Public Protection and Disaster Relief (PPDR) need for dedicated communications and why they cannot rely on public systems for mission critical communications

Input from UK, France, Netherlands for LEWP-RCEG + PT49

Contents

1 Introduction

In this document we present a study on one large event and two every day life situations which Public Protection and Disaster Relief organisations have to face. We also explain how the radio communication needs increase extremely quickly in case of an unpredictable crisis.

For the large event, we present a scenario based on the royal wedding that took place in London in 2011. This scenario aims at demonstrating public safety need for fast communications and why they cannot rely on public systems for mission communications. An analysis of the scenario is then provided.

For the everyday life scenarios, we took one from the perspective of law enforcement and another from the emergency and medical services. These scenarios are presented in the same format as those in the document "Public Safety Statement of Requirements for Communications and Interoperability" edited by the US Department of Homeland security.

Then, through a short analysis, we show what kind of networks will be able to ensure communications and why dedicated resources are necessary for public protection and disaster relief (PPDR).

Finally, we conclude that we need dedicated spectrum for public protection and disaster relief organisations in order to react to all kind of situations (every day life, big event and unpredictable crisis).

2 Operational situations descriptions

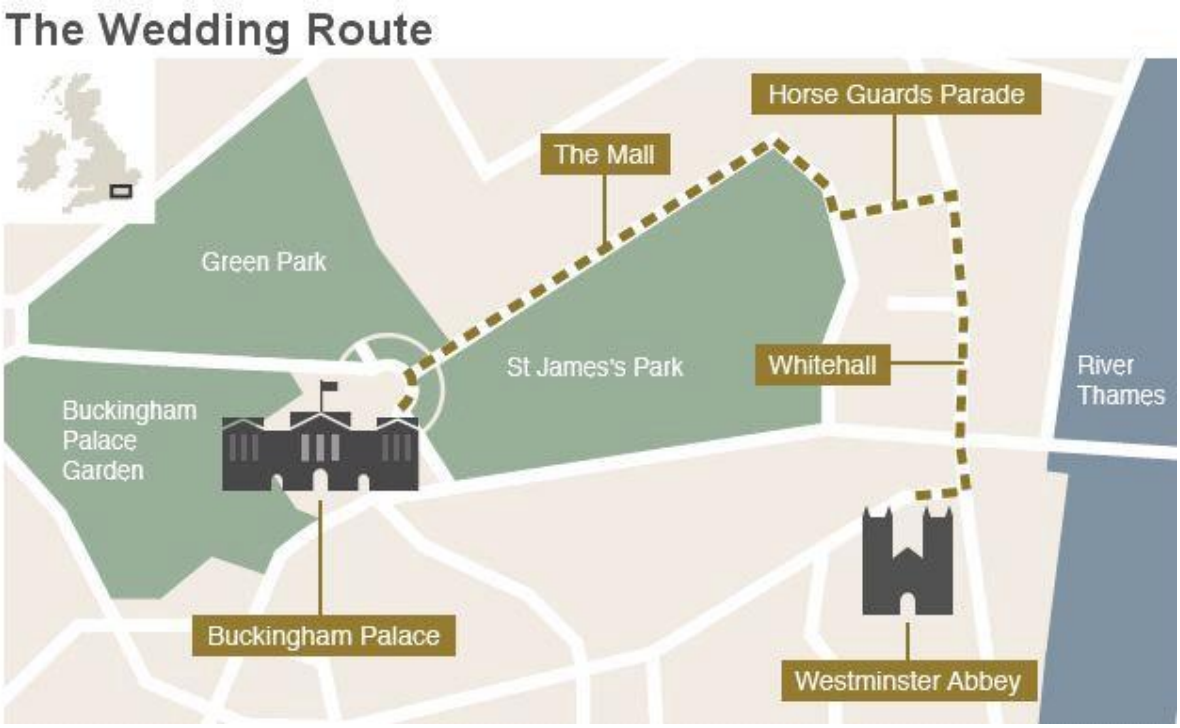
2.1 A royal wedding scenario

2.1.1 Introduction

Major security events take place frequently and the majority are peaceful and without serious incident. However, any event can rapidly change from peaceful to chaotic in seconds. Fast, clear communications are vital to maintain security and restore public safety quickly. The scenario is based around the 2011 Royal Wedding that took place in London, UK, 2011. The first part of this scenario deals with facts associated with the wedding to help provide context to the scenario and to illustrate the size and complexity of such operations. The second part illustrates what might have happened and how poor communications aided a terrorist attack. An analysis is provided at the end.

