magsubscriptions.com
Subscribe by phone: +44 (0) 1722 716997
Printed by: Pensord Press Ltd

The paper used within this publication has been sourced from Chain-of-Custody certified manufacturers, operating within international environmental standards, to ensure sustainable sourcing of the raw materials, sustainable production and to minimise our carbon footprint.

recycle
When you have finished with this magazine please recycle it.

*Cover credit: Adobe Stock/Radomir Jovanovic*

**NOVEMBER 2023**




NOVEMBER 2023

# In the wake of disaster

*CCT* editor **Philip Mason** discusses the contents of the latest issue, from the core theme of disaster response to important news in the field of national roll-outs

## MISSION STATEMENT

*Critical Communications Today provides the global mission-critical community with insight into the latest technology and best practice required to ensure that its members always have access to the instant, one-to-many wireless communications that can make all the difference in moments of crisis. We work to stimulate and focus debates on the topics that matter most and provide our readers with a means to raise their concerns.*

## GET IN TOUCH

**@CritCommsToday**

**criticalcomms.com**

**philip.mason@markallengroup.com**

## READ MORE ONLINE

Welcome to the latest edition of *CCT* magazine, the leading resource for those working within the critical communications sector.

This editor's letter is being written at a time of enormous tribulation across many parts of the globe. Much has been written about the ongoing climate crisis, for instance, the effects of which only seem to be getting more apparent with every passing year.

At the same time, the human race also seems intent on hurting itself by more direct methods, with two major conflicts currently taking place in different parts of the world. This is to say nothing of far-less-reported-upon violence in Syria, Yemen, Haiti and elsewhere.

As has always been the case during times like these, the ones who suffer most tend to be ordinary citizens, who inevitably have comparatively few resources to aid in their own survival when disasters strike.

With that in mind, in this issue we are focusing on the ways in which communications technology can contribute to disaster relief efforts, with the aim of helping to protect the most vulnerable.

Head to page 14 for an article focusing on the work of Disaster Tech Labs, which specialises in the roll-out of temporary wireless networks in disaster zones. The organisation has deployed in a variety of places across the world, including Ukraine, where it currently provides emergency connectivity.

On page 18, meanwhile, you'll find another disaster-themed article, this time reporting on increasingly ubiquitous 'public warning' technology. European states are currently mandated to operate these kinds of systems, but what provision is there for less-well-off parts of the world, the citizens of which are always inevitably more vulnerable?

Alongside these core themes, you will also find the latest news and opinions about important goings on within the mission-critical comms sector itself. In the realm of national roll-outs, for instance, head to our news section to read about the renewed SINE TETRA contract in Denmark, as well as continued concerns around ESN in the UK.

Staying in the broadband ballpark, TCCA's Legal and Regulatory Working Group has recently voiced its concerns about the use of commercial offerings for first-responder networks, in a white paper published in October. Head to page 11 to read more about this, and why – thanks to European regulations – first-responder 'network access' (ie, QPP) may be at risk in some European states.

Enjoy the issue.

**Philip Mason, editor**

*NEW TP9700*

# THE WORLD'S-FIRST

## Meet the World's-First DMR Multiband Portable.

**With DMR Tier 2 & 3, 900MHz 7/800, UHF and VHF.**
**All with professional compliance specifications.**

Available Now

Join us at the PMRExpo 2023
in Koelnmesse, Cologne / 28 - 30 November 2023 / Stand C 040.


Explore beyond.

TAIT TOUGH
PROVEN & TESTED

# Who, what, where

**EUROPE**

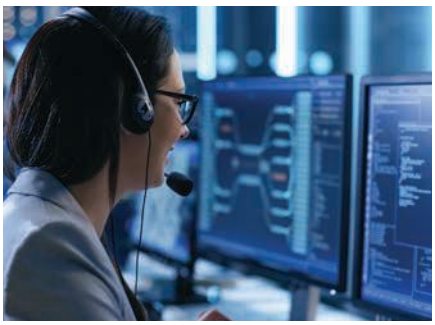
## Change at the top as PSCE appoints new president

Frequentis's Charlotte Roesener is the new president of Public Safety Communication Europe (PSCE).

Roesener has been with Frequentis since 2013, where she has been "driving critical communication applications in the public safety domain as product manager".

To quote a PSCE spokesperson: "Charlotte has a strong expertise in technology and AI and has years of professional experience in the field of public transport, communication for public safety, and more recently with a focus on broadband communication."

Discussing the presidency, she said: "It is a great honour – and equally a pleasure – to take on the presidency for the next months. Since its foundation in 2008, PSCE has become a unique and independent forum."



Adobe Stock/Gorodenkoff

## BT signs air traffic technology agreement

Comms provider BT has signed a seven-year deal with NATS, which it describes as the UK's leading provider of air navigation services.

According to BT, NATS is involved with over 2.5 million flights every year. The new contract is expected to "strengthen its technology infrastructure by creating a future-fit strategic network architecture, supporting air traffic operations in the UK".

A spokesperson for the communications company said: "BT will take responsibility for the consolidation and modernisation of NATS' critical data network, as well as managing digital networking and cybersecurity across its sites.

"It will also develop an enhanced cybersecurity capability with NATS, which will include a new proactive central co-ordination point for cyber resilience."

Adobe Stock/steve

## UK fire and rescue service updates control room tech

Essex County Fire and Rescue Service has deployed new control room technology, provided by Motorola Solutions. Products include the company's Control Room Solution, for call handling and emergency dispatch.

According to a spokesperson for the company, the solution provides: "A unified system for emergency call handling, incident command and resource deployment with an intuitive and highly configurable user experience.

"It also enables flexible operational practices to support collaboration and mutual assistance between fire services during spate conditions, where a large number of calls are received simultaneously."

Essex County is one of the largest fire and rescue services in the UK.

Adobe Stock/jamesteohart

## Norwegian health organisation deployment

Helsetjenestens driftsorganisasjon for Nødnett HF (HDO) in Norway has chosen Frequentis's "multimedia communication solution" LifeX for its control rooms.

According to Frequentis, the technology "will allow control room operators to see all the relevant incoming information about an incident at a glance". Discussing the solution's "additional mobile functionality", the company gives the example of nurses being able to continue consulting with patients by phone "when away from workstations".

The solution will be deployed across all 16 emergency medical communication centres in Norway, as well as more than 150 'general practitioner on-call centrals' and emergency departments. It will "migrate from the current Frequentis ICCS".

**MIDDLE EAST**


## Nedaa signs agreement with Dubai Customs

UAE-based communications technology supplier Nedaa has signed a memorandum of understanding with Dubai Customs. The aim of the agreement, according to Nedaa, is to "develop co-operation and partnership, and exchange experiences and knowledge" in relation to digital technology.

The MoU was signed by the CEO of Nedaa, His Excellency Mansoor Bu Osaiba, and Rashid Al Sharid, executive director, administration and finance division, at Dubai Customs.

According to a statement, via the MoU, the two parties will: "Focus on developing an operational mechanism aimed at ensuring a reliable and effective communication network for Dubai Customs, exchanging information and data related to the field of emergencies and public safety."

**ASIA**

Adobe Stock/LT

## Hytera wins major oil refinery contract in China

Oil and chemical specialist Sinopec Group has procured Hytera radios for use across its industrial sites, in 2023 and 2024.

The scope of the procurement, according to the radio company, includes TETRA infrastructure, PDT and PoC, as well as intrinsically safe radios and bodyworn cameras.

Discussing the roll-out, a spokesperson for Hytera said: "As the world's largest oil refinery and the second-largest chemical company, Sinopec Group has consistently prioritised the development of its ICT infrastructure. This bid leads to its first centralised framework purchase of two-way radio devices and systems."

Hytera China general manager, Mu Qiao, said: "Hytera has proudly served many petrochemical customers across the world, prioritising workplace safety above all else."

ASIA

Adobe Stock/adam

## New train lines deploy TETRA technology

Hytera is providing TETRA technology to the Changsha-Zhuzhou-Xiangtan Intercity Metro Xihuan Line, phase one of which started operation at the end of June.

According to a statement from the company, it is providing the system to "facilitate instant communication among various work groups". These groups include dispatching, maintenance, disaster prevention and environmental control workers.

The company has also provided 350MHz PDT technology, which is being deployed in Metro stations themselves, interconnected with local police and fire departments' communication systems.

The Nanjing-Chuzhou Rail Transit Line – Chuzhou section – officially opened for operation on June 28.

NORTH AMERICA

## FirstNet 2024 operating budget approved

The First Responder Network Authority board has approved US$451m in funding for the 2024 fiscal year.

The board approved $95m for the authority's operating budget and another $95m for reserves. Two-hundred and sixty-one million dollars, meanwhile, will go towards "investments in network coverage and emerging technologies".

FirstNet Authority board chair Richard Carrizzo said: "This demonstrates [the authority's] commitment to advance FirstNet beyond the initial buildout phase."

FirstNet Authority executive director and CEO Joe Wassel said: "Our top priorities for the coming year include the development of a 10-year investment plan to advance 5G and coverage on the network, as well as strengthening our programmes."

SOUTH AMERICA

Adobe Stock/Jose

## Industry giant extends Rio police contract

The Secretariat of State for the Military Police in Rio de Janeiro has extended its contract with Teltronic Brasil by a year.

The agreement will see the company providing "corrective and preventive maintenance services for the radio communications network that makes up the state's integrated critical radio communications system (SIRCE)". Teltronic Brasil is a subsidiary of Spanish telecoms giant Teltronic.

Discussing the technology in question, a spokesperson said: "The Nebula TETRA system began to be implemented on the occasion of the Pan American Games in 2007. Since then, in addition to managing the daily communications of the public security services, it has served to increase security during events such as the Rio Olympic Games in 2016."

