



**Use Cases for Cognitive Applications in Public Safety  
Communications Systems**

**Volume 1: Review of the 7 July Bombing of the London  
Underground**

**Approved 8 November 2007**

**SDRF-07-P-0019-V1.0.0**

## **ACKNOWLEDGEMENTS**

This document was drafted by the Public Safety Special Interest Group of the SDR Forum. In addition, the document was reviewed by members of the National Institute of Justice Communications Technology Working Group, and by representatives of the Intelligent Transportation System United Kingdom who also have experience in law enforcement and incident command. Their contributions were significant and gratefully appreciated.

## TABLE OF CONTENTS

1.	Introduction.....	1
1.1.	The SDR Forum Public Safety Special Interest Group .....	1
1.2.	Document Overview .....	2
2.	Background and Assumptions .....	3
2.1.	Cognitive Radio Technology .....	3
2.2.	Assumptions.....	5
3.	Methodology .....	7
3.1.	Select Scenarios .....	7
3.2.	Develop Timeline.....	7
3.3.	Identify Use Case.....	8
3.4.	Analyze Use Case .....	8
3.5.	Review Results with Public Safety .....	10
4.	London Bombings of 7 July 2005.....	11
4.1.	Scenario Assumptions.....	11
4.2.	Scenario Timeline .....	12
4.3.	Cognitive Use Case Discussion .....	12
4.3.1.	Use Case 1: Network Extension for Coverage and Reachback .....	12
4.3.2.	Use Case 2: Dynamically Access Additional Spectrum.....	17
4.3.3.	Use Case 3: Temporarily Reconfigure First Responder Communication Device Priorities .....	21
4.3.4.	Use Case 4: Interface to Non-First Responders .....	25
5.	Multi-Use Case Functional Capabilities .....	30
5.1.	Roles .....	30
5.2.	Command and Control.....	31
5.3.	Interoperability.....	34
5.4.	Restoring Default Configurations .....	34
5.5.	Security .....	35
5.5.1.	User and Role Authentication.....	35
5.5.2.	Device and Network Authentication.....	37
5.5.3.	Reconfiguration Controls.....	37
5.6.	Transition and Interface to Legacy System .....	37
5.7.	Interaction of Use Cases .....	38
5.8.	Standards.....	38
6.	Summary .....	40
	Appendix A: London Bombing Scenario .....	A-1

## LIST OF FIGURES

Figure 4-1. Map of the London Bombing Incident Locations .....	11
Figure 4-2. Network Coverage Extension Use Case Example .....	14

## LIST OF TABLES

Table 1. Possible Dynamic Prioritization Approaches .....	24
Table 2. London Bombing July 7, 2005 Timeline of Events.....	A-1

## EXECUTIVE SUMMARY

This report is the first in a planned series of reports to be written by the SDR Forum to develop concepts for the application of cognitive radio technology to enhance the communications capabilities of public safety first responders. The objective of this series is to provide:

- **Researchers and system developers** with an understanding of the desired cognitive capabilities, from which technical requirements and specifications can be derived;
- **Regulatory agencies** with an understanding of the regulatory issues and identification of potential changes that may be required to fully utilize evolving cognitive radio technology to benefit public safety; and
- **Public safety agencies** with an understanding of the potential value of cognitive radio technology and an understanding of policy and procedural changes that may be required to fully utilize evolving cognitive radio technology and regulatory changes.

The methodology for developing cognitive use cases is based on an analysis of response to actual or hypothesized events. This report is an analysis of the events of 7 July 2005, a terrorist attack involving coordinated explosions of bombs in and around the London Underground. This analysis is not an evaluation of that response, but instead uses the lessons learned from real events and the observed response to envision how evolving cognitive technology could enhance the ability of responders in the future to communicate more effectively and efficiently than available technology allowed.

Based on the analysis, we conclude that development of cognitive capabilities has potential to dramatically increase the ability of incident commanders. Four examples of how cognitive radio technology could be utilized in such situations (defined as cognitive use cases) are identified and described in this report:

1. Network extension for coverage and reachback.
2. Dynamic access of spectrum.
3. Dynamic prioritization.
4. Dynamic network configuration to include non-first responders.

The cognitive radio functional capabilities, regulatory implications, and policy and procedure implications for each use case are analyzed as well. Beyond capabilities associated with specific use cases, additional capabilities that apply to all of these use cases are also identified. This report was originally drafted by the Public Safety Special Interest Group within the SDR Forum, which includes representatives of public safety agencies, manufacturers, research & development organizations, and regulators. The report then underwent additional review and comment by public safety practitioners in both the United States and the United Kingdom.

Although there are significant technical, regulatory, and procedural developments required to realize the benefits, development of cognitive capabilities can dramatically increase the ability of incident commanders. First responders will be assured that critical information will flow as needed despite changes in coverage, connectivity, and loading on communications systems.

This page intentionally left blank.

## 1. INTRODUCTION

The maturing of software defined radio technology and evolving concepts of cognitive radios hold great promise for public safety communications. The Public Safety Special Interest Group (SIG) of the Software Defined Radio (SDR) Forum has already released a report summarizing potential applications of SDR and cognitive technology to public safety.<sup>1</sup> One of the key areas of interest defined in that report is cognitive applications.

This report is the first in a planned series of reports to be written by the SDR Forum to develop concepts for the application of cognitive radio technology to enhance the communications capabilities of public safety first responders. The purpose of this series of documents is to explore in greater detail specific examples of how cognitive applications can be used in public safety communications networks to enhance communications capabilities.

The objectives of the Public Safety SIG in generating this series of documents are as follows:

1. Provide **researchers and system developers** with an understanding of the desired cognitive and related functional capabilities, from which technical requirements and specifications can be derived;
2. Provide **regulatory agencies** with an understanding of the regulatory issues and identification of potential changes that may be required to fully utilize evolving cognitive radio technology to benefit public safety; and
3. Provide **public safety agencies** with an understanding of the potential value of cognitive radio technology and an understanding of policy and procedural changes that may be required to fully utilize evolving cognitive radio technology and regulatory changes.

### 1.1. The SDR Forum Public Safety Special Interest Group

The SDR Forum is an open, non-profit corporation dedicated to supporting the development, deployment, and use of open architectures for advanced wireless systems, with a mission to accelerate the proliferation of SDR technologies in wireless networks to support the needs of civil, commercial, and military market sectors. Activities focus on:

- Developing requirements and/or standards for SDR technologies, including working in liaison with other organizations to ensure that Forum recommendations are easily adapted to existing and evolving wireless systems;
- Cooperatively addressing the global regulatory environment;
- Providing a common ground to codify global developments;
- Serving as an industry meeting place.

The Public Safety Special Interest Group is one of several special interest groups within the Forum that bring together developers, users, regulators, and educators to address issues specific to the application of SDR technology to a particular domain or market area. Goals of the Public Safety SIG are to interface with the public safety community (including both users and vendors), to raise

---

<sup>1</sup> SDR Forum, *Software Defined Radio Technology for Public Safety*, Software Defined Radio Forum Report SDRF-06-A-0001-0.0, 14 April 2006, available at [www.sdrforum.org](http://www.sdrforum.org).

awareness of SDR, to publicize the activities of the Forum in addressing those issues, and to increase participation of the public safety community in the SDR Forum. The Public Safety SIG also interacts with other committees and working groups within the Forum to provide the public safety community's inputs into the publications and initiatives undertaken by the Forum. In the case of this report, members of the SDR Forum Security and Cognitive Radio Working Groups have participated in the preparation of this report. The Public Safety SIG is a unique venue, because participation in the SIG has historically included public safety organizations, land mobile radio vendors, manufacturers of SDR for military applications, software developers, researchers, and regulators.

## **1.2. Document Overview**

The methodology for developing cognitive use cases is based on analysis of response to actual or hypothesized events. This report is an analysis of the events of 7 July 2005, a terrorist attack involving coordinated explosions of bombs in and around the London Underground. This analysis is not an evaluation of that response. Rather, it is an attempt to use the lessons learned from real events and a real response to envision how evolving cognitive technology could enhance the ability of responders in the future to communicate more effectively and efficiently than current technology allows.

The background and assumptions of our analysis is provided in Section 2. In Section 3, we provide an overview of the methodology to be used throughout this series of documents. Identification and analysis of specific use cases is included in Section 4. Section 5 includes a discussion of issues that apply to multiple use cases. A summary is provided in Section 6, and a timeline of the events of the London Bombing Scenario is presented in Appendix A.



## 2. BACKGROUND AND ASSUMPTIONS

As noted in the Introductory Section, the potential value of cognitive capabilities for public safety has already been identified. In the Report on Software Defined Radio Technology for Public Safety<sup>2</sup>, and based on subsequent work, the following potential observations were made on the role of cognitive radio capabilities for public safety:

1. The first responder can better focus on the incident/threat by eliminating radio operations ranging from routine to complex through the use of cognitive radio applications to:
  - a. Be aware of its RF environment (e.g., vicinity of public safety incident);
  - b. Detect available and authorized RF resources;
  - c. Decide how to best operate within the existing infrastructure/network;
  - d. Use geolocation, spectrum, and network awareness to minimize interference;
  - e. Automatically reconfigure and connect; and
  - f. Learn how to perform these steps better the next time.
2. Cognitive radios offer a broad range of RF techniques to improve performance, interoperability, and efficiency.
3. Cognitive radio is becoming a significant concept for *all* future communications systems and devices for two fundamental reasons:
  - a. It enhances spectrum efficiency and improves access by making dynamic channel assignments, taking specialized measures to avoid harmful interference to others, and reducing unused channel seconds.
  - b. It enables “intelligent” self-configuring, auto-adapting systems and devices that can handle the growth trend of complex waveforms and user requirements.
4. Public Safety must carefully balance spectrum efficiency benefits against the critical need for system reliability, robustness, security, “instant on,” and other application-specific requirements of the first responder.

This report documents the initial efforts of the Public Safety SIG to follow up their report by exploring and analyzing the potential value of cognitive applications for public safety.

### 2.1. Cognitive Radio Technology

Cognitive radio technology (note definitions in the box that follows) is rapidly evolving as a significant driver of capabilities in new radio systems. Initial capabilities to adapt frequencies automatically to prevent interference to legacy radio systems was successfully field-demonstrated under the Defense Advanced Research Projects Agency (DARPA) XG radio program in August, 2006.<sup>3</sup> Demonstrations at the 2007 DySPAN Conference included real-time spectrum sensing/monitoring, secondary spectrum use by cooperating cognitive radios, policy engines, and

<sup>2</sup> Ibid., Section 4.3 Role of Cognitive Applications.

<sup>3</sup> Seeling, Frederick W., *A Description of the August 2006 XG Demonstrations at Fort A.P. Hill*, Proceedings of the IEEE Conference on Dynamic Spectrum Access Networks (DySPAN), April, 2007.

cognitive radio development platforms.<sup>4</sup> Such demonstrations indicate that these basic capabilities are achievable in the near term. We recognize that from these building blocks it will still be necessary to develop functional capabilities that not only work with existing radio systems but that are also proven under field conditions before such capabilities can be adopted for public safety use.

### Definitions

(from *SDRF Cognitive Radio Definitions*. SDR Forum Report SDRF-06-R-0011)

- **Radio:** (a) Technology for wirelessly transmitting or receiving electromagnetic radiation to facilitate transfer of information. (b) System or device incorporating technology as defined in (a). (c) A general term applied to the use of radio waves—from ITU-R Radio Regulations, Article 1 (Terms and Definitions, Section 1.4).
- **Software Defined Radio:** *Radio* in which some or all of the *physical layer* functions are *Software Defined*.
- **Software Defined:** Software defined refers to the use of software processing within the radio system or device to implement operating (but not control) functions.
- **Adaptive Radio:** Radio in which communications systems have a means of monitoring their own performance and a means of varying their own parameters by closed-loop action to improve their performance.
- **Cognitive Radio:**
  - a) *Radio* in which communication systems are aware of their environment and internal state and can make decisions about their radio operating behavior based on that information. The environmental information may or may not include location information related to communication systems.
  - b) *Radio* (as defined in a.) that utilizes *Software Defined Radio*, *Adaptive Radio*, and other technologies to automatically adjust its behavior or operations to achieve desired objectives
- **Cognitive Network:** A cognitive network is a network able to establish links between its *Cognitive Radio Nodes* to provide connectivity, and to adjust its connectivity to adapt to changes in topology, operating conditions, or user needs. A cognitive network consists of nodes that are cognitive radios. In such a network, the cognitive abilities of the radio nodes include awareness of the network environment, network state and topology, and shared awareness obtained by exchanging information with neighboring nodes or other network accessible information sources. Cognitive decision making considers this collective information and is performed in coordination and/or collaboration with other nodes.
- **Public safety:** the function of safeguarding the lives and property of the general population.
- **First responder:** an individual from a police department, fire department, emergency medical team, or other similar organization. His/her responsibilities when responding to an incident are to take necessary action to save lives, protect the welfare of others, and inform other personnel of any potential danger at the scene of an incident.