2.1.2 The Wedding – facts

1. The marriage of His Royal Highness Prince William, 2nd in line to the throne, to Kate Middleton took place on Friday 29th April 2011 at Westminster Abbey, London, UK.
2. A crowd of well-wishers estimated to be around 1 million lined the short wedding procession route between Westminster Abbey and Buckingham palace in order to get a glimpse of the couple.



3. As part of the £20 million security operation a "ring of steel" deploying 5000 police officers guarded the royal wedding route to protect the Royal family and other dignitaries invited to the ceremony. A combination of high profile uniformed policing including armed officers together with covert officers from a variety of agencies mingled with the crowds to prevent, detect and disrupt any attempt to attack the event. Marksmen took up position on roofs along the ceremonial route as search teams and sniffer dogs checked vulnerable locations. More than 80 VIPs were given close-protection bodyguards. There was no intelligence of a specific terrorism threat although the UK was on the second-highest alert to an attack from al-Qaeda and a substantial risk of a strike from dissident Irish republicans.
4. Mobile phone companies also prepared for the wedding in anticipation of high demand for their services. *"O2 and Vodafone both said they will install temporary mobile masts in St James' Park and Hyde Park. It is hoped the increased capacity will be sufficient to serve the hundreds of thousands expected to gather with smartphone in hand....Not only will people want to phone each other so they can meet up, but they will want to capture the event and share it with friends and family, so we expect to see a spike in demand as people upload photos to Facebook and check up on Twitter," its spokesman said. O2 said it had planned its royal wedding coverage using traffic statistics from the London Marathon and Notting Hill Carnival, which attracts more than a million revellers every year. Some 300,000 of its 28 million UK subscribers are expected to join the celebrations on Friday. According to the firm's estimates, as well as make a one minute phone call, they will send an average of at least four texts and one email via the 283 masts along the route."*[1]
5. From a security operation perspective, the Royal Wedding passed without major incident. A total of 55 arrests were made for a range of offences.
6. However, despite considerable additional capacity being made available in mobile communication networks, the commercial networks became congested. In one example[2], professional photographers complained of congestion on the mobile phone networks preventing them from sending pictures to their editors.

[1] http://www.telegraph.co.uk/news/uknews/royal-wedding/8474555/Royal-wedding-mobile-operators-upgrade-networks.html

[2] http://www.amateurphotographer.co.uk/news/Nikon_saves_royal_wedding_photographers_from_disaster_update_news_307282.html

All the above is based on fact. The mobile communication requirements for the police and related agencies were handled by a dedicated network. If the police, other security agencies and public safety organisations had been reliant on commercial networks then even a peaceful high security event would in this instance have become problematic. Consider the potential consequences in the following based around the wedding.