# BAPCO

The Annual Event

## 6-7 MARCH 2024

COVENTRY BUILDING SOCIETY ARENA

RESERVE A FREE PASS

## THE UK'S LEADING PUBLIC SAFETY EVENT

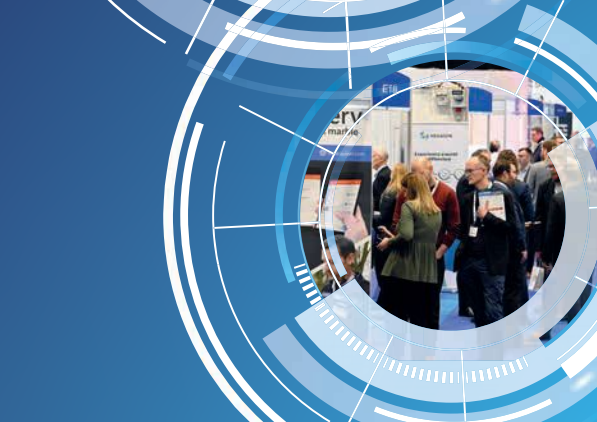
**80+** public safety technology companies

Gain valuable insights from

**world-class speakers**

**3 captivating** theatres

**NEW** product launches



## BAPCO-SHOW.CO.UK

@BAPCOEvent  BAPCO Annual Event

# News round-up

## PAC voices continued ESN concerns

The UK Public Accounts Committee (PAC) has said that "significant costs are being created for emergency services" due to the protracted roll-out of the Emergency Services Network.

The findings appeared in the committee's fourth report on the project, which was published earlier in the year. The document also stated that UK first-responder organisations were having to deal with the aforementioned costs without a "specific mechanism put in place by government" to help bear them.

Following the most recent inquiry, the PAC has called on the UK government to explore how to help fund the transition to ESN. It has likewise called on the UK Home Office to look at provision of new devices for the still-incumbent Airwave network, as well as maintenance of the legacy network itself. It has also asked for an "outline plan for the main building blocks of ESN" by the end of this year.

To quote the statement accompanying the report: "The PAC's inquiry, its fourth into the delayed programme, looked into how much delays to ESN had cost the emergency services, which have had to pay for additional Airwave devices as a result.

"ESN transitional costs for the ambulance service amount to £9.5m, while the fire service said it had spent £6m preparing for transition, and £2m on early versions of ESN which now had to be replaced. Police forces estimate that Airwave devices cost £125m since 2018 and expect to spend another £25m by 2026."

The statement continued: "Forces had spent a further £5m on transition teams. Further costs are inevitable, as current systems will be obsolete in 2028 and may need replacing again before ESN is ready."

The report also states that the Home Office appears "complacent in its confidence" that it could reduce the risks to the project, and that "its optimism appears disconnected from the reality of its performance to date and the challenges ahead".

The report follows Motorola Solutions' departure from the project, which took place in light of its issues with the Competition & Markets Authority over the company's provision of Airwave. Motorola was the original 'Lot 2' contractor, providing user services. The statement continued: "Following Motorola's departure from the project, to whom the department estimates it has paid some £140m without the taxpayer getting full value, only limited further progress can be made before the Home Office finds a new supplier.

"Other challenges include integrating the various parts of ESN together, testing the technology, providing the right level of coverage and resilience, and transitioning all emergency services onto the new service."

Public Accounts Committee chair, Dame Meg Hillier MP, said: "A clear direction must of course be established for this long-delayed project, but ESN raises wider issues on the approach to public procurement. The Home Office told our inquiry that it admits the commercial approach taken with ESN is suboptimal, but will be pursuing it regardless.

"New risks will be created if it now rushes procurement or delivery as it searches for a replacement main contractor. The risks of outsourcing services must be better managed, as the government is still accountable for value for money when it does so."

## British military leverages LEO connectivity

The crew of the Royal Fleet Auxiliary ship Argus is using internet with coverage provided by low Earth orbit satellite. The technology was supplied by OneWeb, in collaboration with its distribution partner Airbus.

The connectivity is being provided by the company's Kymeta Peregrine u8 terminal, which was fitted while Argus was docked in Falmouth in Cornwall earlier in the summer. The company says that it is the first military vessel to be using the technology.

Discussing the product, a spokesperson said: "The maritime terminal will provide reliable, low-latency, high-speed broadband connectivity anywhere in the world, even during challenging sea conditions and high-speed motions."

Lieutenant commander Ben Slater from the Royal Navy's digital unit said: "Crew welfare and morale is a key tenet of a platform's fighting capability. Enhanced connectivity, such as that delivered by low Earth orbit satellite networks, is an area that the Royal Navy are looking to exploit.

"Through close collaboration with industry partners, we have been able to fit a capability on board RFA Argus that will enable her crew to keep in touch with family and friends. [We are] looking forward to seeing how it performs at sea for the first time on a naval vessel."

RFA Argus performs several important roles for the UK armed forces, including being their primary casualty-receiving ship, equipped with a 100-bed hospital in times of conflict. It is also a training vessel for military helicopters operating at sea.

# Motorola renews Danish SINE contract


Adobe Stock/Mapics

Dansk Beredskabskommunikation (DBK) – owned by Motorola Solutions – has been awarded an eight-year contract to upgrade the SINE TETRA network in Denmark.

The contract was awarded by the Danish National Police's Center for Emergency Communication. As well as DBK's continued provision of the network, the agreement also includes details around new functionality, enabling "first-responders to automatically switch between land mobile radio and broadband, including Wi-Fi, 4G and 5G networks".

The agreement also includes the operation of a security operations centre, intended to monitor the performance of the network in real time, in order to address potential cybersecurity concerns.

Discussing the SINE network (otherwise known as Sikkerhedsnet), a spokesperson for Motorola said: "DBK provides the existing TETRA system which has, since its implementation, proven its reliability and criticality to Denmark's 40,000 first-responders and military personnel in day-to-day operations and emergency situations.

"The new TETRA infrastructure will enable first-responders to maintain reliable and uninterrupted communication through their TETRA talk groups when radio users move out of range, for example, in indoor or underground facilities."

Corporate vice-president at Motorola Solutions, Michael Kaae, said: "We are excited to build on our trusted relationship with the Danish National Police and the public safety agencies that keep communities safe.

"With the expertise of our teams in Copenhagen and worldwide, we will continue to provide exceptional operational service and TETRA innovation for decades to come."

## TCCA News

TCCA has published a white paper raising concerns around mission-critical user access to commercial networks.

The document focuses on the legal aspect of mission-critical broadband roll-outs, in particular how European regulations on net neutrality may affect "public safety operators that utilise radio coverage from commercial MNOs".

The white paper highlights in particular an apparent disparity between nation states in the adoption of rules ensuring quality of service, priority and pre-emption (QPP) on mission-critical networks.

Discussing this, a spokesperson for the organisation said: "While some EU/EEA countries have already adopted national rules to enable the use of QPP services under an exemption, under the TSM regulation, others are only at the starting point of assessing the legal possibilities.

"There are indications that different countries may interpret the TSM regulation on net neutrality differently. In some countries, the possibility to prioritise PPDR by national law has not yet been considered. This could lead to an equal treatment of PPDR and other end-users, even in emergency situations."

According to a statement, TCCA believes that "modifications to the existing regulations at EU-level" will help to secure mission-critical services for public safety across the continent. For future regulation, it says, "the mission-critical [community's] needs should be included from day one".

The spokesperson continued: "It is widely accepted that quality, priority and pre-emption is critical to secure effective mission-critical communications using commercial networks. The 3GPP standard and technical solutions currently available in the market support this.

"However, there is a concern whether it is possible to provide QPP services without breaching European regulation on net neutrality. Without QPP, PPDR users will have no priority above other mobile network users and may – if the traffic in the network is heavy – be prevented from communicating with other PPDR users."

Chair of TCCA Legal and Regulatory Working Group, Nina Myren, said: "It is essential that mission-critical users have priority in a crisis situation if they are using a commercial network service.

"Through TCCA, we are promoting co-operation between countries to develop a common understanding of the TSM regulation, including its applicability, so that the challenges can be addressed."

The TCCA white paper is called 'Legal and regulatory aspects regarding the realisation of quality of service, priority and pre-emption (QPP) in commercial networks'. In other TCCA-related news, the association has recently gained several new members. These include Consort Digital, Eventide and FirstNet.

# Maturing the network

**Philip Mason** talks to AT&T's head of FirstNet operations, **Scott Agnew**, about the evolution of the offer and the benefits of a competition-based model when it comes to scaling devices

**The FirstNet build-out began over half a decade ago. At what stage are you in terms of overall network coverage?**

We executed final operating capability in March of this year, but you couldn't say that FirstNet is ever 'done'. It's a 25-year commitment between AT&T, the American federal government and, of course, public safety.

In terms of the coverage itself, that was actually 'nationwide' in 2017. We've since completed the initial five-year build-out, and met/exceeded the contractual coverage requirements set by the federal government. But we aren't stopping there.

**What does that mean in real, geographical, terms?**

We have 250,000 more square miles covered than any other carrier, which basically equates to the size of Texas. The level of investment from the FirstNet Authority, alongside the commitment from AT&T to build Band 14, has led to a tremendous, powerful network.

In addition, we've also launched MegaRange, which harnesses Band 14. This is high-power user equipment – devices which can go up to six times further from the tower.

At the same time, there is also innovation when it comes to our 'deployables' [to provide additional coverage]. We started with 72 dedicated network-deployable assets that are specifically for FirstNet customers, in addition to the hundreds that we use for AT&T. Now we're up to more than 180 dedicated assets, and they can go anywhere in the US within 14 hours.

We've also driven innovation by developing Compact Rapid Deployables [CRDs], which can be hitched to a vehicle, as well as miniCRDs. These are the size of two suitcases, and which public safety organisations have the opportunity to own and operate themselves. From a deployment perspective, we view all this as highly successful, and arguably one of the best public/private partnerships in US history.

