ROKE

5G & Law Enforcement

How it could impact investigation & crime prevention

We often hear people talk about 'the 5G network' as if it's a single network and a single technology. In reality, 5G describes the latest broad range of technologies that make up the fifth generation of cellular network standards. These standards are set by a range of organisations such as the 3rd Generation Partnership Project (3GPP) and the European Telecommunications Standards Institute (ETSI), among others.

5G's predecessors (4G and 3G) brought mobile internet to the masses, making high quality video and faster browsing speeds the norm.

5G itself is now being rolled out in the UK, and promises to be superfast (up to 10 times faster than 4G). It also uses technology that's far more advanced than current mobile networks and will allow more devices to access mobile internet at the same time. This means it's likely to transform the way we interact with critical services, from energy, healthcare, transport and crucially, law enforcement.

As time goes on and more dedicated 5G infrastructure comes into use, policing is set to evolve. 5G offers extremely low latency, high reliability and much improved security and privacy. Given information is the lifeblood of policing, law enforcement agencies have to address the digital challenge, harnessing rich new sources of data and thus intelligence to risks to the public to better protect the communities they serve.

It's clear this will bring significant challenges and benefits to the ways in which law enforcement agencies operate.

5G New Radio (NR) & spectrum

Spectrum is the fuel for cellular networks, it's the radio waves that carry data from our mobile devices to cell towers, back into the network and onto the internet. In 5G, this spectrum is becoming even more important.

Many of the advancements in 5G NR make use of more spectrum, use existing spectrum more efficiently and provide operators with increased bandwidth. The use of higher frequencies often referred to as mmWave, frequencies typically above 24GHz, is of particular interest.

The mmWave spectrum allows operators to offer hugely improved download and upload speeds to their customers. These can easily reach above 2Gbps (2,000Mbps), whereas today's best 4G networks top out at about 100Mbps in real world scenarios.

However, as always, there are trade-offs. With higher frequencies comes reduced range. Where a 2G cell (typically operating at <1GHz) may easily have a range of 10s of kilometres, a 5G cell operating at 26GHz may have a range of less than 200 metres in an urban environment. This means that operators need to deploy significantly more cells in order to deliver coverage to their customers. In early deployments, we're seeing on average between 30 and 50 mmWave cells per km^2. A benefit of all of these cells operating with small ranges is that it becomes much easier to identify the location of devices using the network.

For law enforcement, one of the key tools in finding vulnerable missing persons is knowing which cell their phone is or was last connected to. This allows

ROKE

investigators to understand at least the rough area they are or were in. With the deployment of mmWave cells, these areas of potentially 100s of km^2 can become more defined areas of square metres, allowing more accuracy in the search for the missing person, including the identification of buildings of interest. In future 5G releases there are even plans to enable centimetre accuracy for device locations, although in reality this will likely be limited to specific and niche use cases.

With all of this new spectrum there comes a potential new challenge around the use of Radio Frequency (RF) surveys. Much of the equipment used today cannot operate at these higher frequencies and is expensive to buy, maintain and upgrade. For law enforcement, the use of software defined RF survey equipment may help to overcome some of these challenges as the equipment's software can simply be updated as new spectrum gets used by network operators.

New technologies such as multi-user multiple-input and multiple-output (MIMO) and beamforming alter the way that cells operate, no longer covering a static area but changing as users come and go from that cell.

It may, however, become difficult to understand the true RF environment in a location, as it will never be the same at any two points in time.

Network Function Virtualisation (NFV) & cloud-native cores

NGC is where most of the new and interesting developments are taking place, after all this is where most of the work happens within a cellular network. Network Function Virtualisation (NFV) for example has introduced completely new ways of thinking about how networks are built and operated, leading to network functions being largely instantiated in software rather than bespoke hardware.

The technology means networks can be easily run on generic servers and other commodity hardware, making it a lot cheaper and simpler to build and upgrade software as technology develops. In the future it may even be possible to run much of a core network in the cloud for certain functions, using a cloud provider such as Amazon Web Services (AWS) given that there's no specialist hardware required. The term 'cloud-native core' is now beginning to develop and this means that core network functions are being developed specifically to be run in this new way, in the cloud.

This virtualisation also allows for much easier scaling of the network as traffic increases and decreases through the day and during special events. Modern development and integration methodologies such as DevOps and Continuous Integration and Continuous Delivery (CICD) can be adopted by vendors and network operators when the functions are virtualised.

This has a number of implications for law enforcement. It could lead to a rapid potential pace of change, something the law enforcement community already struggles with in some areas. The IT infrastructure industry is an excellent example of a successful pace of change due to network development. It's now not uncommon to see software being updated on at least a weekly basis with sometimes even daily developments. Here much of the testing and integration is entirely automated.

One of the other benefits of virtualisation for network operators is that it begins to remove the need to have large and expensive dedicated centres for housing physical equipment due to its new home on the cloud. This does however, present some potentially major concerns for law enforcement and policy makers, because as networks move to cloud infrastructure it becomes increasingly difficult, even impossible in some areas, to know where data is being processed and stored leaving questions around jurisdiction and the potential to lose control of sensitive data.