2.1.3 Royal Wedding – the need for fast reliable guaranteed communications

1. The Royal Wedding is a high profile high security event that will draw vast crowds eager to get a close look at His Royal Highness and Kate Middleton and to be part an historic occasion. Security operations however have to strike a balance between allowing the crowds to get close to and have sight of the couple against keeping the Royal family and over VIPs attending the ceremony safe from extremists.
2. The security optimised route planned for the royal procession varies from wide tree-lined roads to narrow streets overlooked by tall mainly office accommodation providing an opportunity for an attack by an assassin or terrorist seeking to capitalise from a high profile highly public event. London sees a number of high profile, high security events and the Royal Wedding presents the security organisations with no specific issues over those of other events. The policing/security operation of major events is well rehearsed and practiced.
3. On the day of the wedding the police and other security organisations have performed their last minute security checks and have reported back to control. The public are starting to pour into central London and seek out an advantageous position that will enable them to get a close look at the couple. Covert and overt teams have been deployed to mingle with the crowd and to look for suspicious activity. Trained firearms officers and observers are stationed at key roof-top vantage point along the route.
4. The Bride, Bridegroom, members of the Royal House Hold and other dignitaries safely arrive at Westminster Abbey where the Wedding ceremony is being held. A routine check of the communication links is performed; primarily voice, officer location information and a small number of medium resolution pictures from temporary cameras located at strategic points to monitor a number of previously identified security vulnerabilities that are difficult to cover by any other means. There is one radio-linked camera covertly located on the Wedding coach to provide a forward look capability and to help rapidly assess any situation as it develops. After the ceremony, the newly wedded couple and close members of the Royal household emerge from Abbey to an excited, loudly cheering flag waving crowd.
5. As the married couple start their journey in an open-topped horse-drawn coach to Buckingham Palace a few kilometres away, command alert officers of the progress of the cortege. The excited crowd, eager to get a look at the couple, use their camera phones to take pictures of this historic event as the carriage passes by. As the coach passes by and out of their view, many in the crowd eager to share their experience excitedly start to send their pictures directly to their friends and via their Face book accounts. Commercial networks are becoming increasingly congested despite the significant capacity increase to cater for the increased traffic and routine communications by the police, security services and other organisations are starting to become interrupted.

6. An armed surveillance officer on a roof top overlooking the wedding route 300m from the Abbey notices potentially suspicious activity towards the back of the crowd in front of him just as the horse-drawn carriage pulls away from Westminster Abbey. Despite his high vantage point, it is difficult to make out exactly what is happening as the activity is obscured by the depth of the crowd. The officer has to gather more intelligence on the situation before requesting the wedding coach is diverted and disrupt the occasion. He immediately advises control of the situation, requests a ground team is sent to investigate and requests control to zoom-in using a local line-connected camera. On his 2nd attempt he receives an acknowledgement that covert ground team Alpha 32 are 50m away, according to positional information regularly sent to control by the surveillance teams, and that they have been instructed to investigate. The video is patched through to Alpha 32, the roof top officer and senior commanders. It is still not possible to determine whether there is an imminent security threat at this stage due to the density of the crowd and the numerous flags being waved making it extremely difficult to see clearly what is happening.
7. Alpha 32 makes an urgent request for more information; the size, density and excited nature of the crowd are making it extremely difficult to identify the suspects who have few distinguishing features and are dressed in patriotic hats and T-shirts like many in the crowd. As a consequence of the way the suspects are blending into the background, Alpha 32 need a greater level of detail to ascertain their exact location. The high quality picture Alpha 32 expected from the roof top officer, as per procedure for high threat situations, has not been received. Neither has control received the picture so that a computerised facial recognition check can be conducted in parallel with the ground operation.
8. The wedding coach is now almost opposite the area where suspicious activity has been detected. The mobile communications sites near the roof-top officer are now permanently congested as the wedding coach approaches. Alpha 32 makes another call as no acknowledgement has been received. Yet another call is made as the seconds tick away and the carriage draws opposite to where the roof top officer is located. This time the call is received. The roof top officer acknowledges the situation and at the press of a button sends another picture of the suspects to Alpha 32. But again, the picture is not received.
9. Pictures from the wedding coach camera have permantly been intermittent as the coach is continuously under the coverage of congested cells and provides virtually no useful information. The roof top officer attempts to relay an enhanced description of the suspects' appearance and their new location as they have now diagonally pushed their way forward closer the barrier and 10m further away from the Abbey. And within 5m of another covert team, Alpha 33. But control are unaware as Alpha 33's location updates have not been received for a while due to network congestion. Alpha 33 are not aware of the unfolding situation as they communicate on a different talk group.

10. The armed Royal Protection Officer dressed as a footman and riding the wedding coach, is not aware of the situation developing in front of him as the numerous radio cells covering the passage of the newlywed's coach have been congested as the coach passes under them. If he had been aware of a potential security situation in front of the coach he would, without disruption to the ceremony, been able to take some precautionary action, as per procedure, that might have save the lives of the recently wedded couple.