**On what basis did the build-out progress in the first instance? Was it primarily according to which states had signed up?**

The build-out in a given location didn't start until the state opted in. By the end of 2017, all 50 states had [opted in]. Every state, US territory and the District of Columbia had the option to either opt into FirstNet or use the Band 14 spectrum to build their own state RAN network.

Each state also had the opportunity to provide feedback and update their custom state plan. After careful review, each governor ultimately chose to opt into FirstNet. This meant that FirstNet truly was a nationwide network – exactly as public safety had envisioned.

**Has the 'competition' model been beneficial in getting commercial partners involved? What impact has it had on the availability of devices, for instance?**

As far as provision of devices is concerned, it's critical. We currently have over 720 devices certified on FirstNet, and when we look at the use-cases, it's just voluminous. That includes tablets, EMS vehicles, smartphones, PTT being used by police, IoT solutions, bodyworn video and more.

It's not just two-way communications now, because users are in the data world. So, form factors have to be broad and, as a result, we've done a lot of device certification.

From my perspective, we have to use the commercial model for devices and infrastructure, because that's the only way we're going to get the scale, as well as the device choices, and the cost that customers are looking for. They're used to going into a store and buying a couple of 100-dollar devices. Maybe they'll pay a premium, but the bottom line [from the user perspective] really is cost-effectiveness.

The only way to [provide the requisite devices] to scale is to use the commercial market. While, of course, at the same time, providing certification and any required maintenance releases to make sure they're secure and work for public safety.

**Can you describe the FirstNet-specific testing that takes place?**

I'd estimate that several thousands of additional tests occur, meaning that OEMs have to make the decision as to whether they're going to invest in that process. One of the concerns we had early on was whether we were going to get the device manufacturers to the table, because they're obviously always looking for volume.

> **We have to use the commercial model for devices and infrastructure, because that's the only way we're going to scale**

*AT&T's head of FirstNet operations,* ***Scott Agnew***

Sonim and Samsung came on board immediately, as did Apple and other device manufacturers. Having Band 14 as part of the device is second nature now.

**Would it have worked leveraging a different model, in terms of device certification and supply?**

We could have done it with different models, but the whole success of FirstNet is built off of that ability to scale. We dedicate where we must – the core and the spectrum – and scale wherever we can.

**How is the network currently being exploited by users? How has that evolved since the initial roll-out?**

A lot has changed over the years, and naturally, use-cases are continuing to change as well. When we started, users were primarily leveraging data. You'd see mobile data terminals in police cars, connected ambulances and so on. It was very straightforward in that regard.

We're now starting to see the mission-critical voice aspect, with user organisations wanting to use FirstNet in its entirety. That could be on a hybrid LTE/LMR device or a voice-only LTE device. Public safety in the US doesn't seem to want to invest in purely voice-only land mobile any more.

At the same time, IoT is coming into full force, with bodyworn video being one of the first key solutions being leveraged. I know this has been spoken about a lot, but the future really is video, video and video.

That being the case, we have to make sure that we continue to implement the technology that affords public safety the right quality of service for those particular solutions. That also includes things like closed-circuit surveillance, gun-shot detectors and so on.

**You mentioned the increasing popularity of broadband-enabled MCPTT among US users. Where does that leave P25?**

Customers are essentially asking whether there's an option to use FirstNet for MCPTT, and right now we're seeing them maintain both our network and P25. We offer multiple interoperable solutions.

"The future really is video, video and video"

Most of those are hardware-based, but some are based in the cloud. We're in the process of launching an interworking function that will provide another option for an IP, cloud-based solution. Most of our current conversations are around that. We see what's happening now as the natural process of the network. First-responders have become comfortable with the performance and coverage on FirstNet, and the number of MCPTT users now is growing steadily.

**Other US mobile network operators now offer services to the public safety market. To what degree has the evolution of FirstNet been driven by competition in that sense?**

When it comes to innovation and the evolution of the network, I always say that we're competing against ourselves just to get better.

In terms of the US market, I think it would be fair to say that FirstNet has driven it to be more conscious of the needs of public safety. That's a very good thing.

However, the difference between commercial carriers and FirstNet are things like the dedicated spectrum and core. If it were me – if I was a user – I would be using FirstNet.

**Do the users see it like that, from what you can gather? There are many factors involved in procurement decisions, after all…**

Public safety – or indeed, any user – buys on a variety of factors, including coverage, price and speed. That's what you look for.

Beyond that, public safety has a rich history of trusting its own communications infrastructure. Until now, they could not scale to a nationwide system built just for them, but FirstNet gives them that option, along with all of the other decision factors. America's public safety network is a reality and they are adopting in huge numbers.

Feedback from first-responders continues to go back into our network process, and we go forward from there.

For instance, we already have a non-standalone 5G solution for public safety.

Public safety users already have access to AT&T's 5G spectrum. And when that's at capacity, they'll fall back onto Band 14 LTE, with priority and pre-emption.

# Comms lifeline

Whether the result of climate change or conflict, 2023 has and continues to witness large-scale humanitarian emergencies taking place around the globe. Here, **James Atkinson** talks to voluntary organisation Disaster Tech Labs about its ongoing implementation of temporary wireless networks in areas hit by disasters

Communication networks are often heavily impacted by major natural and humanitarian disasters. Remoter areas of the globe may have little or no access to communication networks in the first place. Either way, it is imperative to provide temporary communications and internet access as quickly as possible in the wake of a disaster if the response is to be effective.

Disaster Tech Labs (DTL) is one of the leading organisations globally in the provision of communication services and internet access in areas affected by natural and humanitarian disasters. Evert Bopp, DTL's founder and CEO, set up the organisation in the wake of the terrible 2010 earthquake in Haiti, which claimed approximately 300,000 lives.

Initially conceived as a one-off project, DTL has since grown considerably. It has provided communications solutions all over the world, including the USA, Africa, Fiji, Nepal, Philippines, Italy and Ecuador. It has also provided them in Greece following the Syrian refugee disaster, Ukraine, in the wake of the Russian invasion, and also in Turkey and Morocco after the earthquakes this year.

DTL typically deploys a 'hub and spoke' model to set up a local Wi-Fi network. "That network needs to be connected to the internet, so in most cases that is satellite," says Bopp. "In some locations, where it is available, we use 5G. Or, if there is a reasonable distance – 15-25 miles – to a fibre link, we can build point-to-point [PTP] wireless radio links to the fibre hub."

From the central hub or network operating centre (NOC), DTL builds PTP spokes from the hub and internet backhaul fibre access points out to various smaller sites five to 10 miles away. "We put a router or a switch in place depending on the size of the need and create a local wireless LAN. We then have multiple small wireless LANs backhauled to the central NOC location and from there to the actual internet," explains Bopp.

In the past, DTL tended to use Ku and Ka band satellites, but as Bopp says: "They work, but they are not hugely fast, certainly by current standards and requirements. And they are horrendously expensive.

"The big change since then is the arrival of Starlink. That has had a huge impact, because it offers us the opportunity to use satellite-based backhaul for our terrestrial networks on very convenient, almost plug-and-play


Adobe Stock/Radomir Jovanovic

type of equipment, and at a very low cost."

The price service comparison between Starlink and the Ku and Ka band satellite services is considerable. A 4Mb uplink on the latter costs "several thousands of US dollars a month", according to Bopp. In contrast, the Starlink hardware itself costs €300-600, while the service cost for a 100Mb uplink is US$100 a month. "So, that is a significant price difference," he observes.

## Hub and spoke model

Drilling down into a typical network implementation, Bopp says: "We set up a Starlink dish with an ethernet cable. Starlink provides a router, which has no internet portal, only Wi-Fi, which doesn't serve what we need. But you can buy an adapter that gives you an ethernet port, which you can then plug into a switch.

"From the switch we would connect one or multiple Wi-Fi routers to an antenna that would be one point of a PTP link. Quite often we use sectoral antennas, as that allows us to use it as the end point for two or three PTP links in different locations. We might have two or three sectoral antennas on the mast to cover a 360-degree range."

> **"Our remote administrators are able to provision the configuration from anywhere across the world"**

PTP links then connect to the smaller spoke sites, which follow a similar set-up, albeit on a smaller scale than the NOC. For the uplink to the satellite and local site connectivity, DTL deploys a combination of long- and medium-distanced wireless PTP links, often using 5.4GHz and sometimes microwave depending on what the local licensing requirements and possibilities are.

"The smaller site antennas are more likely to be directional antennas connected via a cable down to the structure where the router is," explains Bopp. "The router either has Wi-Fi capacity itself or is plugged into a Wi-Fi access point, which provides the local connectivity. You can then use desktops, laptops and, more and more these days, mobile and portable devices such as tablets and smartphones."

DTL relies on volunteers to set up and configure all the equipment it uses, so it needs equipment that can be used out of the box and which can be remotely provisioned by one trained-up volunteer anywhere in the world. "That is the great advantage of the equipment we are using now," says Bopp. "We've used lots of equipment over the years, but in terms of wireless equipment, we now work with Cambium Networks out of the US for a variety of reasons.

"Their equipment is very good and serves exactly the purposes we need. Not only is it very durable in a physical sense, but they also have an online portal for wireless network management called cnMaestro. It allows you to provision the equipment, maintain and monitor the network."


Adobe Stock/DenisNata

## State and non-state actors

Network management can be carried out in a very granular way, says Bopp, right down to individual users, along with traffic monitoring and security. "It is all very easy to use, and that is important, because a lot of our people on the ground are volunteers. They all have a background in IT/networking, but not everyone is familiar with specific Cambium Networks hardware."

Cambium's remote portal allows DTL to create a configuration profile for different bits of equipment or different situations. Bopp says: "If we need to install a new router or access point, we can ship the unit to the location and then it is just a question of the local volunteer at the site plugging it into a network connection."