Often the terms “first responder,” “emergency services,” and “public safety” are used interchangeably. These terms generally refer to the same group of people and functions. We use the term “public safety” in this report, but in the International Telecommunication Union (ITU) and in many parts of the world, the phrase “public protection and disaster relief (PPDR)” is the agreed terminology. For convenience, we have used the term public safety consistently throughout the report, but the acronym “PPDR” could be substituted in all occurrences without changing the meaning of the text or the objectives of the report.

<sup>4</sup> A summary of each of the demonstrated capabilities is available at <http://www.ieee-dyspan.org/Demonstrations.html>.

We also recognize that there are major issues that must be addressed to realize the potential of cognitive radios. One of the challenges in dynamic spectrum access is the hidden node problem—assuming that a frequency can be utilized when in fact it is already in use by a transmitter or receiver “hidden” (electromagnetically) from the cognitive radio. Another important issue is that cognitive capabilities assume some level of reconfigurability of the radio which could have implications on the size, weight, and/or power requirements of a portable public safety radio. While not discounting the significance of these challenges, progress to date in this field suggests that they can be resolved to a level sufficient to realize the use cases outlined in this document.

## 2.2. Assumptions

The analysis of the scenarios in the remainder of this document, and the conclusions that are drawn in Section 6, are based on the following assumptions.

1. The focus of this document is on derivation of functional capabilities from identified use cases for enhanced communications capability. We recognize that the technology to realize these use cases is generally not available in current public safety radio systems. In fact, the capabilities envisioned in this document range from those that exist in some types of radios (but have not generally been implemented in public safety radios) to other capabilities that may require additional research & development. While attempting to be forward-looking we also limited the scope of capabilities to those that could be reasonably achieved with extensions of technology that is at least in the research stage.
2. As noted above, the capabilities defined in the use cases include technologies that have yet to be fully developed, and as such, the cost of implementing proposed capabilities is not addressed explicitly. The Public Safety SIG is concurrently developing cost models for analyzing the cost-benefit tradeoffs of proposed SDR and cognitive capabilities. These cost models, upon completion, can be applied to the functional capabilities identified in this document to support analysis of the cost implications and tradeoffs associated with implementation of the identified capabilities.
3. The proposed use cases are not limited by existing regulatory regimes. We have attempted to be realistic in what regulatory changes are feasible. But also, given a compelling use case for public safety, we assume that the regulatory community would consider appropriate changes to existing rules, so “feasibility” is not defined in terms of current thinking but rather in terms of the use cases defined in this document. Thus for each use case documented in this report, we also identify regulatory issues that may need to be addressed to enhance the ability of first responders to communicate more effectively than is currently available. We also note that regulatory perspectives differ by country and world region, and adoption of regulatory changes identified in this document will vary.
4. In general we use the term “cognitive capabilities” in this document to reinforce the concept that the cognition required to support public safety communications is not likely to fully reside in a single radio or device. More likely, the combination of capabilities to be aware of the environment, make decisions about how to enhance the performance of the communications capability, and the reconfiguration of the infrastructure and subscriber equipment to achieve performance enhancement, will be distributed in multiple nodes within the public safety communications systems.

5. Many of the circumstances that impacted response in the London bombing scenario have already been addressed through deployment of additional communications capabilities that do not involve cognitive capabilities. If all events are known a priori, non-cognitive solutions can be implemented to account for those events. However, major incidents and disasters are often characterized by circumstances that are beyond the scope of planning; in addition, fiscal realities preclude implementing contingencies for all possible situations. The real power of cognitive capabilities is to rapidly adjust to changes in the operating environment in order to maintain communications in the face of dynamic and often unanticipated circumstances. Thus we assume that the use cases discussed in this document are not specific cases that are optimally addressed by cognitive capabilities, but rather representative of a class of cases that can be *effectively* addressed by cognitive capabilities.
6. Communications in incident response are based on guidelines of appropriate multi-agency incident command and coordination, such as the Gold and Silver coordinating groups in London, and comparable incident command structures elsewhere, such as the National Incident Management System (NIMS) in the United States.
7. Scenarios assume non-cognitive legacy radios will continue to be used, and need to be considered in the solutions provided in the use cases. We assume that any implementation of cognitive radio capabilities will include capability to interoperate with legacy (non-cognitive) radios.
8. There may be the need to connect the public safety radio system with non-public safety radios such as commercial cellular networks. Part of the use case analysis addresses the technical capabilities required to ensure that the public safety radios/networks are not compromised by the inclusion of the non-public safety radios.

### 3. METHODOLOGY

The overall methodology is intended to establish use cases within the context of multiple scenarios based on actual or credible events relevant to public safety. Each scenario will be analyzed in detail to determine how cognitive radio capabilities could positively impact the communications of the public safety activity. The results of each individual scenario analysis will then be compiled to create a final analysis of the potential application of cognitive radios for public safety applications, along with the technical, regulatory, and procedural issues that must be considered and addressed to realize the enhanced communications capabilities.

In each scenario we analyze the events to derive use cases. This document includes analysis of the 7 July bombings in London. Subsequent reports in this series of documents will include analysis of other scenarios. The analysis of each scenario will follow a common approach:

- Develop a timeline of events in the scenario.
- Identify points in the timeline in which cognitive capabilities could enhance communications (the cognitive use cases).
- Analyze these use cases in terms of the technical, regulatory, and procedural issues that need to be addressed to achieve the enhanced communications.
- Review the use cases with public safety practitioners to ensure relevance and validity.

The remainder of this section describes this approach in more detail.

#### 3.1. Select Scenarios

The first step in the overall methodology is to identify scenarios for analysis. The scenarios must be sufficiently rich in activity to support analysis of a broad segment of use cases, with sufficient realism to maintain credibility with the stakeholders (in the case of the public safety community), and sufficient detail to allow derivation of relevant cognitive radio capabilities from the use cases. The initial scenario to be selected was the series of bombings that took place in London on July 7, 2005. It was selected based on the credibility of a real scenario and the extensive documentation in after action reports<sup>5</sup>. This scenario provided an excellent starting point, and highlighted certain areas for cognitive capabilities, but did not reflect the whole breadth of possible use cases. The additional scenarios may be either actual events or hypothetical scenarios developed for analysis and training purposes, and will be analyzed in a similar manner.

#### 3.2. Develop Timeline

The second step in the analysis is to establish a detailed timeline of scenario events. In the case of the London bombing scenario, the timeline was in place and detailed in the after action reports. In some places in the timeline we supplemented the existing documentation by postulating intermediate events or events that were implied but not articulated in the after action documentation as communications events.

---

<sup>5</sup> Greater London Authority, *Report of the 7 July Review Committee*, June 2006.

### 3.3. Identify Use Case

Having established the timeline, the next step is to identify those situations in which cognitive capabilities and dynamic spectrum access could have positively impacted the response(s) defined in the scenario. In analyzing the timelines, we consider the following types of questions to determine whether cognitive radios could enhance communications capabilities:

- Are there communications capabilities and links that are needed but do not exist?
- Are there communications capabilities and links that are established but need to be established in a more timely manner?
- Are there communications capabilities and links that are established in a timely manner whose performance needs to be improved?

By posing these questions in comparison with the timeline of events, we identify situations in which cognitive capabilities could enhance communications capabilities. The applications of cognitive capabilities in these situations are defined as cognitive use cases.

### 3.4. Analyze Use Case

For each identified use case, the next step is to analyze that use case with respect to:

- how it would impact the communications capability of the responders,
- how it would potentially impact the response scenario, and
- any potential negative impacts that could occur if the cognitive capability were part of the scenario.

We recognize that the use cases described in Section 4 require functional capabilities that are not necessarily available with current technology. (In fact, one of the purposes of this document is to provide input to the SDR Forum's Cognitive Radio Working Group to conduct a gap analysis to identify technology readiness needs.) As the focus of this document is on functional capabilities rather than available technologies, we deliberately attempted to place as few constraints as possible on technologies that would need to be deployed to realize the use cases. We considered capabilities that were realistic even if they would require future research and development to be implemented. However, the approach taken was to lay a foundation of capabilities and allow other researchers to assess the level of technological advancement required to realize the proposed capability.

Likewise, regulatory, policy, and procedural considerations did not constrain the identification of potential use cases. Regulatory and procedural implications and/or changes were noted in the analysis section.

In considering the use cases, we identify five aspects of the communications environment that are useful in framing key issues and challenges. Each of them may change over time.

1. **Physical:** This aspect is concerned with the physical world, including issues of geography, geometry, topography, proximity, density, RF propagation characteristics, and locale. What resources are where, and how can they get to where they are needed? How large is the area for which communications coverage is required? What is the geometric distribution of injured people, hospitals with capacity available, and transport to move them? How are

responders moving over time and how is the geographic layout of the responders changing over time (e.g., expanding a perimeter)? What are the facilities for recharging radios?

2. **Network:** This item deals with the technical issues of how information flows, both normally and in response to the emergency, and how failed systems are restored. How are radio systems structured, and how do they connect with other networks such as personal area networks, commercial systems such as the telephone network or WiFi/WiMAX capabilities? Is there a need for interoperability? How much bandwidth is needed? What Quality of Service is needed? What kinds of terminals are available? How do all the different agencies talk with each other and distribute data? Does the network use infrastructure, repeaters, direct peer to peer, or an ad hoc mesh? What authentication mechanisms are used in the network? What cryptographic algorithms support communications security? How are keys distributed? Can radio functionality be modified over the network, or is hands-on intervention needed?
3. **Procedural:** This issue deals with the role of people in the system, including authority, command, control, operating procedures, communications security procedures, and activation of contingency plans. Who develops contingency plans? Are there memoranda of understanding (MoU) in place to establish communications interoperability and ensure a chain of command is in place at the time of the incident? Who has command and control of the situation? Who authorizes individuals or groups to operate radios? What is the registration process for new communications devices requiring authentication? Who reviews requests for registration? How are cryptographic keys managed and what are the respective roles of humans and automation in key management? Who reprograms radios? Who assigns tasks and/or roles to individual units?
4. **Regulatory:** Regulators administer the use of spectrum, issue licenses for radio operation, resolve issues of interference, and make rules for radio operation. What modulation techniques and frequencies can be used? What are the rules for operation in unlicensed spectrum? How can extra spectrum be made available under emergency conditions? Are spectrum sharing agreements in place? What agencies have jurisdiction?
5. **Chronological:** Time is an overarching consideration that applies to all of the other aspects listed above. During the time before a specific event, there is time for establishing organizations, procuring equipment, recruiting and training personnel, building networks, defining policies and procedures, and development of contingency plans. When an event occurs, the first problem is awareness that something has happened, and learning enough to assess the situation. Then decisions are needed to determine the nature of the response, what resources to commit to it, and what actions to pursue. Operations continue until the emergency is resolved, and then the units involved stand down. After the event is over, an after-action review considers how well the operations were executed, and what can be done to improve preparedness for subsequent emergencies. A primary value of cognitive radio capabilities is to adapt to the changing environment much more rapidly than present systems.

