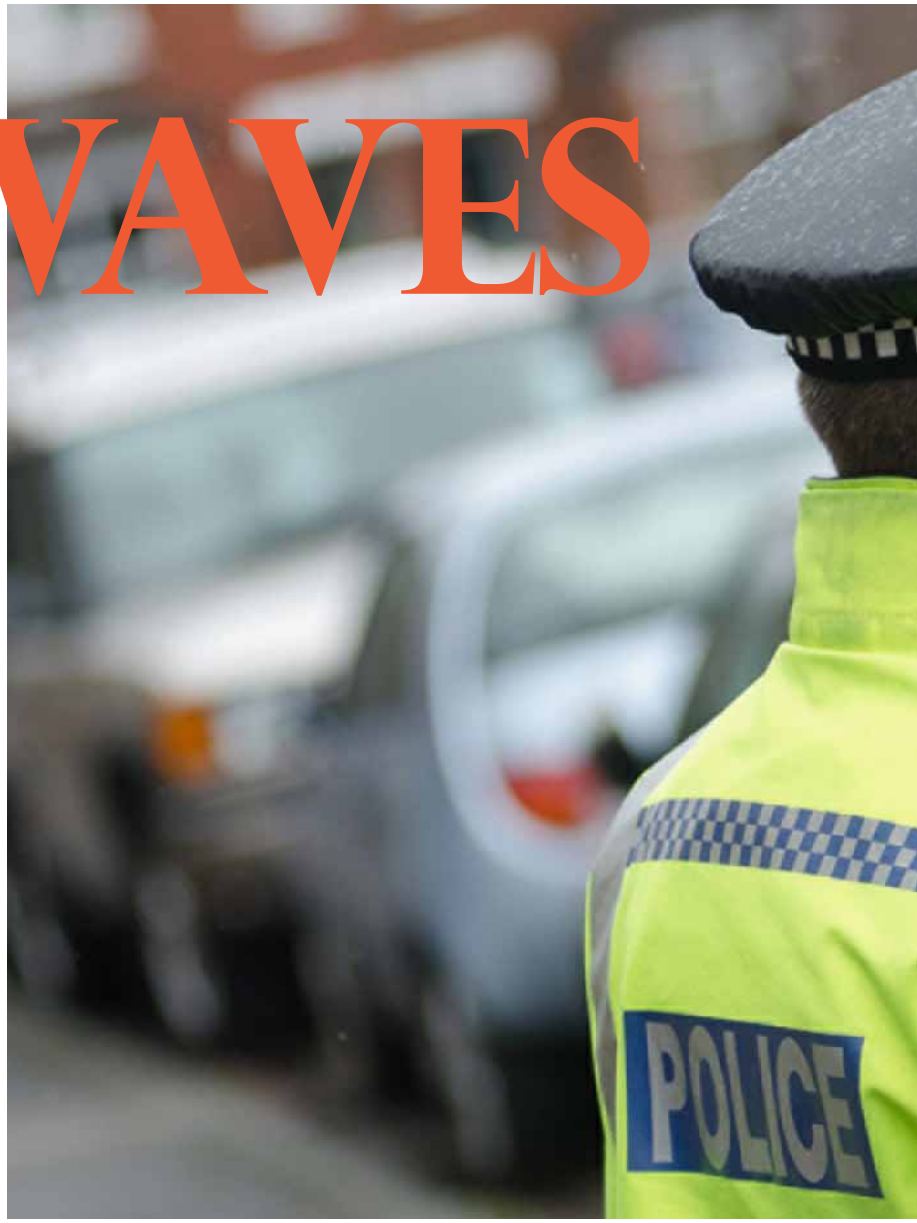
**Steve Pearson** assesses the communications systems available to the emergency services during major incidents and asks whether they can provide effective command and control

# ON THE AIRWAVES

At a recent meeting between this writer and Kevin Roberts, the Global CEO of Saatchi & Saatchi, he explained that, while he was at the Pentagon advising on how Brand USA can improve its global image, a three star general told him that we're living in a VUCA world. That is, a world that's volatile, a world of uncertainty, a world of complexity and a world of ambiguity. For the military and government, VUCA is a practical code for awareness and readiness, and this has never been more applicable than in the current climate. The world, in light of the terrorist threats from al-Qaeda, ISIS and other terrorist organisations, is probably more volatile than it has been for many years. Uncertainty as to where and when the threats will materialise is also at an all-time high. It is, therefore, up to countries both individually and collectively to ensure they are as prepared to face the threats as possible. By not doing so, they are leaving themselves open to terror attacks on unprecedented scales. The solutions are complex – far too complex for this article – and we will therefore focus on one important aspect of readiness to deal with major incidents should they arise: communications.

