PROTECTING THE PUBLIC

Chris Mason *reveals the importance of improved connectivity and a reliable network to keeping people safe at large gatherings*

No matter the circumstance, protecting the public is the number one priority, and emergency response teams across the globe need the highest-quality equipment available to achieve optimum results. In today's climate, much of that equipment relies on connectivity, particularly surveillance equipment. Real-time, reliable, full coverage surveillance is crucial for keeping the public safe, particularly at large-scale events. However, for spontaneous and sporadic events, current infrastructure may not support the capacity the emergency services require. For cases such as these, a wireless infrastructure must be deployed rapidly to provide public safety organisations with the connectivity they need to protect the public, personnel and even property, when and where they need it.

With so much to focus on keeping the public safe, for first responders and emergency response teams, reliable communication should not be a concern. A typical example of the sort of event that needs this extra coverage is a royal wedding, where hundreds of thousands of visitors and guests come together to catch a glimpse of the couple. The area needs to be securely monitored with footage available at multiple surveillance points and delivered in real-time; in high definition to keep the public and royal family safe.

During events like a royal wedding the whole area needs to be securely monitored

There are several challenges to overcome when providing connectivity during public safety operations. Constant visibility is essential for protecting people. The benefits of this enhanced visibility range from providing first responders with a clear picture of the situation they are about to encounter; to providing greater safety during public events by enabling officers to control crowds and manage traffic effectively.

Indeed, providing secure, reliable, anytime connectivity is a challenge in many such environments. For example, blind spots can be created by dense infrastructure, and connectivity speeds can reduce with network congestion. For unforeseen incidents, in particular, deploying a reliable network quickly can be hugely problematic.

LINES OF COMMUNICATION

When protecting the public, emergency services often have to deal with an array of different communication technologies, each used for specific tasks, which increases the potential for incompatible equipment. This can lead to organisations being unable to receive real-time data. All areas must also have adequate bandwidth to access data such as on-scene video, aerial imagery, maps and images, and many existing public safety networks do not have that capacity.

Alongside infrastructure challenges, the network also needs to comply with the requests of Government security, law enforcement, first responders and citizens. This inevitably includes budgetary constraints, which are always a consideration when planning and implementing networks.

To provide optimum public safety, high-quality wireless infrastructure is needed to prevent limited or fragmented connectivity between mobile personnel and vehicles, which can create severe and possibly life-threatening gaps in situational awareness. Despite any potential challenges, it is evident that public safety organisations cannot afford to compromise when it comes to security.

Whether it is a royal wedding, a concert or simply a carnival, visibility is crucial for policing operations to achieve situational awareness. Emergency services have taken advantage of developments in technology to ensure they have a high degree of visibility. An example of this can be seen during the Coronavirus pandemic as some countries introduced drones and ground-based robots to monitor cities and enforce social distancing regulations.

Indeed, commercial use of drones for tasks like surveillance and aerial photography/videography has increased in recent years, but they are not without their challenges. To support the use of drones, a mission-critical wireless network must be deployed easily and quickly to provide the necessary level of security.

Even industrial drones are based on simplistic computing architectures that were not designed to be highly secure, much like the Internet of Things (IoT) devices, making them vulnerable to even average-calibre hackers. These hackers can use standard debug tools to circumvent the software and hack the drone to control it, preventing it from completing its crucial tasks.

If the drone is running on an inadequately secured wireless network, the hacked drone can cause network interference, which could have detrimental effects on emergency service operations. Equally, the drones would be collecting and storing highly sensitive data locally. If the drone crashes and the information is unencrypted, anyone can access the memory element inside it and view this data. Additionally, it can be hacked to see what data it is collecting or what tasks it is performing.

The emergency services deal with a vast amount of private information and cannot afford for this to be publicised. Making sure the network is secure is crucial for the security of any event, so equipment can be used without any potential risk.

During events having connectivity and real-time situational awareness is crucial to optimise the deployment of security or emergency response resources. When it comes to monitoring high-profile events, police teams need constant visuals, which means having constant connectivity. Equally, fire and rescue teams also rely on visuals, and bomb squads and HAZMAT teams require connectivity to operate robotics that disarm and dispose of hazardous packages or materials.