### **3.5. Review Results with Public Safety**

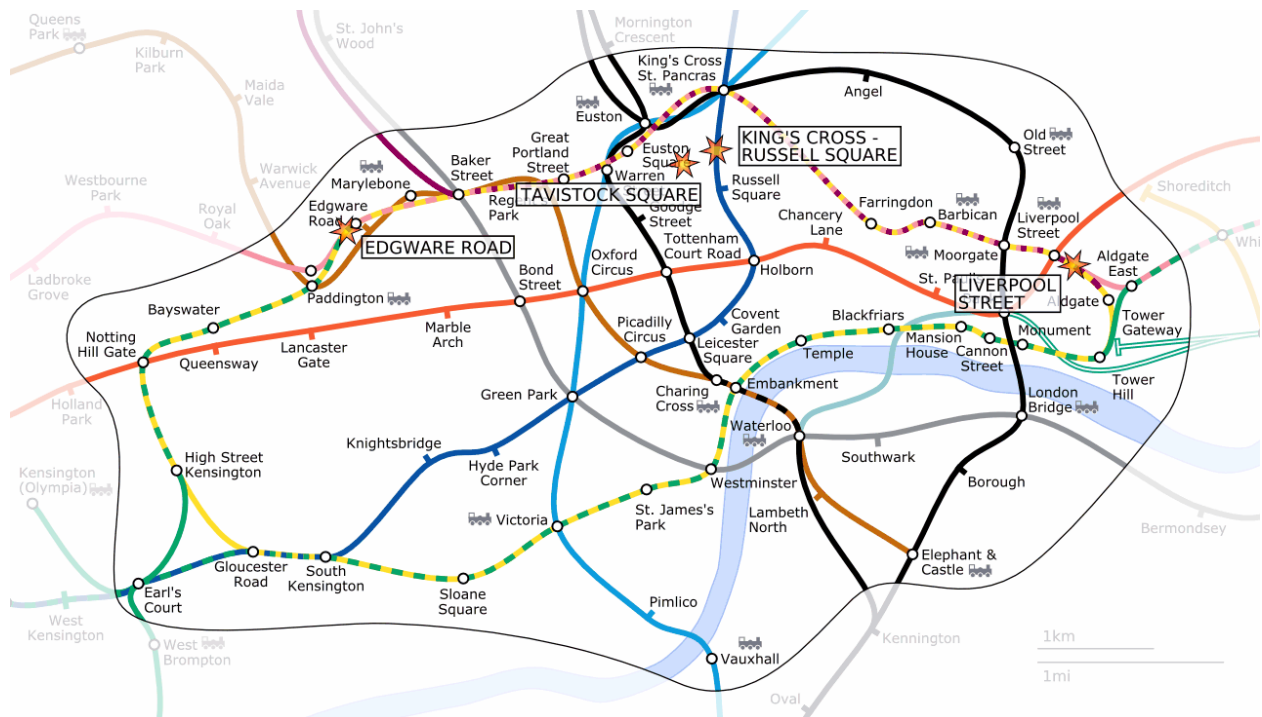
To ensure that the assumptions made concerning public safety incident response were valid, the analysis was reviewed by representatives of the public safety community. Comments were solicited and received from members of the National Institute of Justice (NIJ) Communications Technology Working Group and representatives of the ITS UK who also have experience in law enforcement and homeland security. Their comments were provided as individuals and not as official positions of their organizations, and were valuable contributions to the formation of this document. Their inputs provided valuable guidance and credibility for the analysis.



## 4. LONDON BOMBINGS OF 7 JULY 2005

“For hundreds of thousands of people commuting into London, the morning of July 7, 2005 began just like any other. But at the peak of the rush hour, bombs were detonated in three crowded subway trains and aboard a London bus. At least 52 people died, along with four bombers, and 700 were injured.”<sup>6</sup> As shown in Figure 4-1, the explosions were spread out across several incident sites, and as shown in the timeline in Appendix A, occurred over the course of an hour.

This event provides a real-world scenario that illustrates the significant challenges in responding to a terrorist event. As noted in the Report of the 7 July Review Committee,<sup>7</sup> the response was characterized by countless acts of heroism and compassion by first responders and ordinary citizens alike, and that both the communications and the command and control capabilities generally functioned as well as could be expected under the circumstances.<sup>8</sup> The purpose of this section is to use the sequence of events that occurred on that day and the communications that occurred as part of the response to identify circumstances in which future cognitive capabilities could provide more efficient and effective communications in similar situations.



**Figure 4-1. Map of the London Bombing Incident Locations**

### 4.1. Scenario Assumptions

Since this scenario is drawn from actual events, our only assumption is that the events unfolded as reconstructed in the after-action reports. In some cases we also assume the existence of communications not specifically identified in the after action reports but logically based on incident

<sup>6</sup> CNN, “Bombers Target London,” available at <http://www.cnn.com/SPECIALS/2005/london.bombing/>.

<sup>7</sup> Greater London Authority, *Report of the 7 July Review Committee*, June 2006.

<sup>8</sup> London Emergency Services Liaison Panel, “Major Incident Procedure Manual”, 6<sup>th</sup> edition, July 2004.

response and subsequent events (e.g., we assume units were dispatched to a scene if they arrived at the scene but the dispatch activity is not specifically noted).

## 4.2. Scenario Timeline

The timeline of the London bombing incident was derived from the after action reports and included as Appendix A. In the scenario there are a number of places in the timeline (use cases) where the Public Safety SIG identified potential applications for cognitive capabilities to improve the communications capability that existed at that time. In the timeline these events are shown with a yellow shaded cell in the table. Section 4.3 provides a detailed discussion of these use cases.

## 4.3. Cognitive Use Case Discussion

A number of potential cognitive use cases have been identified based on the scenario timeline as described in the preceding section. In this section, each use case is discussed in much greater detail. The use cases are ordered in descending priority based on operational relevance and feasibility as provided by the public safety practitioners who provided input to and feedback on the report.

### 4.3.1. Use Case 1: Network Extension for Coverage and Reachback

Cognitive radio capabilities could be used to automatically reconfigure radios to include a repeater capability to extend network coverage to areas where radios are otherwise cut off from their infrastructure, particularly during initial response to an incident prior to additional communications resources being deployed.

#### 4.3.1.1 *Summary of Scenario Situation*

In terms of the aspects of the public safety communications environment:

1. **Physical:** Bombs exploded on three London Underground trains inside tunnels with varying distances to the nearest station. Some passengers were severely wounded. There was no light. The only escape was by walking through the tunnel to the nearest station. Responders had to walk to the scene through the tunnel.

A number of different agencies, including Metropolitan Police, British Transport Police, the London Fire Brigade, and London Ambulance responded to the emergency by entering tunnels through the nearest station.

2. **Network:** Once police and fire responders went into the tunnels, their radios lost connectivity to the above-ground infrastructure. The only means for responders to communicate back to their respective command centers and any above ground personnel was to walk to the nearest station and position themselves at the entrance to the Metro system. Individual radios were not capable of exploiting peer-to-peer capabilities to provide network extension to connect isolated nodes to the network.
3. **Procedural:** Responders had adequate authority to communicate on their own networks, but as noted under Network were unable to do so. Procedures were established to maintain some flow of information by having responders communicate to (above ground) command

centers from the entrance to the tunnels, but that process required responders to walk from the scene to the entrance, which took as long as 15 minutes in some cases.

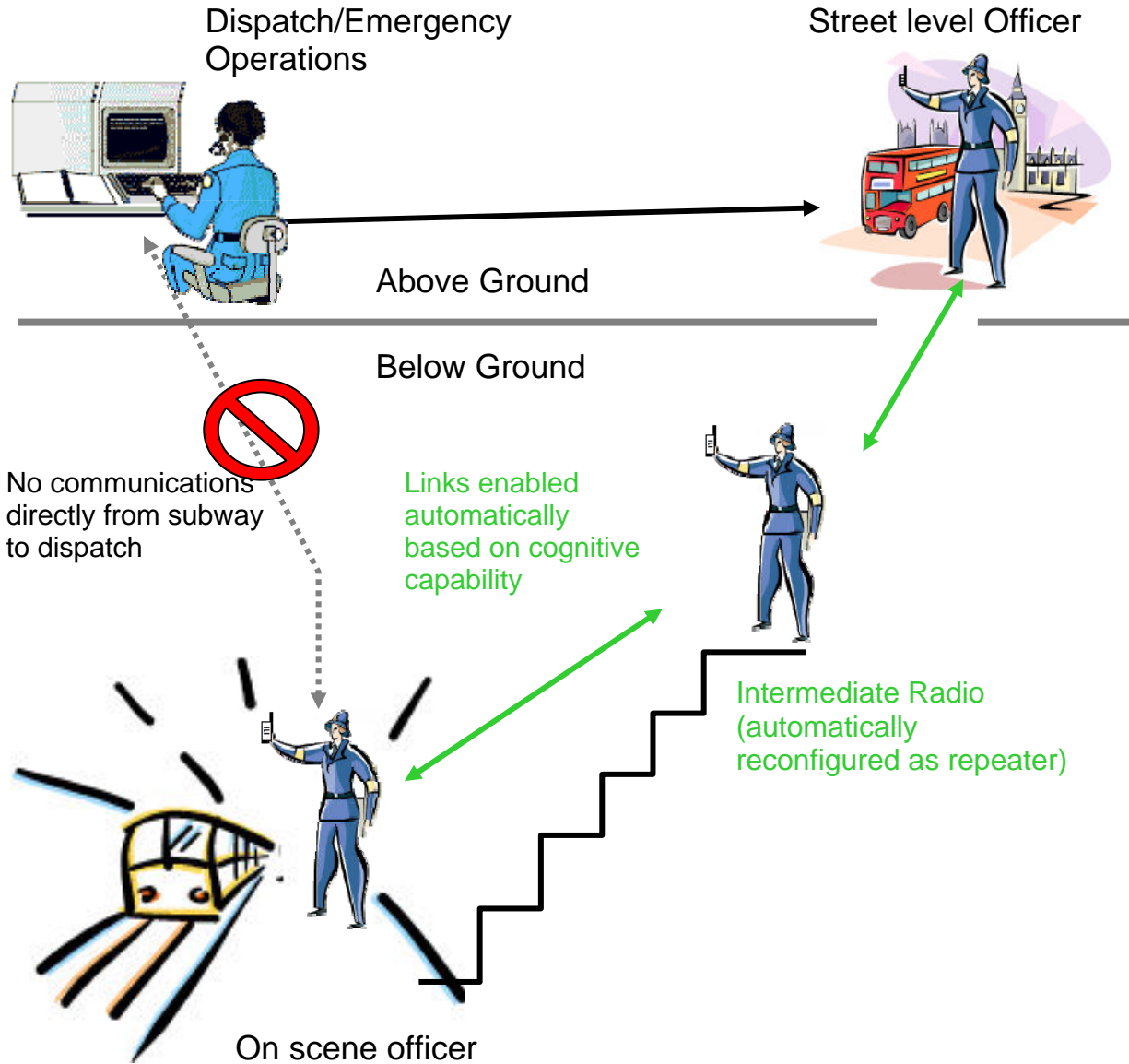
4. **Regulatory:** No regulatory issues were involved as the situation reflected an inability to communicate on licensed frequencies due to physical constraints.
5. **Chronological:** Prior planning had been performed, but infrastructure damage precluded the use of some communications capabilities that were in place and part of the plan.

The other critical chronological consideration is the amount of time (as much as 15 minutes) required to move information from the scene of the accident underground to the command centers.

#### 4.3.1.2 *Description of Use Case*

Cognitive radio technology could be implemented to reconfigure responders' radios to create an extension to the existing network. This network extension would allow transmissions to be passed back and forth from the incident site along a network of individual responder radios operating in peer-to-peer mode to a radio which can communicate with the main radio system/network. A radio would be positioned where it could maintain connectivity with the above-ground infrastructure (such as at an opening to the tunnel) and function as a repeater to bridge between the otherwise disconnected radios and the infrastructure. Depending on distribution of radios in the tunnels, additional radios could also be automatically reconfigured to act as repeaters among the disconnected radios.

The concept is illustrated in Figure 4-2. As shown, communications is enabled between personnel at the opening of the tunnel to dispatch and emergency management centers, but not from responders at the scene of the explosion in the tunnels. The concept of the network extension capability is reflected in the additional links that could be established automatically among responders otherwise cut off from communication with the above-ground system. This provides immediate restoration of communications for all users without requiring additional equipment at the scene.



**Figure 4-2. Network Coverage Extension Use Case Example**

The impact of these capabilities is that on-scene responders would have direct communications to command centers without leaving the incident scene or resorting to runners that delayed communications by as much as 15 minutes. With respect to the specific aspects of the scenario situation noted in Section 4.3.1.1, this use case would result in the following:

1. **Physical:** No change from the physical situation described above.
2. **Network:** Responders would maintain connectivity with their network at all times regardless of where they were located. (Note that it would be possible to achieve the same effect by deploying repeaters at strategic locations to create the necessary extension. However, the cognitive capability has significant advantages that justify this use case:
  - a. Cognitive capabilities and the ability to reconfigure radios would provide the network extension immediately, rather than after the period of time necessary to deploy repeaters.