He continues: "Then one of our remote administrators can provision the configuration from anywhere in the world using the online management platform. That makes things much more efficient, as we do not need to train everyone up to know all the latest systems all the time."

Of course, the networks also need power. Initially, DTL used petrol and diesel generators, but fairly early on it switched to solar and wind power. Obviously this has environmental benefits, but the main reason was that fuel supplies often run out.

"We now have some designs that can be put up with our network equipment," says Bopp. "We use a combination of solar and wind, because it can never be [just] 99 per cent reliable. We build in a certain amount of safety margin in the amount of power that we require and generate.

"By using a combination of different sources you can be fairly certain that the network will keep up and running," he says. "We can monitor the performance of the generators too. So, we have the ▸


Adobe Stock/TimeaPeter

whole package now, not just the comms network, but also the power that keeps it operating."

Network security is another aspect that DTL has had to work on. At one time, DTL just put up a wireless network and let anyone use it. But it became apparent during the Syrian refugee crisis that a lot of state and non-state actors were actively trying to monitor some of the users on the network, such as dissidents.

"There were malware attacks and hacking attempts on both devices and networks, so we had to fairly quickly ramp up the security, not only passively, but also to actively monitor what was going on [with] the network," recalls Bopp. "We have to make the network as secure as possible, as we have a responsibility to our users to provide a certain level of protection."

## Work in Ukraine

Users of DTL's ad hoc networks divide into two main groups. First there are the local communities in the areas affected by the natural disaster or humanitarian crisis. What they need is the ability to stay in contact with friends and family.

They want access to social networks and essential information, such as updates on evacuation procedures, shelter locations, where and how to get medical care, and, if necessary, asylum procedures.

The other main user group is made up of national and local government organisations, NGOs, non-profit organisations and local first-responders. "What they want is business applications like streaming, Zoom, Microsoft Teams meetings and database applications," says Bopp.

"These organisations are basically businesses, so they use a similar approach to what you see in the corporate world. What they use in the office, they want to use in the field, so we have to address the bandwidth and security demands required to support that."

He adds: "The main point is that the technology and network configuration we use is fairly standard. I get the question: 'What is it that you guys do that is different from everyone else?' The answer is: 'We go out and do it.'"

While DTL has often deployed networks in the wake of natural disasters, it has also provided communications following major humanitarian crises.

In 2015, it implemented a network in an olive grove on the Greek island of Lesbos, which became the first Syrian refugee camp. DTL eventually expanded its networks to provide communications in 18 camps. "That collective network had nearly 400,000 people on the network across Greece at one point, so that was quite a significant undertaking," says Bopp.

More recently, DTL has done a lot of work in Ukraine. Initially, it provided communications at the choke points at the border crossings as Ukrainians fled to neighbouring countries at the start of the conflict.

It then provided communications for civilian field hospitals nearer the frontline, so medical staff had access to email, video-conferencing and telemedicine services.

One major problem was that both civilian organisations, as well as the Ukrainian military use Starlink satellite services.

The Russians programmed their reconnaissance drones to recognise the profile of a Starlink dish, which they then targeted with artillery.

Bopp says: "The local population can be very creative in the ways in which they are camouflaging these antennas, as they are targeted by the Russian military".

DTL is currently reviewing all its procedures and equipment to try to improve and future-proof its solutions to enable it to grow into the next 10 years.

DTL has deployed networks in the wake of natural disasters and wars

"We are building modular systems for ease of deployment and management," says Bopp. For example, DTL has assembled a flight kit with a Starlink dish, a router, a couple of Wi-Fi access points and different kinds of antennas, sectorial and directional. It has also assembled the equipment needed to power it.

However, Bopp believes there is a need for greater resilience at national level of communication networks and power grids, as society is now so heavily reliant on both. "Private companies can only do so much. For the continuation of society, this is something that governments need to focus on more.

"In light of the whole climate change issue, the number of extreme weather events will increase.

"Existing telecommunications infrastructure is getting damaged and put out of order temporarily or permanently, so there needs to be an increased focus on making the infrastructure more resilient and able to withstand extreme weather events by building in double or even triple levels of redundancy," he argues.

"We need to ensure that the various organisations, state agencies and first-responders all have the manpower and equipment needed to respond quickly to disasters and to put temporary communication fixes in place," says Bopp.

He also argues that given the recent cyber attacks on utility networks, there needs to be a much stronger focus on protecting power networks, as disruption to these essential utilities causes widespread disruption and also affects comms networks.

"Communications are so vital that there needs to be more focus on resilience and network protection. If you can prevent it in the first place, that is much more valuable than trying to fix it after it has happened," he says.

**"In light of the whole climate change issue, the number of extreme weather events is going to increase"**

Adobe Stock/ChaoticDesignStudio

# Alarming times

In the second of this issue's 'disaster'-themed features, **Philip Mason** talks to Everbridge about the global rise of broadband-based public warning systems

While certainly not a pleasant thought, it would appear that the world is becoming an increasingly dangerous place, particularly when it comes to the most vulnerable.

In the past few years, for instance, we have suffered through a global pandemic, something which had a profound effect both on our health as a species and our collective way of life. At the same time, citizens across the world are now starting to feel the impact of climate change in earnest. This includes wildfires raging across Europe, both last year and this, and most recently, serious flooding in Scotland and New York.

While the natural world is seemingly turning against us, meanwhile, humanity is just as busy turning on itself, with the geopolitical situation also becoming increasingly dangerous, seemingly across the globe.

This obviously includes the ongoing war in Ukraine, which at time of writing has continued for over 600 days, having claimed many lives. And, of course, we can now add to that tragedy the violence taking place in Israel and Gaza, events which have not only impacted many civilians but also put the stability of the whole region at risk.

The implications of all this turmoil have been reflected in various recent public safety initiatives specifically centred around the use of technology. If you are reading this issue of *CCT* from cover to cover, for instance, you will have already learnt how cutting-edge emergency communications are being deployed on the ground in disaster situations.

In this article, meanwhile, we are going to explore the ways in which governments are now able to alert whole populations to imminent danger before it happens. This could be within nation states themselves, or – as per one ongoing UN initiative – across borders.

The emergence of public warning technology has coincided with global legislation mandating its roll-out

## Early warnings for all

The emergence of the latter 'public warning' technology has taken place in tandem with legislation across the world mandating its roll-out.

From a European perspective, the most obvious example of this is Article 110 of the European Communication Code. This requires that: "[EU] Member States shall ensure that, when public warning systems regarding imminent or developing major emergencies and disasters are in place, public warnings are transmitted by providers of mobile-number-based interpersonal communications services to the end-users concerned."

As per the legislation, these measures needed to be in place by 21 June this year, and as such, we have seen high-profile roll-outs in countries including Norway, Estonia and the Netherlands. While no longer even a member of the EU, meanwhile, the UK has also recently deployed its own system, which received a first run-out in the form of a test in April.

The technology for many of these efforts was provided by Everbridge. Discussing the global move towards public warning systems, the company's president and CEO, David Wagner, says: "Our mission is – broadly speaking – to keep people safe and organisations running, using tech to digitise resilience.

"These national alerting systems are an extraordinary application of technology to save lives, and we've been honoured to roll it out in over two-dozen nations. Our support in the EU in the past three or four years is probably the strongest example of that, but we also have projects at state level in countries such as India."

While clearly pleased by his company's work in this field across all parts of the globe, you sense that Wagner is particularly energised when it comes to efforts in developing countries. After all – as he says – when disaster hits, it is invariably the nations with the fewest resources that suffer most.

The project he brings up with the most enthusiasm in regard to this is the United Nations' 'Early Warnings for All' initiative, in which Everbridge is playing a contributory role.

The UN website describes the need for Early Warnings for All in this way: "The Global Status Report (2022) reveals that countries with substantive-to-comprehensive early warnings coverage have disaster mortality eight times lower than countries with limited coverage.

"According to the Global Commission on Adaptation, giving just 24 hours' notice of an impending hazardous event can reduce damage by 30 per cent. Investing just US$800m in such systems in developing countries would prevent losses of $3-$16bn annually."

The statement continues by describing Early Warnings for All as "bringing together the broader UN system, governments, civil society and development partners" in order to "enhance collaboration and accelerated action to address gaps".

> **"We're still working with potential donor and recipient nations"**

The recent UK public warning test took place on the day of the of the London Marathon

Adobe Stock/maniacvector

According to Wagner, from a technological perspective, the aim is essentially to deliver a cloud-based version of the technology. He describes this as "easier to operate and deploy in a sustainable way" than the public warning system as it is deployed in, say, the UK, which functions via physical MNO data centres. (More on which later in the article).

Discussing the progress of the UN initiative, he says: "We're still working with potential donor and recipient nations. And when I say we, I don't mean Everbridge, I mean the international telecommunications arm of the UN and the UN secretary-general themselves.

"We're advocating for prioritisation of funding, and of course sustainability. Not implementing technology just for technology's sake."

## Cell broadcast or SMS?

Returning to the 'nation state' model and in particular the technology involved, the most popular (which is actually to say, pretty much ubiquitous) method of message delivery is currently based on something called cell broadcast.

For those who don't know, cell broadcast is a specific, one-to-many alerting channel, enabling the emergency message to be delivered to every mobile phone within a chosen location. One benefit of this – unlike SMS-based functionality – is that it avoids any potential congestion on the network during times when the message is being sent out.

According to Everbridge vice-president of international public warning systems Valerie Risk, meanwhile, other advantages of cell broadcast include the speed with which an alert can be delivered. Elaborating on this, she says: "Cell broadcast is a one-to-many technology. SMS is a point-to-point technology, meaning that one message will only reach one mobile device. Cell broadcast takes 10 seconds, whereas SMS can take between 30 minutes and several hours.

"If you want to reach one million people with SMS, you need to send out one million SMS messages. With cell broadcast, you can send out one message to reach a million people within a certain area."