HAVING COMPLETE VISIBILITY OFFERS THE OPPORTUNITY TO PREVENT ISSUES BEFORE THEY START

Private networks offer reliable, intelligent and secure wireless broadband connectivity to provide the flexible connectivity that public safety organisations need. Rajant's wireless network can seamlessly integrate with existing communications infrastructure or can be deployed where no infrastructure yet exists to support the highly varied users and needs of these organisations.

Transmission of security and surveillance monitoring data can be achieved with high throughput and low latency across the network. This brings public safety workers the visibility they need to identify potential threats and issues early. In emergencies where anything can happen, having this connectivity is crucial to ensure public safety organisations can respond immediately.

Furthermore, deployment can be achieved swiftly as it does not require a team of network engineers. Once configured, Rajant BreadCrumbs (radio nodes) are turned on, and automatically begin communicating with other nodes in the area, autonomously and without human intervention. Reducing set up and maintenance times allows emergency services to focus on where they are needed most. Such a network can provide resilient emergency services operations by ensuring that there is no single point of failure throughout the system.

Royal weddings in the United Kingdom are a global event, with hundreds of thousands of people flooding to one location to celebrate the big day. With so many people, providing the necessary public safety and security arrangements is no easy feat. In 2018, the UK celebrated two such events: Prince Harry to Meghan Markle and Princess Eugenie to Jack Brooksbank, both in Windsor. It was crucial to have the right network in place to

ensure the safety of the couple and the public during such high-profile events.

The Thames Valley Police were tasked with providing supplementary CCTV coverage of both events. In the urban environment of Windsor, providing the resilience and range that was required would take more than was available on standard networks. A true mesh network was required to allow police and security services to perform at optimum levels.

REAL-TIME, RELIABLE, FULL COVERAGE SURVEILLANCE IS CRUCIAL FOR KEEPING THE PUBLIC SAFE

Rajant was selected as the Kinetic mesh provider and had less than a week to create a full-coverage network of specific areas before the ceremony of Prince Harry and Megan Markle. Rajant used its wealth of experience to ensure the public safety requirements were met quickly and securely for the authorities, rapidly deploying an extensive network of BreadCrumb nodes in three days, providing the high-speed, robust CCTV network the police needed to secure the area.

At both events, Rajant Kinetic Mesh seamlessly integrated with existing communications infrastructure at key locations, enabling large amounts of mission-critical video data to be delivered in real-time to provide the police and other security organisations with the needed visibility. Despite the challenges created by the winding streets of Windsor, every part of the route for the post-wedding processions by the royal couples was covered with CCTV by the Thames Valley Police.

The network utilised multiple high-bandwidth frequencies, which ensured that the massive amount of wireless output from broadcasters, other security organisations and the general public did not prevent transmission of the vital imagery. The imagery provided over the network was also several seconds ahead of the television broadcasters covering the event, ensuring that Thames Valley Police was always one step ahead.

COMPLETE VISIBILITY

The technology proved so successful that Thames Valley Police decided to work with Rajant again to support security at Royal Ascot, which attracts approximately 300,000 racing fans. Using the now-familiar Kinetic Mesh network, Thames Valley Police rapidly deployed and managed the network, providing coverage for CCTV in areas that were difficult to reach or not yet served by permanently installed networks.

For planned and unplanned events, reliable and full coverage connectivity can make a huge difference. Having complete visibility offers the opportunity to prevent issues before they even start. In environments that are fast moving and high risk, maintaining a level of connectivity that will allow for accessing and sending large amounts of data from any location and in real-time is a significant task. Furthermore, this connectivity needs to meet the requirements of stringent, public safety organisations and be installed quickly and effortlessly. For police, firefighters and emergency units, reliable connectivity is crucial for rapid, real-time response anytime, anywhere, to ensure the public remains safe ●

Chris Mason is Vice President of Sales – EMEA for Rajant and is responsible for sales and channel activities across the UK, Europe, Middle East and Africa. He has over 30 years of Information Communications Technology (ICT) experience, specifically in radio solutions.

When protecting the public, emergency services often have to deal with an array of different communication options