- b. Cognitive capabilities would automatically determine appropriate network configuration. Repeaters would require manual determination of the repeater location, frequencies, and so on.
  - c. Cognitive capabilities would allow the network extension to accommodate the dynamics of the response, as users arrive and leave, as the physical location of the responders changes, and so on.
3. **Procedural:** In general the procedures normally used for communications among responders and between the responders and the above ground command centers would be followed in this situation. Additional procedures would be followed to position radios as needed to function as repeaters to ensure connectivity. However, unless the radios acting as repeaters have a full duplex capability, the responders must allow for a variable time lag for their message to be received and stored and then re-transmitted at each repeater and for an appropriate response back from the other party(ies) involved in the communications.
4. **Regulatory:** No significant regulatory change would be required as this capability assumes operation on existing licensed frequencies, however regulatory approval of operating mode changes would be required. See Section 4.3.1.4.
5. **Chronological:** The pre-planning would still be effective as network connectivity would be maintained despite infrastructure damage or the response by responders whose radio system was not normally extended into the tunnels. In addition, the timelines to move information from the scene to the command centers could be reduced from as much 15 minutes to a few seconds.

#### 4.3.1.3 Functional Capabilities

There are a number of functional capabilities assumed by this cognitive use case. First, the radios must be capable of being reconfigured to function as a network extension (e.g., the radios can operate on appropriate spectrum; the radios have reconfiguration algorithms, and so on). Second, there must be some level of cognitive capability for a collection of radios to “understand” that they have lost their ability to communicate with the system infrastructure. More specifically, radios must be capable of:

- Determining that they are disconnected from the system infrastructure;
- Finding and identifying peer radios;
- Identifying and authenticating reconfigurable compatible radios;
- Determining which radio/radios is/are within coverage of the infrastructure and which radios are not within the coverage of the infrastructure;
- Forming a satisfactory network extension route to the infrastructure from each affected radio using non-interfering frequencies for each “hop”;
- Adjusting the network as responders arrive and depart from the area where coverage is unavailable; and
- Preserving the level of security of the baseline network in the network extensions.
- Providing either full duplex (simultaneous receive and transmit) operation or including a “store and forward” capability for user voice and/or data communications.

There are a number of approaches that could be utilized to achieve the network extension, such as ad hoc or mesh networks. The feasibility of existing protocols to accomplish this is a relevant research topic.

#### *4.3.1.4 Regulatory Implications*

The proposed capability would rely on existing peer-to-peer modes of operation for which regulatory rules are already in place. Thus no major regulatory changes are required (although air interface could change from being used in simplex mode to semi-duplex or duplex mode.) However, it is possible that the spectrum and protocols required to implement such a capability would require the ability to utilize spectrum not routinely licensed to such users under current regulatory rules. Thus it may be necessary to consider allowing use of spectrum for such purposes. Part of the cognitive capability of identifying the disconnection from system infrastructure could be to ensure that spectrum used for peer-to-peer communication would not interfere with other users. In the case of the tunnel bombing, such interference would be unlikely because the area in question is generally cut off from most above-ground infrastructure. However, to generalize this use case to other situations in addition to the tunnel scenario, channel assignments should be made on approved frequencies.

#### *4.3.1.5 Policy Implications*

As noted above, the objective of this use case is to seamlessly restore lost connectivity of responders who have already been authorized and authenticated to use the network. Ideally responders would be unaware of the reconfiguration of radios, although an audio or visual alert should be included to indicate that the radio is following the network extension protocols. Policies governing use of the network (e.g., who may use the network, radio protocols, use of channel) would be the same for the network extension as when the radio is within range of the infrastructure.

Some procedures will need to be modified or added to reflect that some radio behavior, such as the rebroadcast of voice transmissions, may be evident to the responders because of response delays. Training will be generated to be appropriate so that users will be familiar with the differences in radio performance and behavior. In addition, training will be established for responders to understand the impact of physical location and how best to deploy, particularly if they were going to carry a radio that can be reconfigured as a repeater. Consideration should also be given to allowing individual first responders the option of excluding their radio from participating in the network (see discussion in Section 5.2).

Network management policies (e.g., machine readable policies) that govern the manner in which radios are reconfigured to achieve network extension will need to be implemented in advance to facilitate such operations. However the impact on usage behavior should be minimal.

Some training will also be needed to fully exploit such capabilities. For example, responders would need to understand how the radios respond when outside network coverage. Users should be familiar with performance aspects of the radios such as changes in delay times, capabilities and performance of the radio when acting as a repeater, the impact of physical location of the radios on network performance, and similar information.

Policies and procedures will need to be established for operation of radios that end up being used as repeaters. For example, a responder whose radio is used as a repeater may need to stay in a specific physical location and “man” the position to maintain the communication link, and may not be able to participate in other functions of the response. Agencies will need to consider the tradeoffs

of how to allocate responders accordingly. Procedures may also be established for responders “dropping off” radios as needed to allow the network extension to function (here again the issue is how best to allocate resources, with the radio and the responder being considered separate resources). Given the proposed capabilities of the radios, spare or cache radios which can be rapidly delivered to the scene may also be part of an incident response strategy.

#### **4.3.2. Use Case 2: Dynamically Access Additional Spectrum**

At several points in the scenario there were communications difficulties because of the sheer volume of calls on the voice communications networks. Dynamic spectrum access, or the ability for cognitive radios to identify unused or underutilized spectrum, could be a solution in this scenario and provide a means for expanding capacity when needed.

We understand that there are significant technical issues associated with implementation of this use case that are dependent on the technology used in the system infrastructure. The focus of this discussion is the overall desirability and benefit to public safety of being able to expand capacity in emergency situations in a timely manner.

Note, however, that most dynamic spectrum access approaches assume that the user is operating as a secondary user, and able to relocate to other spectrum as needed if a primary user utilizes the spectrum. This use case in this scenario would be significantly different—in an emergency situation, dynamic spectrum access for responders would be as a primary user—to specifically appropriate spectrum that is not being used, or can be appropriated for emergency use.

##### *4.3.2.1 Summary of Scenario Situation*

In terms of the aspects of public safety communications:

1. **Physical:** In the process of responding to the situation, the density of radios and access attempts overloaded some infrastructure elements in a specific geographic area. Key considerations include that the scenario took place in a densely populated urban area during a workday. In addition, multiple incident locations created demand for services that impacted the system as a whole.
2. **Network:** Based on the demand exceeding capacity, access control mechanisms (ACCOLC) were invoked in the area around Aldgate East to block access for some users, including first responders that did not have priority access.
3. **Procedural:** A significant decision process was executed to determine whether or not to invoke Access Overload Control (ACCOLC)<sup>9</sup> when the mobile phone system could not handle the number of attempted calls. Part of the decision process was assessment of the impact of ACCOLC on responders who were supporting the response but whose radios did not have priority.

---

<sup>9</sup> We recognize that the increasing deployment of Airwave (a dedicated public safety communications system) into the police and fire services is reducing the use of public networks by first responders, and therefore reducing the chances of a recurrence of the specific circumstances under which ACCOLC was invoked in this scenario. Nevertheless, this scenario highlights the general challenge of obtaining adequate capacity for first responder communications in an escalating event, for which dynamic spectrum access is an important use case for cognitive radio capabilities.

4. **Regulatory:** No regulatory procedures existed for dynamic allocation and use of spectrum outside the previously licensed frequencies.
5. **Chronological:** The ACCOLC decision process occurred as the response to the bombing events was unfolding.

#### 4.3.2.2 *Description of the Use Case*

This use case involves identifying and utilizing spectrum not normally utilized by the system—in this case the mobile phone system.

There are three different approaches that can be considered to realize this use case, as outlined (underlined) below:

Pre-defined agreement among organizations: One approach to dynamic spectrum access, taking advantage of reconfigurable radios/cell phones, is to establish agreements among organizations that would allow a non-licensed authorized user to utilize additional spectrum under defined circumstances and by mutual agreement. Implementation of this cognitive capability may be limited to the ability to identify the channel loading limits that would require accessing additional spectrum. The cognitive capability may also be used to manage network and subscriber reconfiguration to enhance the utilization of the allocated spectrum. There is a broad range of potential types of agreements under which spectrum could be dynamically accessed. The following is by no means conclusive but serves to provide a range of possibilities:

- Dynamic spectrum access that is triggered by a pre-defined event, such as reaching a capacity limit;
- Dynamic spectrum access that occurs when one organization requests access and the licensed organization grants it (e.g., spectrum mutual aid).
- Dynamic spectrum access granted to another user (spectrum leasing) or to a secondary user on a non-interfering basis.

Emergency declaration: Another approach to dynamic spectrum access, again requiring the ability to reconfigure radios/cell phones is to establish rules by which some spectrum (licensed for other services) is accessed for emergency response under a governmental declaration. Here again the cognitive capability may be limited to identifying the load circumstances under which access of additional spectrum is appropriate, or may be used to manage network and subscriber reconfiguration to enhance spectrum utilization.

Identify unused or underutilized spectrum not licensed to the network: Another approach to dynamic spectrum access is to monitor spectrum utilization in frequencies not licensed to the network, identify spectrum which is unused or underutilized (“white space”), and reconfigure the network and subscriber equipment to utilize that spectrum. Clearly this type of dynamic spectrum access would be limited to emergency situations and only be allowed under clearly defined circumstances (such as a governmental declaration). Cognitive capabilities would be required to identify available spectrum and to reconfigure the network and subscribers accordingly.

1. **Physical:** No change from the physical situation described above.
2. **Network:** In this scenario, the network congestion would be relieved by providing more spectrum for use by all network users including first responders. If the infrastructure has a cellular architecture, it may be possible to dynamically reallocate the channel distribution to



create additional capacity in the afflicted cells. Alternately, there may be a place in nearby spectrum where some other service can be pre-empted to satisfy the demand.

3. **Procedural:** There are a number of procedural decisions involved in implementing this use case. Key procedures include determining at what point to invoke dynamic spectrum access procedures, procedures for identifying spectrum that can be utilized, and when to release the bandwidth. The specific procedural implications are a function of the implementation approach. For example, this use case could be based on a fully automated determination of the need for additional spectrum and the spectrum to be utilized; in other implementations there may be a human in the decision loop, in which case the procedures for making such a decision must be defined. Also, different procedures may be appropriate depending on whether the additional spectrum is based on a pre-defined procedure or agreement, or whether additional spectrum is identified in real-time during the course of an incident.
4. **Regulatory:** The regulatory implications of dynamically accessing spectrum depend on the approach (as outlined above) that is used. Some pre-defined agreements among organizations may be feasible under existing regulatory rules, particularly if the spectrum is allocated under the same service rules or if the rules explicitly provide for secondary spectrum usage. Rules may require modification if the dynamically allocated spectrum is normally allocated under different service rules, or if there is no explicit allowance for such agreements to be put in place. In general the approach that allows spectrum to be accessed for emergency response is not embodied in existing regulations and would need to be added to allow this approach. Likewise, the ability to identify and access unused or underutilized spectrum not licensed to the network is not generally part of existing regulations. We recognize that these regulatory changes can involve sweeping changes to how spectrum is utilized in emergency situations, and that crafting rules which balance the needs of emergency response and other legitimate uses of spectrum during emergencies will require extensive research, development, and public discussion.
5. **Chronological:** This kind of Spectrum Sharing would require a significant amount of advanced detailed planning. Plans can have varying degrees of dynamic range. Switching from one fixed plan to another is easier than dynamic cognitive problem solving in real time, but more likely would result in less efficient spectrum utilization. Also note that relinquishing spectrum that has been utilized to facilitate emergency response must be done in a timely manner to have value greater than present systems.

#### 4.3.2.3 *Functional Capabilities*

Dynamic spectrum access implies a number of functional capabilities, as described below.