2.1.4 Analysis

A trained assassin or terrorist is not normally distinguishable from others in a crowded situation. It is normally their behaviour that alerts security officials. In many cases however, what is seen as suspicious behaviour turns out to be unrelated to a security threat. A judgment between acting too soon and causing significant disruption and embarrassment to the proceedings and acting too late is a fine line. Intelligence delivered through fast quality communications are vital in such situations to help with the split-second decisions public safety and others security officials make daily. Commercial networks are geared to the consumer not the requirements of the minority public safety user and cannot provide the level of response needed.
In some instances, mobile signal jamming technology may be deployed to prevent the detonation of remotely triggered explosive devices. The USA presidential cavalcade is one example where it has been suggested such technology is routinely deployed. There are also a number of reports suggesting mobile signal jamming technology was deployed at Westminster Abbey for the Wedding[3] although other sources deny such action having been taken.

"Lost time is never found"[4].

[3] http://www.techweekeurope.co.uk/news/westminster-abbey-blocks-twitter-at-royal-wedding-27697

[4] Benjamin Franklin

2.2 Every day life scenarios

Both scenarios begin with some initial work at the start of the shift.
The system information in the control room must be updated (crew membership, which material and so on...).
Then the communication devices in the car/vehicle must also be updated (authentication, authorization, first exchanges with the voice dispatcher) .
In both scenarios, these updates are done wirelessly and are essential prior to operational deployment. The automatic data exchanges avoid heavy manual verifications.

2.2.1 EMS: Routine Patient Services

- Routine patient service

At 7 am, the paramedic team arrives at the patient's home. They use a camera and video transmission to communicate with a doctor and work under the direction of this doctor who is in the control room.
All the data concerning the patient is forwarded to the hospital by the network through air interface first. The patient is then taken to the clinic by an ambulance called by the control room.

- Response to car crash

At 8:40 the control room is informed of a car crash. They use the information provided by the people who called (speech, photo and video through public data networks). They also use information provided by the sensors in the car which has an access to the public network.
Emergency and medical services as well as police are dispatched immediately.
The crews are given the best route to reach the accident location through the mobile communications network and all information available about the car crash. An alert is also sent to place a helicopter on standby.
At 8:42 a paramedic is mobile on route to the car crash site. They arrive at 8:52. Considering the emergency they ask for the helicopter and an ambulance. Thanks to the images and the situation description (location), the helicopter can land with very little help from the "on-land" people.
The police also arrive and secure the area to ensure authorised personnel only enter the area. The police start to gather evidence to help establish exactly what happened.
The first patient is a 50 year old male driver, responding to voice, has no visible injuries and is complaining of shoulder pain. The paramedic uses several devices with radio interface (EKG, vital measurements etc..). The male patient profile is sent to the control room. The control room identifies the hospital the patient should be taken to. All data are automatically sent to the hospital, while, the name of the hospital is given to the ambulance. The male patient has a medallion providing more medical data. Through all the data the doctor in the control room make a diagnosis of a heart attack. The decision is made to take him to another hospital where specialist facilities exist. All data are transmitted to ambulance while some initial treatment is provided to stabilise the patient.
The second patient is female. The roof of the car has collapsed. She is unresponsive but breathing. She has an open head injury.
At 9:02 a heavy rescue vehicle arrives. The car roof is cut and removed.
At 9:12 a cardiologist from the hospital joins the incident group call (voice and video) and advice providing advice to the male patient in the ambulance.

The female patient is taken care of by the doctor. All medical data is sent to the control room to be put in the database. The medical crew monitors the female patient while she is transported in the helicopter.

Analysis :
Throughout the scenario, all information is electronic – there is no paperwork. All the information goes through the wireless interface and then to the network. This information contains geo-location data, medical data, all the voice and data for the control room to track and pilot the ambulances, helicopter, paramedic and medical teams on the field or in the control room or in external sites (hospital).
→ The choice can be made to have less doctors on the roads, thereby improving the efficiency of qualified employees. Specialist can always be asked for help through the fixed and mobile network.
In this scenario much information is critical, that is to say, the different crews would lack important information in case of a network crash. All the information exchanges between the control room and the crews on the field are essential and require dedicated resources to always be made even if public network has collapsed or is overloaded (31st of December, important crisis etc...)
→ Information arrives through the public network as emergency call. This traffic should be given the correct priority. But we consider the operations can be lead without this data.
We also notice the group calls should be configurable. That is to say the control room should be able to make experts enter the different calls as necessary.
→ The probability for this kind of event happening is highly dependent on the density of population. For instance in Paris at peak hour, there can be 200 to 400 fire brigades vehicles on different interventions.