As might be expected, Risk worked closely with the British government on its recent roll-out of the technology, tested – as mentioned – on the day of the London Marathon in April.

While not necessarily a complete success (some devices failed to receive the alert on the day, while others received the message up to a minute early), the test was valuable in the sense that it familiarised the British public with what until then had been an essentially alien technology.

More to the point, it also got them used to the reality of the alert itself, both in terms of the onscreen message and the deeply disruptive, 10-second tone accompanying it. This is something which Risk rather aptly refers to as the user's "personal air raid siren".

Going into greater detail about the ▸


Adobe Stock/Andreas

UK public warning system from an operational point of view, she says that in the first instance, the messages are initiated by the Cabinet Office. This is carried out on behalf of the relevant government/public safety agencies, via a central critical communications centre. The alerts themselves can either be bespoke or created via the use of a template.

Once drafted, the message is sent through via the major mobile network operators, by way of what Risk refers to as "a cell broadcast centre embedded in the network". It is then directed to specific geographic cells as required, with the appropriate location for the alert once again decided by the control room.

Discussing this, she says: "In the first instance, the warning will come into the centre to be assessed according to the proper operating procedures. They'll have a menu of messages that they've already created, as well as the ability to create them from scratch. The message is known as a 'broadcast cell entity'."

She continues: "The cell broadcast centre is essentially a server running very specific software, located within the mobile operator network. That intelligent centre can take the message, understand the geographical location that the sender has indicated, draw a map of the area and literally identify the cells within it."

Drilling down further into the role of the MNOs in all this, UK commercial operators were contracted for the project, with the aim of providing 99.9 per cent geographical coverage. These in turn have chosen their own partners, with Everbridge collaborating with EE, O2 and Three.

From the user side, meanwhile, the network subscriber does retain a certain amount of agency in that they have the option of turning their phone off altogether prior to an alert's arrival or putting it in 'airplane' mode. This, needless to say, isn't particularly practical when it comes to day-to-day use of the device; particularly if the recipient doesn't know that the alert is coming.

Climate change is a major issue facing the planet

## Bespoke deployments

Everbridge has been involved in over 20 roll-outs of this kind of technology across a variety of different nation states. That being the case, you can't help but wonder what the key differences might be between each project.

Each country is different, after all, politically, culturally and, of course, economically. The buy-in from telecoms providers themselves, meanwhile, may also differ from place to place.

Discussing how the company approaches these inevitable disparities, Wagner says: "These public warning projects are entirely bespoke. Obviously, the telecoms infrastructures vary a lot from place to place, as well as the regulation around them.

"On one end of the scale, you've got somewhere like Norway, which is very advanced, technologically speaking, and doesn't have a lot of people when it comes to its population. That means it's able to be really agile in terms of implementing technology at a national level. The Norwegian project took us something like 100 days."

He continues: "At the other end of the spectrum, we have a couple of Latin American customers, and those projects can take a lot longer. The politics are different from other places in the world, and the mobile network operating is much more complex, so projects can take years."

While some of the roll-outs are clearly more complicated than others, however, Warner insists that none of them are exactly what you would call straightforward.

Taking the UK as an example, he says that it has "great technology people" alongside a co-operative government. At the same time, the company still had to co-ordinate across three different MNOs, "with technology deployed in dozens of centres across the country".

"You get all the software and hardware lined up, and then you test it," he continues. "And if you have any glitches, you fix those in the test".

This complexity, he insists, was a key reason that not everything necessarily went as it should have on that fateful day in April. "Some of the glitches were right down at the individual cell phone level, with some people not having devices that were modern enough to accept an alert or updates".

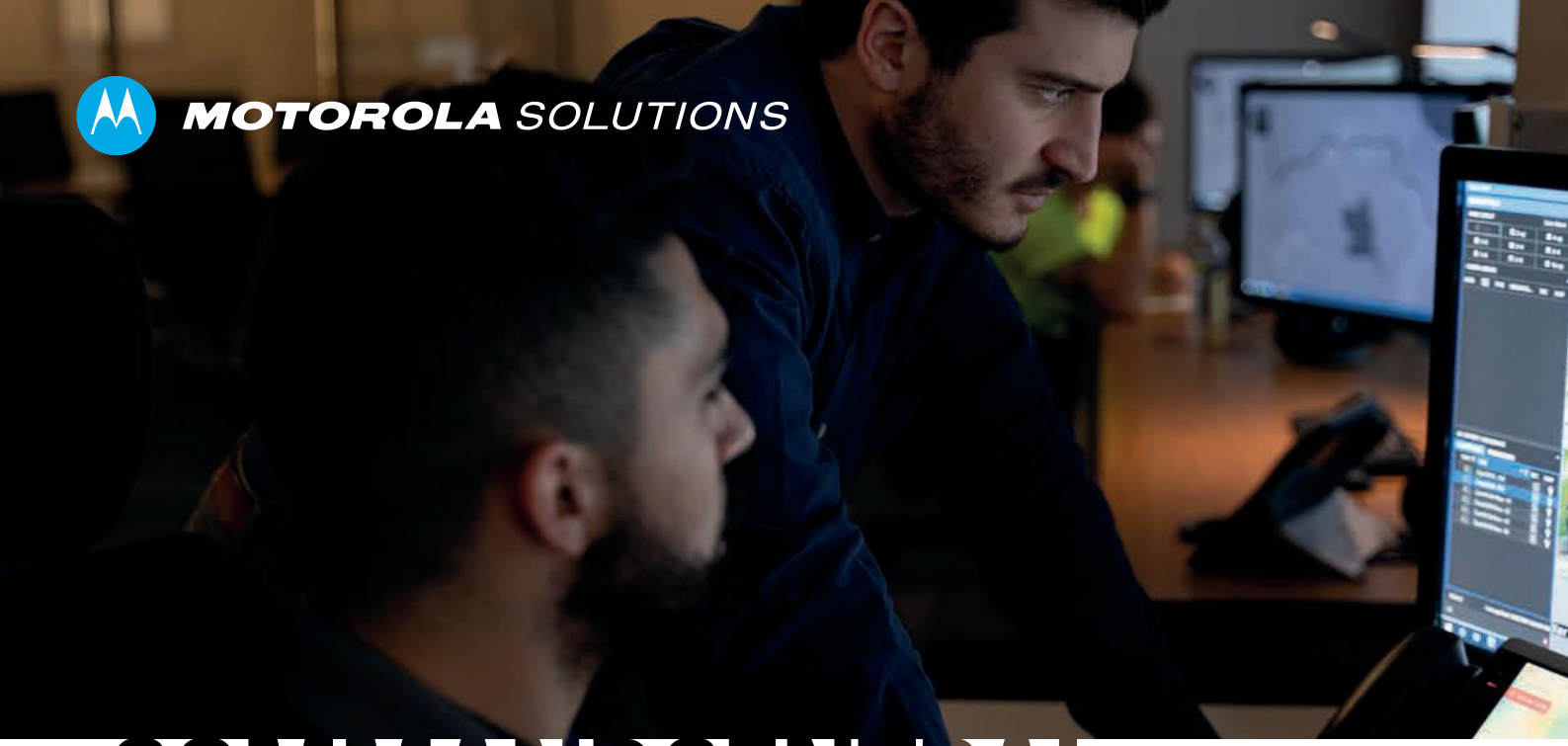
Emergency alerting is becoming an increasingly relevant technology when it comes to keeping the public safe.

At the moment, message delivery is facilitated by cell broadcast, which in Warner's words "has the advantage of being simple, direct and highly accessible".

Looking to the future, however, he is not discounting the possibility of SMS becoming the dominant standard in the field, despite its current drawbacks. "SMS has a little bit more complexity," he says, "but it could give a huge advantage when it gets to the next level of maturity, with citizens having the ability to respond back to emergency communications".

He continues: "The other really big uplift with it is that you can communicate with cell phones days and weeks later, over the whole period of recovery. Of course, that needs to take privacy concerns into account, which is both a cultural and a technological hurdle."

With the global situation apparently deteriorating on a monthly basis, it will be instructive – and also sobering – to monitor where public warning technology and its deployment evolve from here.



MOTOROLA SOLUTIONS

# COMMANDCENTRAL CONTROL ROOM SOLUTION

## SAVE CLICKS. SAVE SECONDS. SAVE LIVES.

**CommandCentral Control Room Solution streamlines incident management with a unified, intuitive workflow that meets the real-world needs of call takers and dispatchers. Phone calls, SMS, radio communications and multimedia files are seamlessly integrated, empowering control room staff to engage with communities and keep officers safe.**

### COORDINATE A FASTER RESPONSE

Answer and respond to emergency calls while interacting with intuitive radio controls to optimise incident response performance. Connect with front line staff over radio talkgroups or text.

### ENHANCE SITUATIONAL INTELLIGENCE

Capture key incident details during a call through intuitive forms. Linked data from previous incidents is automatically surfaced for greater situational intelligence.

### IMPROVE AGENCY EFFICIENCY

Automatically export call recordings and metadata to augment digital evidence associated with an incident. By reducing workflow barriers agencies can focus on keeping officers and the public safe.

### INVEST WHERE IT COUNTS

Broaden deployment options and reduce operating costs. CommandCentral Control Room Solution is accessible via common web browsers, with no need for costly bespoke hardware.

**Find out more at www.motorolasolutions.com/CommandCentralCRS**

Motorola Solutions Ltd. Nova South, 160 Victoria Street, London, SW1E 5LB, United Kingdom.

# Meeting the future

*CCT* reports from CCW 2023, held in the Finnish capital of Helsinki earlier this year

TCCA's Critical Communications World 2023 event took place at a pivotal time for the industry, with many nations now well under way in the ongoing move from narrowband to mission-critical broadband for first-responders.

The location for this year's event was also significant, however, with hosts Finland – via its Virve 2 project – playing a leading role in what might be considered the 'second wave' of national MC broadband roll-outs.