- The network must be able to identify capacity loading that meets whatever criteria are in place to initiate the dynamic spectrum access.
- The network must be capable of identifying spectrum resources that can be utilized to offload some calls. There are two possible approaches to identifying additional spectrum.
  - First, there may be established agreements in place that under certain circumstances spectrum normally used for one purpose is made available to support communications networks being utilized in an emergency. Such identification could be based on established agreements among spectrum

“owners” or based on allocation of spectrum for emergency use in the event of a certain level of emergency.

- Alternatively, cognitive capabilities to search for underutilized spectrum (“white space”) that could be dynamically accessed. Note that in this case a scheme must be implemented to manage the hidden node problem. Also, the network must be able to support the ability to deconflict the situation if multiple users attempt to access the same available spectrum “white space”.
- The network infrastructure must be able to reconfigure to use the new spectrum. If the system is a trunked system, the network must be able to incorporate additional frequency options into the system. Network transmitters and receivers must be able to be reconfigured to utilize the additional spectrum. If the additional spectrum is based on a pre-defined agreement, frequencies may be pre-programmed, in which case only an execution command is required to access the additional spectrum.
- Subscriber equipment must be able to reconfigure to use the new spectrum, i.e., must be able to transmit and receive on the additional frequencies.
- Reconfiguration information must be communicated among the radios and the network infrastructure to coordinate the utilization of additional spectrum.
- Dynamic access of spectrum must be consistent with the regulatory requirements of that spectrum (e.g., in terms of bandwidth, out of band emissions, power management, location based rules) to ensure that other users in that service are not adversely impacted by use of a specific frequency.

#### 4.3.2.4 *Regulatory Implications*

The regulatory implications of this use case depend largely on the manner in which spectrum is dynamically accessed.

Approaches based on pre-defined agreements among organizations that allow users to utilize spectrum in emergency situations may require regulatory approval to allow secondary use (secondary markets, leased spectrum, etc.) of spectrum by non-licensed users.

One potential regulatory change is to allocate spectrum for first responder use that is otherwise allocated for other non-public safety use during normal conditions (e.g., executive declaration of an emergency automatically dynamically allocates certain commercial use spectrum for emergency responder utilization).

Use of licensed spectrum without pre-arrangements is generally not allowed and would require changes to existing regulations. Use of unlicensed spectrum is generally allowable, although regulatory changes could recognize public safety priority use of unlicensed spectrum in emergency situations (just as drivers yield the right of way to emergency vehicles with lights and sirens).

#### 4.3.2.5 *Policy Implications*

There are a number of policy implications for this use case. Key questions include:

- What are the circumstances under which spectrum can be allocated as described above?
- Who has the authority under which a decision to utilize non-licensed spectrum is made?
- What is the interaction of priority services and dynamically allocated spectrum?

- When and how is dynamically allocated spectrum released?

#### **4.3.3. Use Case 3: Temporarily Reconfigure First Responder Communication Device Priorities**

Cognitive radios (in this case, referring to cell phones) might be able to be temporarily reconfigured with higher priorities based on the circumstances of the emergency responder.

##### *4.3.3.1 Summary of Scenario Situation*

In terms of the aspects of public safety communications:

1. **Physical:** In the process of responding to the situation, the density of radios and access attempts overloaded some infrastructure elements in a specific geographic area.
2. **Network:** Mobile phone network resources were being utilized by public users as well as first responders.
3. **Procedural:** A significant decision process was executed to determine whether or not to invoke Access Overload Control (ACCOLC) when the mobile phone system could not handle the number of attempted calls. Part of the decision process was assessment of the impact of ACCOLC on responders who were supporting the response but whose radios did not have priority.
4. **Regulatory:** No regulatory issues were involved.
5. **Chronological:** The ACCOLC decision process occurred as the response to the bombing events was unfolding.

##### *4.3.3.2 Description of the Use Case*

The dynamic prioritization use case exploits cognitive capabilities to adjust the priorities of responders based on the ongoing communications activity as well as the dynamics of incident response. Priority schemes are implemented in today's public safety and commercial cellular systems. The application of cognitive capabilities provides the opportunity to adjust those priorities to accommodate unanticipated priorities or to manage priority access in real-time.

One of the sources of motivation for this use case comes from one of the major issues that arose in the London bombing scenario. The high demand for cellular calls motivated the Gold Coordinating Group to consider activating the Access Overload Control (ACCOLC) to deny access to the system for any device that did not have the required priority access. One of the considerations in the decision of the Gold Coordinating Group not to invoke ACCOLC was concern that the key responders might not be carrying phones that would allow access were ACCOLC to be invoked.

While the after action reports cited issues surrounding the deliberation to invoke ACCOLC on the day of the bombing, our analysis led to consideration of another use for cognitive capabilities: dynamic priorities. In a crisis situation, as demands for system resources rise, it may become necessary to manage access to the system based on the relative importance of the user and the communication being transmitted. The concept of the use case is to be able to change those priorities in real-time as an event unfolds. In the case of emergency responders using a commercial cell phone network, priority access may be public safety users getting priority access over

commercial users in the event of emergency situations. For example, in land mobile radio systems, “man down” alarms get priority over other communications.

While there are differences in typical use of cell phones for incident response between the United Kingdom and locations in other regions such as the United States, this use case is still generally applicable. It is not uncommon for first responders and incident command staff to use cell phones for non-mission critical communications. While not mission-critical, there may still be significant benefit in managing the priorities of such users. Furthermore, although not the focus of this particular discussion, the entire concept of dynamic prioritization based on responder role can be applied to land mobile radio systems as well. Trunking systems today have prioritization capabilities, but they are statically defined.

The role of cognitive capabilities here is in the ability to adjust in real time those priorities based on the unfolding events of the incident, communications resources demands and availability, and the changing roles of individual responders over the course of an event. In the case of the London bombing scenario, a capability that would have enabled responders who did not have ACCOLC-enabled devices (cell phones) would be to have devices reconfigured over-the-air and in real time. This could have eliminated the risk of responders being denied access to the system in the event that ACCOLC was invoked. These cognitive capabilities could provide more sophisticated and dynamic access management for radio/cellular systems.

The scenario situation would be described as follows:

1. **Physical:** No change from the physical situation described above.
2. **Network:** First responders would be assigned a priority based on their role in support of the response. Priority modifications would be downloaded to the first responders’ mobile phones as needed. In addition, cognitive capabilities in the network management would recognize the increasing load level and congestion levels and block access to lower priority calls as needed. User mobile phones would also have a cognitive capability that indicates that user access has been blocked so that the system loading is not made worse by persistent access attempts.
3. **Procedural:** As discussed in Section 4.3.2.3, there are several approaches to deploying this cognitive use case. Appropriate procedures will be needed, and depend on what particular approach is followed. For example, if individual responders are allowed to change (or request to change) their priority, policies and procedures need to be defined to govern the circumstances and steps to be followed by responders. Likewise, policies and procedures for any request approvals or assignment of priorities as described in the following section will be required.
4. **Regulatory:** Mechanisms for over the air reprovisioning of mobile phones may require regulatory modifications.
5. **Chronological:** Policy and procedures would need to be addressed as part of system planning. During an incident, invocation of access controls would take place upon activation of a set of trigger conditions. When demand no longer exceeds capacity, then the access control mechanisms can be removed, although the normal feedback loop stability criteria must be observed to avoid an on-off-on-off pathology.

#### 4.3.3.3 *Functional Capabilities*

A number of capabilities must be available in order to realize this cognitive use case. First, there must be a mechanism to determine those first responders who have a legitimate need to have priority access to the communications network. Access to the network itself has already been established, i.e., the network has already recognized and authenticated the first responder's cell phone (responder's device). The required capability is to establish that the circumstances of that particular user warrant a level of priority greater than the priority level currently granted to the responder's device.

The definition and assignment of priorities can incorporate a number of different elements of incident response and management. For example, priority assignments could be based on:

- The roles within the response that have been assigned to the individual responder's device;
- Physical location of the responder's device;
- Service of the responder's device (e.g., EMS priority over law enforcement);
- Type of data being communicated;
- Role of the user in the communications process.

There is a potentially broad range of complexity and sophistication of the cognitive capabilities implied by this use case. At the simplest level, assuming that priorities can be dynamically modified, radios could be reconfigured either by the individual responder or manually by a network operator without utilizing any cognitive capability. However, manually determining priorities for individual radios is not very practical for large scale incidents. Relatively simple cognitive capabilities<sup>10</sup> could be implemented to associate priorities with responder assignments, physical location, and/or service. More sophisticated cognitive capabilities could assign priorities automatically based on a variety of parameters associated with the communications of the response, or even in a predictive mode to anticipate, rather than react to, the dynamic needs of the responders.

The advantage of role based priorities (supplemented by other ad hoc assignable methods) is that preplanning can determine the appropriate priorities for each role in a variety of situations of varying complexity. Cognitive capabilities might be able to assess the level of complexity involved and select a suitable priority. All of this is supplemented by the user controlled methods delineated as follows.

One approach to considering the different functional capabilities for handling priority assignments is to consider that there are three possibilities for requesting changes in priority—the responder, some central authority (e.g., incident command, incident communications leader), and the communication network itself. Note that in the case of the communications network, the actual functionality could be distributed between the subscriber unit and the network infrastructure, but the request or the authorization is made automatically without human initiative. Each of these entities may also authorize the requested priority change. This leads to nine possible approaches to priority assignment as shown in Table 1.

---

<sup>10</sup> Relatively simple in this context refers to the notion that the complexity of an algorithm to assign higher priorities to responders in a defined location is low; we recognize that the ability to reconfigure cell phones or other communications devices dynamically is a challenging issue.

**Table 1. Possible Dynamic Prioritization Approaches**

Authorized by  Requested by	Individual Responder	Central Authority	Network
<b>Individual Responder</b>	Priority is controlled by individual responder	Individual requests are granted “manually” by central authority, would not require cognitive capabilities.	Cognitive capability to respond to individual request.
<b>Central Authority</b>	Priority changes are initiated by central authority and “accepted” by individual responder.	Central authority makes unilateral decisions regarding individual responder priorities.	Cognitive capabilities in the communications network evaluate requests initiated by central authority
<b>Network</b>	Cognitive capabilities in network “recommend” priority change to individual responder who must “accept” the change.	Cognitive capabilities in network “recommend” priority changes to central authority who must “accept” the change.	Fully automated capability for priority management with no human in the decision loop.

While any of the above approaches is possible, we recognize that not all approaches will be appropriate for all situations, and user requirements for a specific system may well dictate that only one of the above approaches be implemented in a particular system. In addition, we recognize that an investment may be required to maintain information on responder credentials and to establish general policies as well as specific priorities associated with roles assigned to individual responders. Also note that there are ongoing and planned efforts in developing responder credential infrastructure to support incident management that can be leveraged to support this use case.

The other significant functional capability is the capability to reconfigure such a responder’s device. In this situation involving a GSM-based cellular network<sup>11</sup>, when ACCOLC is invoked, only cell phones with a SIM with priority authorization can access the system; other devices are blocked. The proposed cognitive use case assumes that either the SIM can be provisioned over the air for properly authenticated users, such that the phone would function with priority access. Alternatively, the system could determine that the user was a priority user based on the device ID (as opposed to the priority access code in the SIM) and allow access that way as well; however, the system computational effort to determine whether a call is being initiated by a priority user may involve substantial computational requirements.

We recognize that assignment of priorities presents challenges in making the determination of what communications are more important than others. Part of the ACCOLC decision criteria is the understanding that implementing ACCOLC would deny access to the network for responders (or for

<sup>11</sup> Note that concept of this use case would apply for other types of networks but reconfiguration would be implemented in ways other than over-the-air provisioning of SIMs.

victims and observers who are providing critical information or notifying others). The ability to prioritize communications as proposed in this use case does not guarantee that all critical or important calls are made—there are physical limitations to the capacity of any system. However, this use case provides the opportunity to utilize cognitive radio capabilities to implement the best decisions that can be made with the available information.

In addition to the changes to dynamically modify user priority, it is also important to be able to restore default conditions, such as when the user no longer requires priority access. Different mechanisms for restoration may be implemented but could be similar to the same mechanisms used to implement dynamic prioritization. Restoration could be executed based on a variety of mechanisms, for example user request, incident command direction, and location if the user moves out of the incident area. (see Section 5.4).

#### 4.3.3.4 *Regulatory Implications*

The ability to define priorities and block access to the system for certain types of priorities is part of the GSM specification.<sup>12</sup> Since this use case does not change the basic mechanism of ACCOLC, the regulatory changes are limited to only those that may be necessary to allow reprovisioning of SIMs over-the-air to change priorities.