A major incident, by definition, is any emergency that requires the implementation of special arrangements by one or more of the emergency services, and will generally include the involvement – either directly or indirectly – of large numbers of people. Acts of terrorism, including those suspected of involving chemical, biological, radiological and nuclear (CBRN) devices, are subject to a specific multi-agency response supported by HM Government. Major incidents can, however, also come in the form of major air incidents, such as the devastating terrorist attack on 9/11, which by their very nature are sudden and catastrophic events, placing all organisations concerned with the response under intense pressure. The scale of such events means their effects often cross administrative boundaries and involve an extensive and lengthy recovery operation.

The common theme throughout all types of major incidents is the need for effective command and control, which requires effective communications between all those concerned, including the public as well as the agencies dealing with the incident. Most major incidents have four stages. These are: the initial response; the consolidation phase; the recovery phase; and the restoration of normality. It is therefore essential that throughout all of these phases effective communications exist. The communications requirement falls into two main categories: local area comms and wider area comms; these are achieved with a variety of equipment which will be highlighted later in the article.




©Airwave

***Effective command and control is essential for all major incident response, and cannot be achieved without reliable comms systems***

The emergency services and many other agencies, including the Coastguard and many London boroughs, have introduced TETRA-based Airwave with joint communications interoperability. These agencies are able to use common talkgroups to communicate while still maintaining the integrity of their own individual talkgroups. Access to talkgroups is not shared between different organisations, but there are several categories of shared communications talkgroups, such as Emergency Services (ES), Inter-Agency Talkgroups (IAT), Multi-Agency Mutual Aid (MAMA) and others. The Airwave network is an encrypted system and has a very high level of security. It cannot be decrypted by mass-market scanners and, to date, there is no known incident of an Airwave transmission having been intercepted and decrypted. To all intents and purposes it is a secure network. But scanners to intercept fax mobile telephony or unencrypted radio transmissions on other systems may well be used to intercept information transmitted between the services and agencies. This should be borne in mind when wording any transmission, including cellular telephone conversations, which may contain sensitive information.


Many local authorities have their own integral radio communications systems; these may not be compatible between boroughs or with the emergency services, however, and are not compatible with Airwave. All local authorities do also have emergency satellite phones.

Telecommunications is something we are all familiar with, and is a fundamental enabler underpinning the effective response to any emergency. Resilient communications are able to absorb or mitigate the effects of a disruptive challenge – that is, an event or circumstances that disrupts normal life, such as a terrorist incident. The High Integrity Telecommunications System (HITS) provides a resilient communications backbone between strategic co-ordination centres (SCCs) in police force areas across England and Wales, and central government crisis management facilities. The devolved administrations in Cardiff, Edinburgh and Belfast are also part of the HITS network. The system is delivered in partnership with Astrium and the Ministry of Defence (MoD), and is accredited to handle restricted voice and data communications. It is designed to remain available should all or part of the public switched telephone network (PSTN) be lost. This resilience is obtained through using a combination of a satellite pathway provided by the military SKYNET 5 constellation, which affords high availability levels, and landline connectivity independent of the commercial PSTN. Centres with this dual capability are known as hybrid sites – the great majority of HITS sites are hybrid.

Privilege access schemes will often form part of an organisation's arrangements to enhance the resilience of their telecommunications. But some of the current schemes, notably access to mobile public telecommunications infrastructures, have acquired a level of importance that far exceeds their utility. One such scheme is the Mobile Telephony Privileged Access Scheme (MTPAS), which was launched by the Civil Contingencies Secretariat (CCS) in September 2009. Like its forerunner, the ACCOLC scheme, it is intended to preserve access to mobile networks by those engaged in an emergency response when network capacity is under pressure. Public cellular mobile telephony has played an important part in enabling communications during the response to recent emergencies, but mobile networks can become overwhelmed by a high concentration of calls that often occur immediately after a major incident.