2.2.2 Law Enforcement : Traffic stop scenario

While on routine traffic patrol, a police patrol containing 2 officers observe a car running through a red traffic light at an intersection. The patrol signals to the control room through predefined data message (even pressed by an alert button) that a pursuit is beginning. The camera in the patrol's vehicle begins recording the offending vehicle. The number of the plate of the offending vehicle is automatically sent to national database. The video is available for control room and authorized people connected through the police information system.
As a response to his database query, the police patrol is notified that the car is not stolen and information about the registered owner.
The offending vehicle stops. The video feed will be available on-demand to the dispatch centre, and forwarded in case of an emergency. Both of the policemen approach the car and note that there is only a driver. They request driver's license, but the driver does not provide the documentation.
While requesting the information from the driver, one of the officers observes what he believes to be the remains of marijuana cigarettes in the ashtray. He decides to search the suspect vehicle and contacts dispatch to request a backup unit. Though the automatic vehicle location system, the control room finds the closest unit and forwards them to the incident place. The information is also forwarded to the closest units for information only. A specific group call is created for the incident to share voice and data information. The second unit can access all the incident data (video and databases). The backup unit acknowledges that they go to the incident place.

The supervisor and backup unit bring up the real-time video of the event in the vehicle and control room and briefly observe the situation. All appears under control and they release the video link. The backup unit arrives on scene. The suspect is ordered to get out of the car. A white substance is found that appears to be cocaine. The suspect is put under arrest. A transport vehicle is dispatched by the control room following a request over the radio. The transport unit joins the group call (voice and data) to access the information.
After the arrest, one policeman takes the driver's biometric sample with a specific wireless device. After accessing a database the device returns name, photo and specific information about the driver. He has previously been arrested for drug possession.
The suspect is taken to jail by the transport unit.
After the suspect has left, the policemen take images of the car and the drugs. RFID tags are put on the different objects. All data concerning the car and the driver are then completed and sent by the officer: inventory form, tow report, jail booking form.
A tow truck is requested to impound the vehicle. All geo-location data are automatically sent to the tow truck.
After the car has been taken by the tow truck the first patrol ends his report and retransmits all useful data to the control room.
When the driver arrives at jail all data and forms are ready.

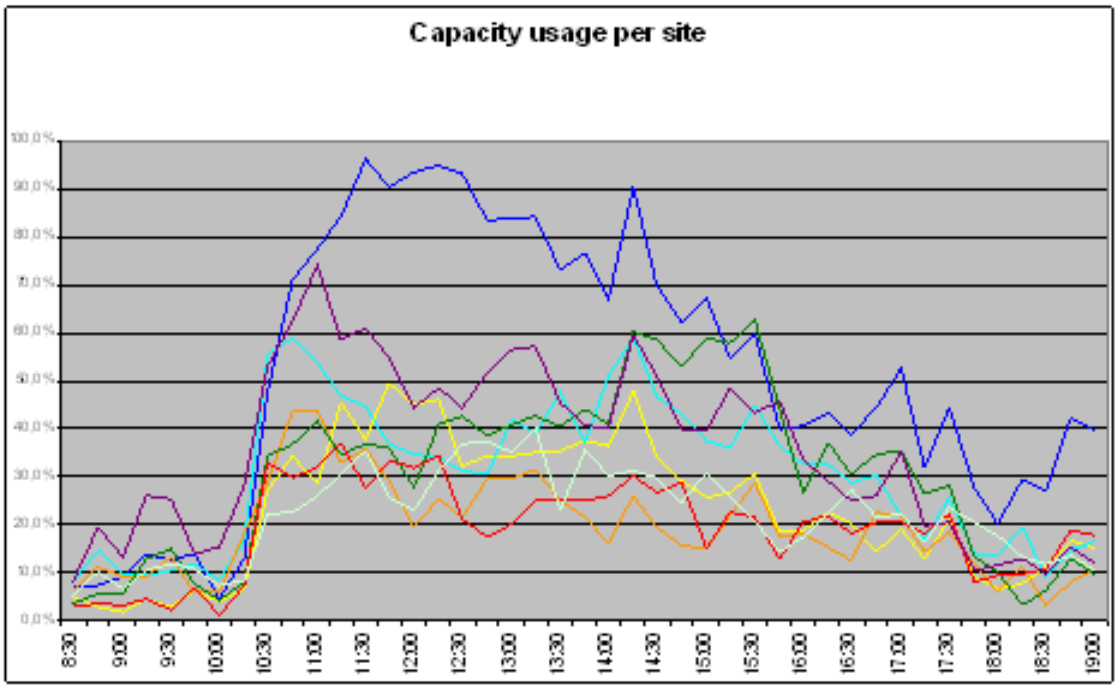
Analysis :