#### 4.3.3.5 *Policy Implications*

There are a number of policy changes implicit in this use case.

- Policies for determining the circumstances under which an emergency responder would be eligible to “upgrade” priority?
- What information is required to authenticate the eligibility of the user to operate with higher priority?
- What procedure is followed if a user requests priority? Is there any human in that decision loop?
- Under what circumstances does the device’s priority revert to original level? Could reversion be automatic based on responder location, or time frame? Could incident command generate a broad directive (e.g., priority communications no longer required for a particular sector/unit/area) that cognitive capabilities could then execute to restore default priorities for all users?
- While not necessarily applicable in the case of ACCOLC, a more general capability to manage user priorities in real-time could also allow reducing default priorities of responders if their role in the response is less critical. Under what circumstances would a responder’s priority be reduced?

#### **4.3.4. Use Case 4: Interface to Non-First Responders**

Cognitive radios could allow non-first responders communications access to first responders in specific situations in which the non-first responders are actively participating in the response, while ensuring that mission critical public safety networks are not impacted.

---

<sup>12</sup> Siemens Insight Consulting, “Communicating in a crisis – which technologies can be relied on?” 22 September 2006, available at <http://www.continuitycentral.com/feature0394.htm>

#### 4.3.4.1 *Summary of Scenario Situation*

In terms of the aspects of public safety communications:

1. **Physical:** A fourth bomb was detonated aboard a bus near Tavistock Square. A group of doctors were within walking distance of the explosion and the injured people. The doctors arrived on the scene more quickly than first responders and therefore had more timely information than the first responders. No specific prior planning had taken place to apply these physicians as emergency response resources.
2. **Network:** The doctors did not have radios on any Public Safety net, but they did have cell phones and landlines were available in the building. However, no dispatch organization knew of doctors' availability, and thus had no ability to initiate contact with them. Any communication from the doctors had to come from 999 calls to dispatch, with information then relayed to command centers.
3. **Procedural:** Since they were not part of a first responder organization, the doctors had no authority to communicate on the first responder network.
4. **Regulatory:** Communication used established facilities.
5. **Chronological:** No prior planning had been done for the specific incident, but medical personnel are aware of the legal implications of what they do in an emergency situation.

#### 4.3.4.2 *Description of the Use Case*

In a mass casualty emergency there is a possibility that there are civilians that have the ability to provide added benefit to the responses that are taking place by the public safety community. In some cases these may be the only response available for an extended period of time. Thus it would be advantageous to leverage this capability and to provide direction to the efforts being put forth. This situation arose in this scenario when the bomb went off in a bus near Tavistock Square, as there was a group of medical doctors meeting in a nearby building. Thus there were a number of qualified medical personnel who were immediately available but were not tied into the incident command communications. These trained medical personnel were not associated with an EMS provider but were on the scene and able to provide qualified medical information regarding casualties. While this was in many respects a fortunate coincidence, a well meaning "good Samaritan" can also do more damage than good if they are unaware of the full situation. Thus the challenge is to establish effective communications with non-first responders without negatively impacting the incident command communications system and capabilities.

In today's communication environment the average person carries as a minimum a basic cell phone with the possibility of text messaging, photo and video capture and transmission. This cognitive use case is an example of how communications capabilities could be adapted to most effectively take advantage of situations in which non-first responder personnel are positioned to play a role in the response.

We recognize that current concepts of operation and existing procedures do not generally include linking first responder communications networks to non-first responder personnel (regardless of their potential role in a response), and any change to such procedures cannot compromise first responder communications.

Also note that the ability to appropriately link first responder communications with non-first responder personnel can also apply where some first responders are only equipped with commercial



equipment. In Europe, for example, volunteers (such as a volunteer fire service) that are part of the response may be equipped with commercial handsets rather than radios that access public safety networks. In such cases, the capability to link them into a first responder network is a vitally important capability.

A cognitive radio capability could allow them to link appropriately (upon proper authentication) to coordinate their activities with public safety professionals as needed. The following provides a view of how this scenario with cognitive radio could unfold:

1. **Physical:** No change from the physical situation described above.
2. **Network:** The initial doctor(s) on the scene would call 999 to report the explosion, and identify themselves as doctors qualified to provide information on the medical status of casualties. Dispatch, upon satisfaction that the caller could provide relevant information, reconfigures the network (infrastructure, portable, or both) to allow the caller to communicate directly with the appropriate emergency management medical coordinator, incident command, and so on as dictated by policy. Once the doctor no longer needs to be connected (i.e., first responder personnel arrive on the scene, the doctor begins performing other functions, or all relevant information has been communicated), the network reconfigurations are rescinded.
3. **Procedural:** Appropriate procedures would be in place to verify that the doctor was qualified to provide the information. This could be accomplished by having medical personnel pre-registered in some manner so that a dispatcher could authenticate the caller (e.g., password, biometric, etc.) and ensure that the individual's credentials already existed in a registry. The doctor(s) would have communications capability as needed to the appropriate organizations within the incident command structure. Procedures would also be in place to establish voice communications channels that would not disrupt mission critical incident command channels.

Given the presence of pre-registered individuals, an additional capability to be leveraged is the ability to push information from dispatch or incident command (using some type of notification system) out to pre-registered users requesting that they make appropriate contact with the incident command staff for allocation and assignment. Location-aware cognitive radios could also provide information to incident command to refine a notification procedure. For example, upon indication of a problem at Tavistock Square, the medical coordinator in dispatch would look at a map that indicates current deployment of medical resources. The concentration of doctors would show up immediately.

From a detailed roster of doctors near the bus, the dispatcher would select an appropriate number, and would send a short message to their mobiles asking if they can respond to a bomb emergency in Tavistock Square. Doctors would be selected based on their qualifications and specialties. The Cognitive element in the network would establish an ad-hoc response network. Each doctor who responds affirmatively would receive network identification information (i.e., callsign).

4. **Regulatory:** Appropriate regulations would be in place to allow non-first responders to communicate over the designated channels in emergency circumstances. Depending on the communications capabilities used, this may or may not require regulatory changes.

5. **Chronological:** This use case would require that some pre-planning takes place that allows doctors to establish the means by which they can be identified as such during an event (i.e., registration).

The above use case postulates that the communications is initiated by the doctors. A variation of this use case considers a situation in which any interface with the first responder networks is initiated by incident command. In this case we assume that a qualified medical person is not pre-registered but has arrived on the scene of the incident. The individual calls 999; dispatch relays the information through normal channels to incident command. The incident commander or appropriate authority within the incident command structure determines that direct communications with the individual is desirable, in which case the appropriate reconfigurations are executed. The scenario situation would be described as follows:

1. **Physical:** No change from the physical situation described above.
2. **Network:** No change from the network situation described above.
3. **Procedural:** A doctor arrives on the scene of the explosion and calls 999. The doctor explains the situation and his/her qualifications to provide more detailed assessment of the medical condition of the victims to the call taker. The call taker obtains contact information for the doctor and relays the information to incident command. Incident command determines that direct contact is beneficial—the cognitive radio capabilities then establish the appropriate communications network linkage between radios within the incident command/first responder units and the doctor at the scene. Note that additional non-first responders can be added to the network through the same process as needed and appropriate.
4. **Regulatory:** Rules are required to describe exactly how such an ad-hoc network is to perform and what channels they use.
5. **Chronological:** This use case would require that some pre-planning takes place that allows doctors to establish the means by which they can be identified as such during an event (i.e., registration). Registration would also cover responsibilities and liabilities that are assumed by the individual to perform such functions in an emergency. At time of notification of the event, each Doctor would have the option of responding, or opting out. If they respond affirmatively, they would become an on-site resource for incident command.

#### 4.3.4.3 *Functional Capabilities*

The specific functional capabilities involved in this use case depend on the approach used to implement it. If the implementation involves reconfiguring non-first responder radios to provide them with a capability to communicate with the incident command/first responders, then the functional capabilities include the ability to download a waveform and the ability for the non-first responders' radios to be reconfigured accordingly. If the implementation is based on infrastructure linking in a non-responder radio, then there must be a means for the non-first responder radio to upload information about the radio type.

A key element of this use, although not considered part of the cognitive capabilities, is ensuring that any user who is linked to the first responders has a legitimate need for such communications, and has a device that will not adversely impact first responder communications. Establishing that a user has a legitimate need for such communications involves a number of issues:

- Is the person someone appropriate for working with first responders? One approach used currently for interaction between first responders and civilians is to utilize some pre-registration process for translators, ministers, physicians, hazard experts, etc. Background checks were performed on all individuals prior to use.
- How is the identity of the user verified? Is the user who he/she claims to be?
- How is information provided by a user verified? In the scenario, assuming a doctor notified dispatch of the existence of casualties, how can that information be verified to a level of confidence necessary to modify communications? (Note that dispatch call-takers routinely evaluate the information provided in incoming calls.)
- How is the potential role of a non-first responder verified?

In addition, the role of such responders would need to be incorporated into the incident management (e.g., NIMS) as appropriate. Note that it is common for existing dispatch centers to have a capability to patch a phone line to a radio channel. This cognitive use case extends that concept to include establishing links between first responder communications channels and non-first responder wireless devices/radios.

#### 4.3.4.4 *Regulatory Implications*

Regulatory implications may also depend on implementation approach. Reconfiguring a non-first responder radio to be able to have some type of access to a public safety network would require changes to the manner in which radios are currently type accepted. The alternative implementation, in which the non-first responder communicates on their existing frequencies which is patched to a public safety network frequency or channel is done with current technology and would not generally require regulatory changes.

#### 4.3.4.5 *Policy Implications*

Policy implications are dependent on the extent to which “non-first responders” are currently incorporated into emergency response/incident management. In locations such as the United Kingdom, where volunteer responders are incorporated into the response team, the only policy change would potentially involve:

- Guidance on the circumstances under which the cognitive capabilities would be exercised to establish access for non-first responders (including policy on authentication, security, and procedures);
- Guidance on what communications are appropriate under such circumstances; and
- Guidance on when and how non-first responders are disassociated with the network.

For agencies that typically do not utilize direct communications with non-first responders, such as those in the U.S., any implementation of this cognitive capability would involve much broader policies.

## 5. MULTI-USE CASE FUNCTIONAL CAPABILITIES

In addition to the functional capabilities that are identified for each specific use case in Section 4, there are functional capabilities that need to be incorporated into any cognitive use case (or combination of use cases) to be operationally viable. In this section we identify those additional functional capabilities, including: Role-Based Capabilities (Section (5.1), Command & Control (Section 5.2) and Security (Section 5.3).

### 5.1. Roles

Many of the concepts of cognitive capabilities include a notion of the “role” of a responder. Although not formally defined in this document, the general concept of role is the function being performed by a responder: traffic control, perimeter security, fire suppression, logistics coordinator, medical transport driver, etc. The role of an individual is typically assigned through a hierarchical chain of command starting with an incident commander (or supervisor during normal operations). An individual’s role may change during the course of an incident, and an individual may be performing more than one role simultaneously. The individual’s communications capability needs to adapt to his role assignments. The use case discussed in Section 4.3.4 postulates a situation in which non-first responders are temporarily fulfilling roles.

Different roles require different communications capabilities, in terms of who needs to talk to whom, the relative priority of communication, the quality of service required for the communication, and so on. Communications capability should support the role of the radio user. This concept exists in rudimentary form today—often departments have commander or supervisor radios with additional functionality and/or channels/talk groups. However, current radio configurations are defined statically such that they require reprogramming or hardware changes to be reconfigured.

The definition of roles has two components: the role that the responder is performing in the course of an incident; and the capabilities of the radio necessary to provide that responder with the communications and connectivity to perform that role. The mapping of radio capabilities to responder roles is generally a pre-defined assignment based on agency policies. A simple example in place today is that some agencies provide supervisors with radios that are programmed differently and/or have different capabilities than other officers. Role definitions could be implemented as a policy that can be authenticated and downloaded once the role of the responder is adequately established.