Privileged access is achieved by the installation of a special Subscriber Identity Module (Sim) card in the telephone handset. These special Sims are only available to entitled users within the responder community and not to members of the public. Privileged Access SIMs are provided by the networks to their customers without additional cost. Individual emergency service organisations should consult their own policy in relation to the numbers of MTPAS-enabled telephones they can obtain. As a guide, each organisation should take into consideration key posts to be supplied with MTPAS-enabled SIM cards. Eligibility is restricted to organisations that have a part to play in responding to, or recovering from, an emergency as defined in the Civil Contingencies Act 2004. Within an eligible organisation, MTPAS will only be available to staff designated as having an operational role at the scene of a major incident or emergency, or be required to directly support those with an operational role at the scene of an incident at a tactical or strategic level. The majority of organisations are sponsored on MTPAS by telecommunications sub groups (TSGs) which operate under the Local Resilience Forum (LRF) structure. The TSGs fully co-ordinate the scheme for their local resilience areas. Some responder organisations work on a national, rather than a local, basis, and these will be sponsored by central government departments.

Another, lesser-used service, which is readily available should it be required, is the Radio Amateurs Emergency Network (RAYNET). The idea of RAYNET came into being in the aftermath of the North Sea flood of 1953, a natural disaster that damaged the communication cables along the east coast of England on the night of 31 January 1953. With communication lines crippled, the police authorities, in desperation, sought help from the few amateur radio operators then licensed; although illegal at that time, the Home Office permitted the use of amateur

radios to direct and co-ordinate the rescue teams. The following year, an infant network first known as RAEN was formed. The Home Office conceded the desirability of an organisation which, in times of emergency, could effect the passing of messages facilitating the rescue operations of the professional services, who themselves lacked the "instant communications" of radio at the time. While RAEN began on a minor scale with only a few operators involved, the network has grown into a nationwide movement now known as "RAYNET".

Most of what we've looked at so far relates to inter-agency communications, but a key area which should not be omitted is communications with the public. This could be from a safety point of view to prevent and restrict the risk of danger to them, but also in the form of general information. The public need to know what is going on – otherwise mass panic and hysteria could develop, which won't help any situation. This information can be communicated by the media via TV and radio announcements, and via the Internet. The growth in social networking sites has meant that information about incidents and events is now more readily available. Speculation can quickly and erroneously become accepted as fact, and the needs of the emergency services to manage the information flow have never been greater. The public have a need to know how they will be affected by an incident and what actions they should take to minimise its impact. While the emergency response to an incident is often confined to the incident area, speculation and hysteria can rapidly affect a far wider area. Effective communication with the public about an incident will minimise its wider impacts and increase the confidence of the public in the emergency services. This involves identifying specific audiences and the appropriate communication tools and messages to achieve this.

Wireless public address systems can also be deployed in areas to make announcements in the streets. There are several available via WiFi networks, such as the ones supplied by Visiplex or the WiFi Bullhorn, but these lack resilience compared to rapidly deployable PA systems, such as those developed by Remvox, which operate via conventional GSM networks or MTPAS for a resilient privileged system and can be used in major incidents and emergencies to provide effective public command and control throughout the incident.

Effective communications for command and control have been developed over a number of years and have been tried and tested in several arenas which has helped to refine and improve upon what is currently in place. The VUCA world requires a need for constant evolution of processes, procedures and equipment. We can't stand still or we'll get caught out. Terror groups are getting more sophisticated in their tactics, equipment and operational capability, and we need to keep at least one step ahead. Communication locally, nationally and globally is paramount in enabling us to do this.


©Airwave

*Good to talk: the Airwave network offers first responders a very high level of security*

**Steve Pearson** is the Chief Executive of Remvox Global Communications Group based in Lancashire, England. He is a former British Army Officer with more than 20 years' experience in the security industry, and has several high tech patents to his name. He was awarded the Entrepreneur of the Year award for 2014.