All the command and control data, the geo-location data, the call from the officer, the video seen by the backup officer are essential data to complete the mission. The availability of radio and network resources are essential for police officer even if nothing goes wrong.
In case of an emergency, the officer on the field should be able to transmit video. If there is no emergency it is important not to transmit to avoid overload of the network and disturbing the control room. The video is available on-demand to dispatchers and supervisors.
As a consequence we need resources for every day life as well as for major crisis or big events. These resources should always remain available even if public network are overloaded (big public events such as football matches or 31st of December). These resources should be oversized to face all possible events.

3 Unpredictable crisis

One scenario could also be written about a sudden and unpredictable crisis such as tempest, terrorist attack etc…
In those cases, all the public networks are overloaded or shutdown.
That's what happened in London in 2005 for instance. In such a situation, the communications of public safety is very quickly increasing and many lives can be saved with good coordination and as a consequence a well working communication system.

We present here a graphic of the increasing voice communication.
The diagram is from the plane crash at Schiphol in February 2009. We can see in the diagram below that resources are increasing extremely quickly, and to an extreme level, within half an hour after the crash.



Tomorrow we will need high speed data and video transmission to make medical diagnosis from the control room to send video to control room or on the field.
Indeed, in case of crisis, people will need to work with the same communication materials as in their every day life. This is essential to their reactivity.
Let us remind in the following images the kind of situations PPDR organisations have to face.

What is mission critical?
In PT49 it was asked to give a definition.
In the LEWP-RCEG meeting of 23rd March the RCEG made the following draft, which will be presented to LEWP:

'Mission critical operations' for PPDR organisations address situations where human life and goods (rescue operations, law enforcement) and other values for society are at risk, especially when time is a vital factor.

- ***This means we define 'mission critical information' as the vital information for PPDR to succeed with the operation.***
- ***'Mission critical communication solutions' therefore means that PPDR needs secure, reliable and available communication and as a consequence cannot afford the risk of having failures in their individual and group communication (e.g. voice and data or video transmissions).***

4 Overall conclusion

All the scenarios and examples we presented above in this document and the increasing resource used during a crisis, show that communications are essential for public safety.

States are responsible for the infrastructure they provide to face all kind of situation. Among these infrastructures, communication networks are more and more critical and need to remain available in any cases. Reserving specific infrastructure and specific spectrum allows public protection and disaster relief (PPDR) organisations to face crisis situations when public networks are overloaded, shut down or inoperative (what significantly happened in several crisis and events through the past ten years).

Furthermore, for one part of PPDR organisations (military, near military or fire brigades for example….) radio communications are tightly joined to the operation. That is to say, when an operation is done, the firemen or policemen rely on their communications and need not to rely on other people (private society) to be able to communicate. They have specific procedures they have accurately trained for and they must remain independent.

We can now conclude that, in order to prepare and face all the situations, PPDR organisations need to define and manage their networks in terms of radio coverage, capacity, quality of service, and ad-hoc deployments.
Some organisations will define high level services with high and specific constraints, others will own and operate their infrastructure, but in all cases they will need a free radio spectrum.
That is why we need to develop specific infrastructures and obtain from regulators a reasonable amount of spectrum which is always available. In every place, enough spectrum should be made available for PPDR organisations. That is the harmonisation challenge.