Cognitive radios can reconfigure based on who the user is and the role that the user is assigned in the response. The ability of radios to be reconfigured based on roles addresses one of the public safety concerns about reconfigurable radios—that radios that can be reconfigured to operate on multiple bands and multiple channels could lead to chaos if “everyone can talk to everyone.” Introduction of the concept of roles can allow department policies to govern communications capabilities while permitting flexibility to allow the communications to evolve as incidents evolve and responders assume various roles. Users performing multiple roles simultaneously could have the union of capabilities associated with the roles.

Cognitive capabilities to support the concept of roles include the following:

- Ability to define radio capabilities and connectivity as a function of roles.

- Ability to interpret policies and procedures as a basis for cognitive decision-making.
- Ability for a radio to support multiple roles.
- Ability to reconfigure radio and network to support different roles in real-time.
- Ability for an authorized user to define new roles and associated communications capabilities in real time, and forward the information to the radios.

While the concept of roles provides a useful construct for reconfiguring radios, we also recognize the challenge of linking the real world activity to cognitive radio capabilities and to the command and control system (as discussed in Section 5.2). When responders are assigned a responsibility within an incident command structure, it may be feasible to assign a role and corresponding communications capabilities based on that role. However, roles may change in real-time, or roles may change based on events at the scene. Agency policy could dictate whether roles could be changed by someone at a higher level in the command and control structure, by responders themselves, or automatically as a function of data type leveraging cognitive capabilities. (Only a small number of situations seem appropriate for the last case, for example, a “man down” communication is assigned highest priority.) Establishing a workable policy that provides flexibility to adjust priorities in real-time without burdening the command structure will require additional research and thought.

## 5.2. Command and Control

One of the consistent themes in all of the cognitive use case discussions is that the flexibility inherent in cognitive radios allows communications to be reconfigured to meet unexpected, unanticipated aspects of the response. Each use case is rooted in situations for which the system was not required to accommodate:

- Destruction of infrastructure in the tunnel,
- Overloading of the available communications capacity,
- The priority of responders’ roles differing from static priority assignments in their communications capabilities, and
- Non-first responders having a potential role in the response.

Cognitive radios not only include the ability to reconfigure to adapt the communications to the evolving situation but could also incorporate some decision making capability into the network and subscribers as well.

One of the challenges unique to this particular scenario is that it evolved from four isolated incidents which, due to their proximity in time and location, evolved into a major incident. One of the incident management challenges was to configure the communications to support the rapidly evolving command and control required to respond to the incident. Initial response procedures were initiated for each incident and needed to be coordinated with a broader response that was executed as the full scope of the attack became clear. Communications capabilities must be able to evolve as an incident evolves—communications structures to support a single incident (such as one of the individual bombings) must be rapidly expanded when coordination of responses to multiple events is required.

To realize the benefits of cognitive radios in the public safety domain without inviting chaos, it is therefore critical that:

- Cognitive capabilities, and the decision making process, be under the control to the extent desired of human(s) responsible for routine or incident response communications (e.g., NIMS Comm Unit Leader, network manager). Note: “To the extent desired” in the preceding statement allows a scalable array of cognitive capabilities to be deployed with varying degrees of human interaction as needed. For example, in the example of dynamic spectrum access, cognitive radios could be allowed to utilize appropriate frequencies as needed, or could provide a recommendation for human confirmation, or be directed to reconfigure to a new frequency specified by a human.
- Communications must support the appropriate command and control policies and procedures governing an incident or routine response (e.g., NIMS).

Functional capabilities to support command and control and the functions of communications management include the following:

- Status information concerning subscriber radio configuration must be accessible by a user, though an appropriate combination of audio and visual cues and visual displays.
- Status information concerning radio and network configuration must be accessible by an authenticated network manager.
- System design incorporating cognitive capabilities should include options for human intervention in the decision process.
- Cognitive capabilities should be able to incorporate command and control policies and procedures.

It is also worth noting the incident location in this scenario did not change, there are other scenarios in which an incident (or collection of incidents) could spread or move—for example, a riot, a kidnapping, or airborne release of a hazardous chemical. The public safety response needs to be equally flexible and to take into account the incident location and the impact on its surroundings – both ‘where it is now’ (current threat) and ‘where it has just come from’ (evidential retention) while seeking to anticipate ‘where it might go next’ (public safety). In such scenarios it is vital that any reconfiguration be under control of a central authorisation. While much of this can be accomplished automatically, some degree of human interaction is required to (a) maintain situation awareness of what is actually occurring and (b) to ensure post-Incident Management evidential continuity and/or contingency planning.<sup>13</sup>

Another aspect of control that cognitive radios could support involves the challenge of first responders “self dispatching” or otherwise participating in the response without the knowledge of incident command. Situations have occurred in which responders’ dedication and strong desire to save lives results in participation in the response without properly coordinating with, or assignment by, incident command. Responders, who have “self-dispatched” themselves to incidents need to be identified, and either allocated to their current activities or withdrawn and reallocated to appropriate duties.<sup>14</sup> Cognitive radio capabilities can support this process in two areas. First, cognitive

<sup>13</sup> Neal Skelton and Mark Cartwright, private email correspondence.

<sup>14</sup> *Ibid.*

capabilities of network attached radios could identify a peer radio that is not attached to the network even if the non-attached radio is only using a peer-to-peer mode of transmission, or potentially some other means of peer discovery. This capability could help identify the presence of responders who are not properly authenticated into the network and may be unknown to incident command. Second, once incident command is able to use the information to contact such a responder, they can be assigned an appropriate role in the response and their radios reconfigured accordingly.

The ability of cognitive radio technology to provide tools for enhanced command and control will require significant training for agencies to realize their benefits. We have postulated several capabilities that give communications unit leaders, network managers, and so on significantly greater control over the communications so that communications capabilities can adjust in real-time to the evolving needs of an incident. Although there are many approaches which can be implemented to realize these use cases, in general we have assumed that:

- To the extent feasible cognitive capabilities can automate some aspects of the communications configuration and reconfiguration while allowing human oversight (i.e., not fully autonomous systems).
- Cognitive capabilities should make as much of the reconfiguration seamless to the end user.
- Cognitive feature capabilities can be tailored to agency needs.

A key aspect of control, both at the network level and the subscriber level, is to ensure that reconfiguration is done with the users' knowledge and, as defined by policies and procedures, with the users' consent. While much of the benefit of cognitive capabilities involves making the behavior of the radios and the network achieve functional goals without requiring significant user intervention, at those times when radio behavior will change (temporarily being reconfigured, changing priorities, connecting with non-first responders), the users need to be aware of the change of capabilities. Policies and procedures will also need to be defined to clarify what control individual users have over the cognitive capabilities. These policies may be defined in terms of the role of the users as discussed in Section 5.1. An example of a policy that likely would be included is the ability to override radio reconfiguration to ensure that life-critical communications are transmitted (i.e., the man-down alarm always gets transmitted regardless).

Assuming the deployment of the capabilities outlined in this document, one of the challenges will be developing sufficient numbers of trained personnel to manage the network, define communications links to support incident command, and provide the appropriate human intervention over the functions of the network. Pre-planning and coordination will continue to be important, but the capability of cognitive radio technology to allow adjustment of communications capabilities in near real time adds complexity to the communication management. Also, capabilities that minimize the demands on the end user are likely to add complexity to the overall network management. In the NIMS structure in the United States, this function is the responsibility of the Comm Unit Leader. For the Gold Coordinating Group, there will be someone responsible for managing network configuration and reconfiguration, authorizing access to additional spectrum, and other similar functions. It will be necessary to provide such individuals with education, training, tools, and experience (e.g., through exercises, participating in support functions during actual incidents) to prepare them to execute this responsibility.

### 5.3. Interoperability

The After Action reports for this scenario did not specifically identify communications interoperability as a significant impediment to the response to the bombings. The initial phases included resources from 3 separate police forces – Metropolitan Police, British Transport Police and City of London Police forces. All are separate and distinctly individual police forces that have their own command/reporting chains. In addition there were responders from the London Ambulance Service involved as well. Communications between responders of these organizations typically only occurs at the highest level. However, by linking cognitive radio technology to the concept of roles described in Section 5.1, there may be opportunities to enhance interoperability among responders based on the communication requirements of the incident. For example, if based on roles it was useful for responders from one agency to communicate with responders from another agency, cognitive radio capabilities could either reconfigure the radios or identify a common channel to support interoperability.

Cognitive radio capabilities could also simplify the planning associated with a major event. For example, when additional law enforcement personnel are brought into an area to assist with an event (e.g. 300 officers from West Midlands Police drafted in to help out at the UK’s Millennium Stadium in Cardiff on Football Cup Final day) it would be useful if their “home” (Wmids) radios could be reconfigured temporarily on the Gwent network.<sup>15</sup>

### 5.4. Restoring Default Configurations

Each of the use cases described in Section 4 involve dynamically reconfiguring subscriber and/or network capabilities based on the evolving requirements of a dynamically changing incident. At some point as the incident winds down, the capabilities must be reconfigured to return to their normal default capabilities. To some extent the concepts that have already been identified, such as roles, can be applied to the ramp down of the incident as well as to the ramp up—when a responder reverts to their normal (daily operations) role, the associated communications capability reverts as well. For example, priorities in a dynamic prioritization scheme would be restored to their normal levels. In the case of network extension, once the responder is back within the normal coverage footprint of the system (e.g., out of the tunnel) the radio would be reconfigured to its initial configuration.

To achieve this ramp down gracefully, there are additional functional capabilities that would be useful in addition to those identified in the use cases in Section 4:

- A capability to recognize when the circumstances that caused initial reconfiguration are no longer relevant. In the case of radios being out of network coverage, the circumstance would be when the radio is back within coverage. In the case of dynamic prioritization, the circumstance would be when the role of the responder changes. In some cases, such as the dynamic prioritization based on responder role, there is a discrete point in which one can explicitly identify that the circumstance has changed—the responder is being discharged from the incident response assignment. In other cases a discrete point will be more difficult to identify—for example, when the demand for communications resources has declined to the point where additional

---

<sup>15</sup> *Ibid.*



spectrum is no longer required. In these cases, specific cognitive functions may be required to identify when the default configurations should be reinstated.

- Records of the configuration changes, both for audit and post-incident analysis purposes, as well as to specific “undo” configuration changes if necessary.
- A cognitive capability to determine whether preferable to simply restore defaults or to sequentially undo each change.

## 5.5. Security

Cognitive radio technology requires consideration of potential risks to public safety communications to avoid introducing new vulnerabilities. By expanding communications options available to first responders, cognitive radio technology also has the potential to open new points of vulnerability in public safety communications systems. For instance, attempts to exploit new cognitive features by individuals or organizations in order to compromise the availability, confidentiality, or integrity of first responder communications is almost certain. Fortunately, technical design features and operational controls should be able to mitigate potential risks to the level that they do not represent a significant threat to the public safety mission. This section briefly reviews three potential controls (user and role authentication, device and network authentication, and reconfiguration control) and recognizes associated technical, operational, and regulatory changes that may be required to implement them.

### 5.5.1. User and Role Authentication

Many advanced public safety communications systems support user (operator) authentication today to prevent unauthorized individuals from accessing public safety networks. However, user authentication in these systems is typically limited to public safety personnel operating on their own closed network. Thus anybody who can access a radio can access and possibly disrupt communications on these networks. In contrast to today’s situation, possibilities exist for *non*-first responders to access the network in one of the cognitive use cases. In another use case, first responders are granted higher priority on a *non*-public safety network, specifically one supporting commercial cellular telephony. In both instances, there is a need to authenticate users seeking privileges not common in day-to-day use of the system. Without a more robust authentication method, in each instance the potential exists for significant misuse or abuse of the cognitive functionality. This can result in congestion or the prevention of communications essential to the life-critical emergency situation.

Authenticating external users to an otherwise closed network need not be a significant challenge, as there are a variety of solutions available from which to choose depending upon the circumstances involved. For example, if the user who needs to join the network has a compatible radio then it might be a simple administrative action over the air to identify the user to the network by a known individual who is already a part of the network. This is known as authentication by proxy. This method can work in a variety of other circumstances. For instance, there may be an individual who is on the scene who needs to get priority on the public cell phone network. A known individual can obtain the ESN of the user and pass it into the public safety system and have the user’s cell phone granted a temporary priority until it is no longer needed. Another example that external users have to add or upgrade authentication software or other supporting software

components on their devices to interoperate with the target network. A cognitive radio could possess the capability to ascertain what components are needed and, with the users authorization, the cognitive radio could automatically proceed to download and implement the necessary software. In other instances, users likely will need to complete some form of registration process prior to the actual use of the system. The managers of the network will also need to build directory services and associated databases to support authentication transactions for the users of the system. In some cases, regulatory changes may be required if current public safety administrative regulations require security controls that are incompatible with the proposed technology, or if use of a network requires personnel clearances not held by the users that would have access to the network. Other regulatory issues might arise if the terms of allocations and radio licenses limit operation to certain classes of users.