The relatively close proximity of Russia to Helsinki, meanwhile, also brought the importance of mission-critical comms and IT into even sharper focus, with the host country sharing a 1,340-kilometre border with its belligerent neighbour.

## Nordic defence

This latter consideration informed one of the most compelling panel discussions from the first day of the CCW conference, focusing as it did on the doctrine of 'total defence' among the Nordic countries.

Participants included Camilla Asp and Ronny Harpe of the Swedish Civil Contingencies Agency, the Norwegian Directorate for Civil Protection's Elisabeth Aarsæther, and Kimmo Kohvakka of the Finnish Ministry of the Interior. Discussing the concept in broad terms, Aarsæther said: "In Norway we are very keen on structures that bring us together. When the Norwegian armed forces are fully mobilised, it's about 75,000 people. The 'total defence' concept has never been laid down after the war, but it has been sleeping.

"But, in 2016, the government decided that we have to put forces together. So, after that we have been exercising a lot together and meeting up, from the governmental structure down to the local structure. Speaking with each other – how do we do this if something happens?"

Aarsæther continued by saying that these discussions also extend to what would happen if civilian support were required. This was echoed by Asp, who said that the


Adobe Stock/Alexey Fedorenko

total defence concept combined military and civil defence, with a "common goal" and "co-ordinated and integrated planning".

She continued by saying that 'civil defence' in this context meant the protection of civilians in relation to shelters, warning systems and evacuation. "It is maintaining the functionality of the society and how to secure the supply of goods and services, cope with disinformation and promote the will to defend the country," she continued.

Those who are familiar with the Nordics from a cultural perspective will recognise this urge to work together among countries such as Finland, Sweden and Norway.

Indeed, the overall theme of this year's CCW was 'success in cooperation', something which is most obviously illustrated – at least from a communications perspective – by the cross-border interoperability baked into those countries' respective emergency services TETRA systems.

Another highlight of the first day was ETSI CTO Adrian Scrase's presentation on the standardisation of 5G, relating in particular to its potential deployment in the mission-critical context.

5G Advanced will mark the mid-generation point between 5G and 6G

> **"BroadWay is about looking for the solution for what we call operational mobility, across Europe"**

Scrase began his presentation by discussing the increasing relevance of the standard, quoting figures suggesting that 240 commercial 5G networks have already been launched. "If we look at the GSMA's figures, roughly two billion 5G connections are likely to be in place by 2025," he said.

"Whichever way we look at this, it is deployment on a grand scale. The clever bit is how can we be sure that the mission-critical elements are captured within that, so that the relatively small [mission critical] community can benefit from the economies of size."

Discussing the ongoing evolution of the technology itself, he stated that 3GPP Release 17 is complete, with work on Release 18 continuing to go forward as we speak. "That," he said, "will be completed by the end of this year and is where we'll change the branding from 5G to 5G Advanced. That will be the mid-generation point between 5G and 6G."

The timeline for Release 19 has already been set, meanwhile, with estimated time of completion being the middle of next year. The research effort around 6G is ongoing.

Summing up – and addressing the audience directly in relation to 6G in particular – he said: "From a mission-critical point of view, the question is really are you sure that what you need is being represented with the people who are setting the plans for future generations.

"Because if not, if you come to the table after the generational plans have been made, then it's going to be very difficult for you to influence them. It's a general call that you [the mission-critical community] should be aware of what's happening in terms of setting the agenda for the future and making sure that every step of the way, mission critical is included in that agenda."

As might have been expected, a large chunk of the CCW 2023 agenda was taken up with content relating to the roll-out of mission-critical broadband to first-responders. This included projects taking place within nation states themselves, as well as multinational endeavours.

The latter is exemplified by the BroadWay/BroadNet project, which is attempting to provide cross-border mission-critical broadband roaming to European emergency services.

Discussing progress during a presentation on the first day of the conference, BroadNet co-ordinator David Lund said: "BroadWay [is about] looking for the solution for what we call operational mobility.

"Operational mobility is the ability for responders to carry out their operations wherever they are, whenever they need to and with whoever they're tasked to co-operate with."

He continued: "BroadWay is a team of 11 countries at ministry and agency level, coming together to jointly procure the solution for operational mobility, based on the 3GPP standards."

During the presentation, Lund was accompanied by Airbus SLC head of Europe Eric Davalo and Gunter Graf, who is the vice-president of innovation at Frequentis. The businesses in question led the two consortiums, which are still in competition, to provide the final system.

## Government authorities

Remaining on the topic of mission-critical broadband deployment, one of the key CCW exhibition features since its return in 2021 has been the 'Government Authorities Global Village'. In Helsinki, this was augmented by GAGV conference panels, with sessions focusing on 'Critical broadband developments from around the world' taking place across all three days.

As might be expected, updates were delivered by a variety of countries including France, Germany, the USA, Australia and, of course, the Nordics. (Alongside Finland, the show was co-hosted by Norway, Denmark, Estonia and Sweden).

Discussing the situation in Germany, BDBOS head of directorate strategy and central management Thomas Scholle said: "We are currently running the largest TETRA system in the world, with more than 1.1 million subscribers and more than 5,000 base stations. It's a mature and good system."

This system, said Scholle, would continue to run for "very, very many years" for mission-critical voice. At the same time, he continued, users desire broadband, which has resulted in the development of a "four phase programme". This was conceived of prior to COVID, in 2019, but is still regarded as valid, although "maybe the timescale needs to be adjusted a little bit".

Describing each of these phases in turn, he said: "We want to start with Phase 0, which is a pre-phase. We're doing this because our users are partly using broadband already, by commercial contracts. They have contracts with national network operators, and we want to consolidate these under one contract."

If this runs in a positive way, he said, "we might even be able to offer national roaming, prioritisation within this contract, but this [remains] to be seen".

Phase 1, meanwhile, will see the setting up of a dedicated core network for PPDR users. That will involve finding one national network operator via a tendering process in order to set up and run the network.

"So, at the end of Phase 1 we will have a core network that we own. We will have full control of our data, and all three big nationwide networks in Germany will be connected.

"At that point, we can start using mission-critical applications." That is planned for the end of this decade, but can only take place – Scholle said – by obtaining the requisite frequency. Phase 3 will see the 'powering down' of the BDBOS TETRA network.

Scholle finished his presentation with a deep dive into the expected timeline, describing the plan year-by-year. He said: "From '27 to '31, we will introduce all relevant MC services, and allow our users also to use their own applications. [That's] from our federal states, from the 16 landers and from other organisations. Then I expect the national plan for the allocation of frequencies to be complete.

"As soon as this is clear, we want to start a tendering process for the radio access network. We will need to build a few more towers, and will also have to go into negotiations with vendors and MNOs again so that we obtain the necessary equipment for the sites. We will start to build them in 2029."

Another compelling presentation from the Government Authorities Global Village stage came from the Danish broadband project's project manager, Jesper Rasmussen. He was speaking on behalf of the Centre for Critical Emergency Communication, which is a part of the Danish national police.

Like Scholle, Rasmussen began his session by providing some context around what the country's emergency services are already using when it comes to critical communications. He said: "Let's start by going back to the good old days, back in 2010, just a couple of years after Apple produced the first iPhone.

"We introduced the nationwide emergency [TETRA] network in Denmark called SINE, which in Danish is short for safety network. The reason for introducing [the technology] was to give public safety the best conditions for efficient communication, when helping and protecting its citizens. The network is operated by DBK, which is a subsidiary of Motorola."

In the years since the network was completed, he said, SINE has become trusted and heavily relied upon by its users, "as TETRA systems tend to".

Having described the current narrowband network, Rasmussen went on to describe the circumstances around planned network evolution. The first step, he said, was to renew the present voice contract, which expired in 2021 but had since been extended to next year. (You can read about recent developments in relation to the SINE network in this issue's news section).

He continued: "Some key information about the next contract of ours... The content will also only

# KEEPING THE EMERGENCY SERVICES CONNECTED


## Secure mission critical communications solutions for public safety organisations.

CSP-MCX is a complete Mission Critical solution implementing all components of the functional model foreseen by with 3GPP Standard MCX.

It includes features from MC PTT, MC Video and MC Data providing PPDR users with the next generation platform for Critical communications over 4G/5G networks. It also provides all standard based configurations and management functions such as: Identity Management Server (IDMS), Configurations Management Server (CMS), Group Management Server (GMS) and Key Management Server (KMS).

uk.leonardo.com

LEONARDO

ACCELERATING TECHNOLOGY EVOLUTION

be voice, as [is the case with] the current one. Our tender [at the time] is technology-neutral, and the model is still a full-service model."

While the tendering process for the new voice contract was taking place, however, something that was becoming "more and more evident in the mission-critical sector [was] the continued interest in broadband technology. So, of course, the question is, what about broadband in Denmark?"

Discussing this, he went on to say that Denmark is already a heavily digitalised country, something which in itself currently affects how its emergency services deal with incidents. "Our own studies also confirm this," he continued. "As well as the way that they already use broadband-dependent tools to handle data during an emergency incident."

At that this point, the broadband tools being leveraged are only commercial "best effort", rather than being based on mission-critical standards. "But the essence is, this is not new to our emergency services with broadband."

Rasmussen drew his session to a close by saying: "To meet these new [broadband-based] requirements, we have initiated a number of new activities, most predominantly the current governance which has been expanded to support broadband discussions among our emergency services.

"We have in the past decade been supporting a governance across our emergency services, deciding on the best use of our mission-critical communication. We have now started to expand this governance so that other types of communication also can be included."

Another important Danish initiative currently "taking up quite a lot of time also" is the work going on around quality of service, pre-emption and priority in regard to any potential mission-critical broadband network.

"And finally," he said, "we also have the ambition to start small-scale testing. This will be primarily focused on exploring the potential for temporary coverage for tactical bubbles, but also the potential for private networks."