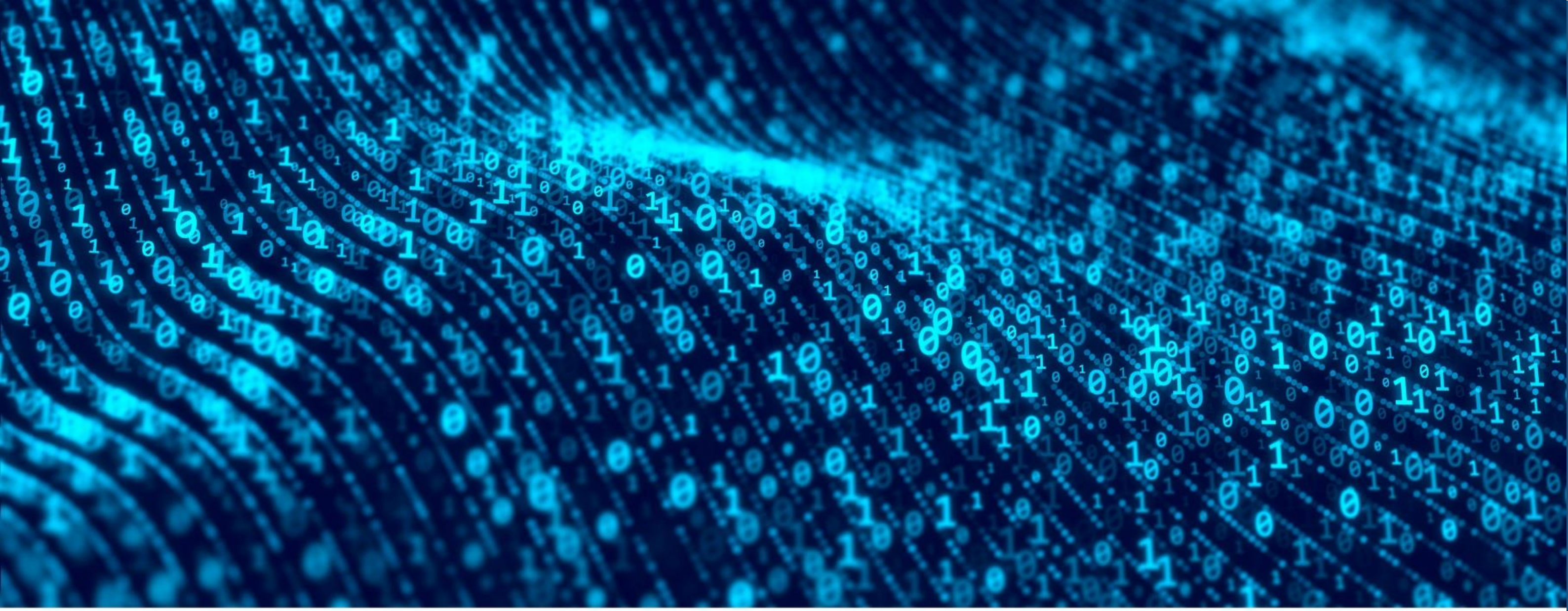
Edge Computing & Network Slicing

In the core network there are a range of other interesting technologies in development such as Edge Computing and Network Slicing. There's often lots of discussion about the potential of these and caution around the extent to which these will have an impact. Edge Computing is a distributed computing paradigm which brings computation and data storage closer to the location where it's needed, improving response times and saving bandwidth. It can currently only be placed internally of where the network encryption terminates i.e. where the encryption from the users device gets taken off so that the network can see and act on the data. For example, in a scenario where Edge Computing is present at a cell tower or in a street cabinet, the crypto would have to terminate there too, something that many network operators would unlikely be comfortable with due to security and privacy concerns.

Other solutions are also in development whereby devices communicate with each other directly, making use of Edge Computing to enable this. In this scenario, data will remain encrypted between the devices and never enter the central elements of the networks. **For law enforcement** this presents some obvious challenges with data never being seen by a network operator and therefore not being currently available.

Network Slicing is an architecture that enables the multiplexing of virtualised and independent logical networks on the same physical network infrastructure. Each network slice is an isolated end-to-end network tailored to fulfil diverse requirements requested by a particular application. It often brings up discussions of there being potentially thousands of slices in a network for all sorts of different applications and use cases. In reality, there are likely to be just a few slices; one for general consumers, one for IoT, and one for critical applications. This may still present some **challenges to the law enforcement community** around the fragmentation of data and the potential for some data to be unavailable in certain situations.

The benefits and challenges will continue to develop as 5G technology evolves. At Roke, we're at the forefront of the 5G journey, using our capabilities to research for and advise our clients on the best way to understand, eliminate and manage remaining security risks sensibly.



ROKE

We believe in improving the world through innovation. We do it by bringing the physical and digital together in ways that revolutionise industries.

That's why we've fostered an environment where some of the world's finest minds have the freedom, support and trust to succeed.

Roke is a team of curious and deeply technical engineers dedicated to safely unlocking the economic and societal potential of connected real-world assets. Our 60 year heritage and deep knowledge in sensors, communications, cyber and AI means our people are uniquely placed to combine and apply these technologies in ways that keep people safe whilst unlocking value. For our clients, we're a trusted partner that welcomes any problem confident that our consulting, research, innovation and product development will help them revolutionise and improve their world.

If you're bringing the physical and digital worlds together, we'd love to talk.

Roke Manor Research Ltd
Romsey, Hampshire, SO51 0ZN, UK
T: +44 (0)1794 833000
info@roke.co.uk www.roke.co.uk