Another presentation relevant to the location of this year's show, meanwhile, focused on cybersecurity.

Titled 'How war in Ukraine has changed the cybersecurity landscape', the session featured NATO CCDCOE head of technology branch Urmas Ruuto and Milrem Robotics science and development director Raul Rikk.

Discussing Russian 'supply chain' attacks which took place towards the beginning of the invasion in 2022, Ruuto said: "One of the things that we can see is that attacks are more politically motivated. Speaking in general, cyber attacks are mainly ransomware because hackers want money. Now, it's just the breaking of things."

He followed this up with information derived from the Estonian state information agency, discussing denial-of-service attacks taking place in 2021/2022. "The number of attacks is four times higher. Obviously, if you do something which is not popular [with] the Russian Federation, you might expect to be hit."

He augmented this with a slide detailing the removal of a Soviet-era tank monument from the Estonian city of Narva in August of last year. Following this, he said, "there was a huge attack rate coming to Estonia".

The CCW 2023 exhibition floor was full across all three days

## The exhibition floor

CCW in Helsinki offered one of the fullest conference programmes in the history of the show, making it pretty much impossible to cover it all in any depth (certainly not in the space of just a few pages). The same goes for the exhibition floor, which was very full across all three days.

As might be expected, there were plenty of Nordics-based companies exhibiting at the show, including Ericsson and Nokia, both of which we caught up with on the show floor.

Discussing the latter company's presence at the show – and the recent change to its branding – its global head of enterprise business, Chris Johnson, said: "We're here at Critical Communications World, and really proud to be hosting this in our home

# Discover more online today

**News** **Features** **New Products** **Events**
**Interviews** **Expert Opinion** **Video**


Visit our new **LAND MOBILE** website for more news, interviews, features and videos. Visit it at:

## www.landmobile.co.uk

**Land Mobile** informs the complete wireless communications for business buying chain in the UK - all the way from the manufacturer to the end user.

LAND MOBILE
WIRELESS COMMUNICATIONS FOR BUSINESS


Ken Rehbehn chaired GAGV discussions

> **[Previous] branding was associated with mobile phones, which we haven't done for a long time**

country. Our brand was last refreshed about 55 years ago, so there's been a lot of water under the bridge.

"The old branding was quite often associated with mobile phones, and we haven't done that for a long time. There's a whole new generation of customers and partners that weren't around then. Nokia today is primarily telco infrastructure and more prominently now, B2B, enterprise and government."

Linking in with an important theme of the conference mentioned above, meanwhile, one key area of work being demonstrated by Ericsson was its knowledge of the "threat landscape" in relation to mobile networks.

Discussing this, a spokesperson for the company said: "We want operators to be prepared using our software. And to be prepared in these kinds of dynamic networks, one needs to automate a lot of things.

"Automation is key to what we do, making sure the posture is as good as possible to protect the network."

Another big name on the exhibition floor was Sepura. Traditionally associated with the manufacture of narrowband products, the company is now branching out into hybrid solutions, such as its SCU3.

Discussing the latter, head of pre-sales engineering Luke Stanley said: "New to the show, it's our first LTE mobile. Released later this year, it now has TETRA on board as well.

"So, [customers] have the option to take TETRA mobile, but [they] also have an Android OS platform there, with all of the applications. It's also a router and Wi-Fi hotspot."

Control room manufacturers were also represented on the exhibition floor, including Frequentis and Hexagon.

Discussing why the latter decided to exhibit at the show for the first time in 2023, its managing director, Peter Prater, said: "In the safety [vertical], Hexagon provides collaboration tools, command and control tools, event management tools. The reason we're [at CCW] is to demonstrate the ever-closer ties between the command and control centre and the solutions that are sold here, and their immediate proximity to the radio networks."

Prater continued: "What we've found in the marketplace over the last five to 10 years is more of a coming together of the radio control and command and control. Different things, but now coming together in one product base."

Another product area which is becoming increasingly crucial to mission-critical communications is satellite – for instance, in the provision of backhaul for remote locations.

Discussing its offering, Globalstar IoT regional sales manager Robert Clarke said: "Globalstar is a worldwide satellite network, and we see [CCW] as a means of communicating with customers the need for satellite to fill gaps in where cellular and terrestrial are not available.

"Globalstar has the ability to offer services globally for both personal monitoring and asset tracking. We have many different types of verticals."

Another first-time exhibitor, meanwhile, was Cyrus Technology, which manufactures ruggedised devices across a variety of verticals, in and outside of the mission-critical sphere. "Mission critical has always been very good business for us, and from the beginning, we saw the huge potential in this market," said the company's VP of global sales and marketing, Javier Holguin Trujillo.

Finally, we were able to catch up with Zebra Technologies, which also provides handheld devices across a range of industries.

Discussing its presence at the show, Zebra's Oliver Ledgard said: "In the last five or 10 years, we've been getting pockets of wins in this space, but there hasn't been an overarching focus on [these verticals]. So I'm now looking at a strategy to target government, public safety and public sector customers, specifically across EMEA."

He continued to illustrate the "wins" the company has had so far by talking about the roll-out of its L10 tablet to the Spanish police. The company has also collaborated with emergency incident management specialist Unblur.

Critical Communications World has always been an important show in its sector and is continuing to make good on that reputation in the years following the COVID-19 pandemic. Its next iteration will see it leaving Europe for the first time since 2019 and heading to Dubai.

# Tell your side of the story

Join the discussion and stay up to date with the latest news

Look out for LAND MOBILE's tweets on breaking news and industry events

Tweet us at **@Land_Mobile**

**Expand the reach of your network**
Connect with us via. LinkedIn

Search: "**Group: Land Mobile**"


3 WAYS to connect

**Twitter:** @land_mobile
**LinkedIn:** linkedin.com/groups/4761728
**Website:** landmobile.co.uk

LAND MOBILE
WIRELESS COMMUNICATIONS FOR BUSINESS

# Product news

Adobe Stock/Scrudje

Adobe Stock/Alexey Fedorenko

Adobe Stock/3dsculptor

## Nokia launches 5G devices for industrial environments

Nokia has launched a range of industrial 5G devices, for use in environments such as "ports, mines, chemical plants and offshore platforms".

These include ruggedised handheld devices, as well as "enhancements to worker and device related applications". Discussing the move, a spokesperson said: "By adding these new assets to our end-to-end platform for industrial digitalisation – along with our private wireless and edge applications – Nokia reinforces its industry leadership with a market-leading portfolio."

The range includes a ruggedised handheld unit, intended to support public safety workers communicating over Band 68. "The US-manufactured device," says Nokia, "has a long lifecycle and is IP68-rated for operation in remote or harsh environments."

The company is also adding to its portfolio of ruggedised 5G handhelds with EX-rated phones, having partnered with i.safe MOBILE GmbH. The company describes the latter as a "world market leader for explosion-proof mobile devices and solutions".

Other new products include industrial solutions deployed over the company's Digital Automation Cloud, and the updated Nokia Team Comms 23 application.

Discussing the launch, CEO of i.safe MOBILE, Martin Haaf, said: "We are pleased to support Nokia with our decades of expertise in explosion-proof mobile devices. The combination of our devices with Nokia's solutions offers companies a great added value on their digitalisation journey."

## Airbus Agnet MCx introduced to Luxembourg

Airbus has signed an agreement with operator POST Luxembourg to introduce its Agnet MCx solution to the Luxembourg market.

Discussing the agreement, an Airbus spokesperson said: "Agnet MCx will be made available to POST Luxembourg critical communications customers for use on their 5G network. Public safety and governmental organisations – as well as communal administrations and private companies – will be able to benefit from [this]."

The company describes Agnet MCx as providing mission-critical push-to-talk, as well as secure instant messaging, video streaming/sharing and location services.

Airbus SLC head of Europe, Eric Davalo, said: "We are very pleased to enter into this partnership. Airbus has a leading role in the critical communications industry, and is involved in leading projects in Europe such as BroadWay and RRF.

"It has long-term partnerships with mobile network operators in many different countries and continents."

Cliff Konsbruck, deputy managing director of POST Luxembourg, said: "POST Luxembourg is entering a strategic partnership with a European industry flagship, the common goal being to bring value creation to the Luxembourg market.

"Airbus's Agnet MCx solution integrates with POST Luxembourg's core network, while taking advantage of specific 5G features such as slicing, so that network capacity can be allocated and guaranteed to mission-critical communications."

## Vodafone engineer carries out 5G space call

AST SpaceMobile and Vodafone have completed a space-based 5G voice call, in what the latter company has claimed to be a world first.

According to a statement, the call was from Hawaii to Spain.

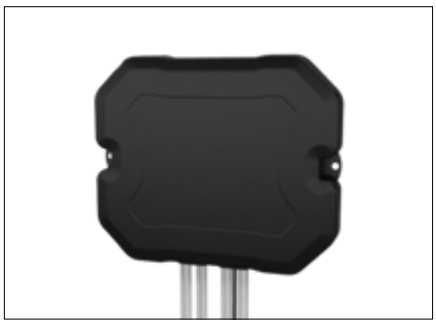
It was made using an "unmodified" Samsung Galaxy S22 smartphone, in conjunction with AST SpaceMobile's BlueWalker 3 test satellite. The company claims that BlueWalker 3 is the "largest commercial communications array deployed in low Earth orbit".

Discussing another test taking place simultaneously, a spokesperson for the companies said: "AST SpaceMobile, [also] supported by Vodafone, broke its previous space-based cellular broadband data session record by achieving a download rate of nearly 14Mbps."

Vodafone group chief executive Margherita Della Valle said: "Vodafone is striving to close the mobile usage gap for millions of people across Europe and Africa. By making the world's first space-based 5G call to Europe, we have taken another important step in realising that ambition."

Going forward, AST SpaceMobile plans to launch five commercial BlueBird satellites, with the estimated moment of deployment being the first quarter of next year.

Meanwhile, Vodafone and Vodacom plan to use low Earth orbit satellites to connect "geographically dispersed cellular antennas back to the companies' core telecom networks".



## Panorama Antennas launches new 'batwing' device

Panorama has launched a new batwing antenna range, in the form of its BAT[G] M4-6-60.

According to a spokesperson for the company, the device is designed to "transform the original batwing antenna into a versatile 4x4 MiMo solution".

The spokesperson continued: "The BAT[X] M4 range offers a comprehensive solution for 4G/5G connectivity in a discrete package. With the added option of GPS/GNSS and dual-band 2.4/5.0-7.2GHz Wi-Fi 6E, this range is a game-changer for covert public safety vehicles."

According to the company, the 4G/5G antenna elements cover 617-960/1427-6000MHz, with the aim of providing "a robust communication link to ensure high data rates even in challenging network coverage areas".

Panorama states that the product can incorporate a GPS/GNSS module with advanced filtering for either L1/E1/G1/B1 only, or dual band L1/E1/G1/B1 with L5/E5a.

It is IP55-rated and designed to be mounted either on or under a vehicle dashboard/parcel shelf.

In the release for the product, Panorama Antennas describes itself as a "family business now in its third generation. [It serves] the consumer wireless, M2M & IoT, in-building and public safety industries".

The company was established in 1947 and is based in London. It celebrated its 75th anniversary in 2022.

Adobe Stock/Dreamframer

## NextNav conducts successful TerraPoiNT test

GPS specialist NextNav has successfully tested its positioning and timing solution, which according to the company combines its own TerraPoiNT product with "existing LTE and 5G network signals". The company describes TerraPoiNT as an "assured PNT [position, navigation and timing] solution".

Discussing the event, a spokesperson for the company said: "The test demonstrates how TerraPoiNT signals can be integrated with existing cellular signals to deliver accurate 3D positioning and timing information that is not reliant on conventional satellite-based GPS and GNSS signals. It took place in and around San Jose in California."

The spokesperson continued: "Using dedicated terrestrial transmitters and LTE/5G signals, NextNav's system can augment or complement GPS in places where GPS signals may not be available. This includes indoors, urban areas, or situations where GPS signals may experience interference.

"Integrating TerraPoiNT with LTE and 5G signals provides a rapid and cost-effective approach to scaling resilient PNT solutions in GPS-denied environments."

Co-founder and CEO of NextNav, Ganesh Pattabiraman, said: "Whether it is utilities, banks, data centres, transportation or emergency services, critical infrastructure today is reliant on GPS for position, navigation and timing services. With this integration we have demonstrated a highly scalable and lower-cost alternative – a 3D PNT solution which overcomes the vulnerabilities of GPS."

Adobe Stock/Lubos Chlubny

## PCTEL omnidirectional antenna

PCTEL has launched a 5G FR1 omnidirectional antenna, optimised for industrial IoT applications.

The company says that the solution is suitable for "a wide variety of mission-critical communication applications", including utilities, smart cities, factory automation and "overall industrial IoT applications".

Discussing the product, a spokesperson for the company said: "PCTEL's new 5G FR1 omnidirectional antenna offers a mechanically robust design, flexible installation, superior bandwidth and superior coverage within the full 5G FR1 frequency range.

"The demand for reliable, secure wireless connectivity and extensive coverage is increasing.

"[The new] antenna has been designed to meet the requirements of today's wireless networks, and to provide continuous connectivity in the harshest environments."

PCTEL's technical product manager, Denis Dmitruk, said: "The new 5G FR1 omnidirectional antenna is a reliable, cost-effective solution that has been tested in the harshest environments and offers high performance across the whole 5G FR1 frequency band."

PCTEL as a company describes itself as "a leading global provider of wireless technology solutions, including purpose-built industrial IoT devices, antenna systems, and test and measurement products.

"[It] solves complex wireless challenges to help organisations stay connected, transform, and grow."

# TCCA Critical Communications World 2024

**Critical Communications World** is a global networking hub uniting mission-critical and business-critical end-users with manufacturers


## 3 CAPTIVATING THEATRES TO EXPLORE

As has become a hallmark for CCW, a 3-day conference programme will be delivered by thought leaders and influencers from across the globe. 2024 will focus on securing society and industry and how connection is the lifeline.

## PRODUCT LAUNCHES & OPPORTUNITIES

Join 100+ exhibiting companies and a host of experts from across the sector with the latest in innovative products, equipment, and solutions. Enjoy connecting in-person as you discuss your specific business needs and search for new technology and opportunities.
Join guided Tech Tours and explore specific areas of interest.

# 14-16 MAY 2024

DUBAI WORLD TRADE CENTRE, DUBAI, UNITED ARAB EMIRATES

**WWW.CRITICAL-COMMUNICATIONS-WORLD.COM**

@CritCommsSeries  TCCA Critical Communications World

and suppliers for 3 days of inspiration, sharing knowledge and making connections. Taking place in Dubai, UAE on **14th - 16th May 2024**, the Dubai Government's Secure network provider Nedaa joins us as Host Operator in collaboration with the Dubai Department of Economy and Tourism.

## NETWORK WITH COLLEAGUES & GLOBAL AUTHORITIES

Join your peers as the entire sector comes together under one roof! This year we are once again looking forward to welcoming government agencies from around the world.
From networking on the exhibition floor to Q&A sessions within the conference, you will find no better opportunity to network face-to-face, build lasting global relationships and catch up with colleagues.

## REGISTER YOUR INTEREST

PRESENTED BY:

TCCA

PLATINUM SPONSOR:

MOTOROLA SOLUTIONS

GOLD SPONSORS:

ERICSSON

# Negotiating new realities

Chair of TCCA's Legal and Regulatory Working Group (LRWG), **Nina Myren**, discusses the group's aims and activities

*Nina Myren*

**The LRWG focuses on the legal/regulatory issues related to the evolution from TETRA to mission-critical broadband. Why has the group been convened?**

The critical communications sector is moving towards broadband. The availability of standards, including test and certification schemes, is crucial.

In addition, there is a need for legal and regulatory frameworks that secure user needs during the system lifetime, in environments where market and technology change rapidly.

The existing regulations for the mobile communications sector were made before critical communications in commercial networks were discussed, and we see that there might be need for changes.

**What can governmental operators do together to shape the critical broadband market in order to deliver standardised and interoperable products?**

A working group where common issues can be discussed would help in establishing common ground and best practices, and to drive regulatory work with one common voice.

We will typically deliver white papers and model procurement texts. The latter will be proposed requirements to be included when purchasing equipment or services.

**How were the group objectives arrived at? What informed that process?**

The group has shared views on objectives, and it was clear early on that there is a need to work together on many complex topics. We started as a European group in order to have a common regulatory framework.

However, we experience that many topics are of interest for most government operators around the world.

One of the objectives of the group is to facilitate deeper engagement between government operators.

**Why is that necessary?**

Governmental operators are all facing similar challenges. We are all building mission-critical broadband networks and services for the first time.

Working together and learning from each other is important.

This is the approach that resulted in the success of the TETRA market, with stakeholders – including competitors – working together to build a viable ecosystem.

Our users need mission-critical solutions. It is for everyone's benefit that approaches to solving problems are harmonised, including legal and regulatory ones.

Technology development does not stop. We need to ensure that new regulations also take care of our users' needs.

**What are the intended outcomes? How does the group hope to influence the regulatory landscape?**

The most important outcome is to identify issues that we need to address. It is also important to develop a common voice to express required changes, procurement guidelines and best practices.

Other tasks for the group include following up relevant work at national ecom regulators (NRAs) and the Body of European Regulators for Electronic Communications (BEREC). Plus, proposing common strategies in order to secure the interests of the critical communications community.

**Can you give some examples of potential 'common strategies'?**

Our first deliveries are two documents. The first is the white paper published in October titled: 'Legal and Regulatory aspects regarding the realisation of Quality of Service, Priority and Pre-emption (QPP) in commercial networks'. In Europe most operators of PPDR-broadband networks will cooperate with commercial network operators, to provide either full or partial PPDR services. This white paper discusses how the European regulation on net neutrality seems to affect public safety operators sharing networks with commercial mobile operators.

The second document will be the first in a series of model procurement text requirements. This will propose model text that network operators, government agencies, and end-user organisations should incorporate within procurement tenders, contracts, and grant guidance documents to identify the compliance requirement that equipment suppliers must meet. By copying and adapting this model text, a government agency establishes the legal basis that ensures 3GPP MCX adoption. This topic was actually first discussed in our Critical Communications Broadband Group [CCBG] and is a good example of the cooperation between TCCA working groups to achieve common goals.

*Nina Myren is a TCCA Board member, sponsored by DSB Norway.*

# CRITICAL COMMUNICATIONS TODAY

The global information resource for mission-critical communications

***Critical Communications Today*** *is the only publication serving all aspects of the mission-critical wireless comms community.*

*Our reach is massive, with over*

**20,000**

*digital and printed copies.*

*Engage with industry professionals in more than*

**105**

*different countries.*


*Contact Jessica at* ***jessica.naranjo@markallengroup.com*** *if you want to take advantage of the exposure that we provide.*

REGISTER FOR YOUR ***FREE*** COPY TODAY

**www.criticalcomms.com**

# CC NETWORK

## THE NETWORK FOR LEADERS IN THE MISSION CRITICAL COMMUNICATIONS TECHNOLOGY INDUSTRY

**The Crit Comms Network is a 365 hub for leaders to:**

- **Share knowledge**
- **Demonstrate thought leadership**
- **Stay up to date with latest industry news**

Supported by the team behind Critical Communications Today and Critical Communications World, it provides a private, trusted space for global experts to exchange ideas all year round.


# REGISTER TODAY

**www.critcommsnetwork.com**