One way to simplify some of the complexity resulting from cognitive capabilities is to limit authentication to the user's role rather than the user's identity. For example, in a major emergency such as the London bombing, it likely is more important that first responders know that a network access request is coming from a medical doctor (a role) than it is to know that the request is from Dr. John Smith of Central Municipal Hospital (a user). A role-based system may need to handle from a limited number of roles, while a user-based system may need to manage thousands of users. Individual users still need to authenticate themselves as being legitimate users, but this authentication can be managed with simple schema currently used (e.g. passwords or physical tokens) in such cases.

To support a role-based system, a user in a particular role could obtain a public key certificate from a nationally trusted certification authority that he or she legitimately serves in that role.<sup>16</sup> The technical characteristics of public key certificates would enable the user to authenticate in any jurisdiction that recognized the national authority, thereby obviating the need for each jurisdiction to maintain or connect to databases for all potential users in that role. Certificates could also be accompanied by relevant capabilities of the individual, such as that he or she is a trauma specialist or has expertise in the handling of explosive or radioactive material. An important consideration with the use of certificates is that a method is required to securely store the credentials. Otherwise they can be exploited by anybody. Maintaining the credentials in the radio (or even in an external token) implies that they can be protected from physical attack and that the actual user has a means of unlocking the certificate and authenticating himself to the radio, such as a user ID and password. While technology to support this system is widely available, the cognitive radio abilities described would require the set-up of a supporting public key infrastructure and related policies and procedures for this particular application.

In some cases, ad hoc roles may be established to support a particular incident. For example, emergency responders may want to identify users that carry camera phones to get images from locations that might be inaccessible as a result of a disaster. In this case, the cell phone users would not be members of a pre-registered group such as medical personnel, but still should be distinguished from users that are not supporting incident response. Users that can serve in a supporting role could be authenticated based in part on their location or, as described earlier, by

---

<sup>16</sup> Another mechanism to achieve role-based authentication is to employ call group keys that are used to encrypt message content. Members of a call group could be associated with a role. When keys are used to encrypt communication, they serve as a *de facto* form of authentication because those without the relevant key will be unable to interpret encrypted communications. PKI provides the tools for key management to ensure that all users who require keys have them..

proxy Cognitive technology could be used to identify these users and determine how to best differentiate them on network so that incident command can easily access them

### **5.5.2. Device and Network Authentication**

With the exception of including ad hoc users into a situation, and as long as the user authenticates himself to the device, it is not the user that needs to be authenticated to the network; rather the device that the user carries. For example, one use case for cognitive radio involves extending the network to radios that cannot reach the regular infrastructure for whatever reason. In this case, the cognitive radio, in effect, serves as a repeater or interface bridge for the radios for which the infrastructure is unavailable. The new functionality introduces two important security issues: first, how do we know that the first responder's radio is connecting to the cognitive repeater and not a rogue radio, perhaps one setup by those who caused the emergency and disruption in communications; second, how is the system preventing rogue radios from accessing the network via the cognitive repeater?

For situations that do not involve legacy radios, the solution is to support mutual authentication between the device and the network to which it connects. In the network extension case, the cognitive radio that extends the network should support an authentication pass-through that would enable authentication services to be performed just as it would under normal circumstances. Of course the cognitive radio which is providing the pass through would first have to authenticate itself to the network. Techniques such as Extensible Authentication Protocol (EAP) support this capability today and are implemented on Wi-Fi equipment and other communications systems. Moreover, they can be implemented in a manner than is transparent to users and does not require operational or regulatory changes. Nevertheless, new cognitive radios that support network extension should be accompanied by device and network authentication modules to protect systems against attack.

### **5.5.3. Reconfiguration Controls**

One of the use cases for cognitive radios is to switch protocols to balance load or allow additional access. In this case, the radio automatically reconfigures itself to provide new benefits. The risk is the radio will not perform the intended function after reconfiguration, perhaps because an adversary has modified radio software modules to cause a system failure or connect to an unauthorized network.

As with any reconfigurable radio, cognitive radios will need to implement security controls to provide assurance that reconfiguration transactions perform as expected with very high integrity and sufficient robustness. Code signing, RF transmission policy enforcement, and memory isolation using secure operating system kernels are all currently technology mechanisms that can prevent unauthorized behavior. The SDR Forum's *Securing Reconfigurable Communications Technology* document (forthcoming) explains these potential controls in greater detail.

## **5.6. Transition and Interface to Legacy System**

Realization of any of the use cases described above will not happen "overnight" even at the point where the technology is proved, supporting regulatory changes have been instituted, and

policies and procedures have evolved accordingly. Thus in each use case functional capabilities, regulatory considerations, and policies and procedures will need to accommodate legacy systems as well.

Specific functional capabilities required to realize this capability include the following:

- The network needs to be able to distinguish legacy equipment and the capabilities of each device—note that since legacy equipment may not be programmed or configurable to transmit specific capabilities information to the network, it may be necessary for the network to recognize the waveform characteristics and derive/infer the device capabilities.
- The network needs to be able to reconfigure transmit/receive capabilities to interface with legacy equipment and bridge as appropriate to establish necessary communications with other subscribers on the network.
- The network may also need to establish/re-establish communications links to avoid interference from legacy equipment.
- An appropriate subset of the above functions should also be implemented at the subscriber level.

## 5.7. Interaction of Use Cases

While these use cases have been described and analyzed independently, there are interactions among the use cases and the cognitive capabilities that support the use cases. For example, dynamic spectrum access and dynamic prioritization could interact such that responders with the highest (or lowest) prioritization could utilize dynamically allocated spectrum to maximize access for the highest priority users. Dynamic spectrum access techniques may be useful in realizing the network extension use case. Network extension capabilities could be used to link to non-first responders. We also recognize that the issues of command and control described in Section 5.2 become even more challenging as capabilities are implemented to realize multiple use cases.

It is beyond the scope of this report to address all of the issues that could arise in the interaction of use cases, so we simply note that there are additional interactions to consider in addressing multiple use cases, in terms of functional capabilities, regulatory considerations, and policies and procedures.

## 5.8. Standards

Some of the use cases involve communication of control information among subscribers (e.g., discovery of peer radios) or between the network and subscribers. Examples of the latter include information concerning roles and priorities. There needs to be standard protocols for the transmission of such information to ensure that radios are interoperable.<sup>17</sup> For example, in the network extension case (Use Case #1), a result in which Vendor A's radios cannot create a link with Vendor B's radios would set back much of the ongoing effort to develop standards such as P25 and

---

<sup>17</sup> Recent legislation passed by the U.S. Congress requires that federal grant money can only be spent for communications equipment developed pursuant to voluntary consensus standards where such standards exists.

TETRA that promote interoperability. The specific protocols requiring standard definitions will depend in many cases on the specific approach used to implement functional capabilities identified in the use case, so it is important to recognize that standards will be needed to ensure interoperability of cognitive radios.

## 6. SUMMARY

The analysis in the preceding sections outlines significant capabilities that can enhance the ability of public safety agencies to communicate, particularly under the challenging conditions of a major event or incident. We have identified the potential use of cognitive capabilities to:

1. Extend existing network coverage when individual radios move outside the coverage footprint of the communications system;
2. Dynamically allocate spectrum to provide greater capacity for overloaded networks;
3. Dynamically prioritize communications to better manage load; and
4. Dynamically reconfigure networks to incorporate non-first responders who have information of value to incident management and/or responders.

In order to realize these use cases, there are a number of functional capabilities that need to be developed (and tested and proven), including the following:

- At the network level:
  - Identify loading that meets criteria for initiating dynamic spectrum access.
  - Identify spectrum resources that can be used to offload calls or expand capacity, either by executing established agreements or by searching for underutilized spectrum (“white space”) that could be dynamically accessed.
  - Manage the hidden node problem.
  - Deconflict the situation of multiple users attempting to access the same available spectrum.
  - Assign and download priorities to subscriber equipment based on user roles.
  - Download reconfiguration information to subscribers.
  - Recognize legacy equipment and manage communications accordingly.
  - Restore normal and default configurations.
- At the subscriber level:
  - Determine when they are disconnected from the network.
  - Find and identify peer radios.
  - Create a network extension route to the infrastructure from each “disconnected” device (also requires determination of non-interfering frequencies for each “hop”).
  - Adjust network as devices enter and exit the area.
  - Preserve the level of security of the baseline network in the network extensions.
  - Reconfigure to incorporate the added transmit/receive frequencies.
  - Reconfigure to function as repeater.
  - Change priority levels.

- Interaction with user and device authentication schemes.
- Ensure reconfiguration does not compromise the security or integrity of the radio or its operations.

We recognize that some these capabilities are deployed today in some form, while others may require significant development. We also recognize that there are substantial regulatory and policy and procedural considerations and changes that will be required in conjunction with the technical developments to realize the impacts described in Section 4. However, we also realize that development of cognitive capabilities can dramatically increase the ability of incident commanders. First responders will be assured that critical information will flow as needed despite changes in coverage, connectivity, and loading on communications systems.

1 **APPENDIX A: LONDON BOMBING SCENARIO**

2 This Appendix provides the timeline events during the London bombing incident of July 7, 2005. In the Scenario there are a number  
 3 of places in the timeline (use cases) where the PS-SIG felt that SDR capabilities could provide an improved capability to what is in place.  
 4 In the timeline these events are shown with a green shaded cell in the table. Section 4.3 provides an expansion on these use cases.

5 The X in the Communication Activity is an indication that there is a form of electronic communication taking place. This  
 6 could be in the form of RF or data via IP.

7  
 8

**Table 2. London Bombing July 7, 2005 Timeline of Events**

Time/ Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
8:50 AM First bomb detonated at Liverpool St.				
8:51 AM Second bomb detonated at Kings Cross.		Multiple, often conflicting, reports were being made, some to London Underground's Network Control Centre, some to the emergency services, and some to the media. There were reports of loud bangs. There was a loss of power on sections of the Underground. 999 calls were made from nearby locations reporting smoke issuing from tunnels and from a grid in a street close to Edgware Road. It was not clear what had happened, or indeed where.	999 calls were made from nearby locations. {Units dispatched.}	
8:52 AM		Serious and non-serious injuries result. In the minutes following the explosions on the Tube trains, passengers were plunged into total darkness.		Line control centers identify lack of communications, attempt alternative routing, generate alert. (Note that cognitive capabilities in the train radio system could be implemented to provide this capability, but since it





Time/ Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
		They did not know whether anyone knew they were there, or if help was on its way. The internal carriage lights went out, internal communications between the driver and passengers of each train were debilitated, and Drivers were unable to communicate with their line control centres. Passengers on the three bombed trains were unable to communicate with the drivers of the trains to alert them to the explosion		does not involve public radio systems it is not included in the use cases in Section 4.
8:53 AM				
8:54 AM Third bomb detonated at Edgware Rd				
8:55 AM	The first British Transport Police officer arrives at the scene and reported 'building shock' and smoke issuing from the tunnel, but no evidence of structural damage.		✘	
8:56 AM	<b>King's Cross</b> The Metropolitan Police Service was first alerted to an incident at King's Cross on the basis of CCTV footage of the station.		✘	
8:57 AM				
8:58 AM	<b>Aldgate</b> The British Transport Police had identified the site of the incident in the tunnel between Aldgate and Liverpool Street, but had not discovered any injured passengers at that point. Power to		✘	

Time/Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
	the track was cut off. <b>Edgware</b> The British Transport Police receive a call to Edgware Road, reporting a person under a train and a train collision with the tunnel wall.			
8:59 AM			Network Control Centre put in an emergency services call to three sites – Aldgate, King’s Cross and Edgware Road.	
9:00 AM	<b>Aldgate</b> The first fire engines arrive. Further Fire Brigade units were mobilized to a reported explosion at Aldgate. <b>Edgware Road</b> The London Fire Brigade mobilized five units, including a Fire Rescue Unit and a Fire Investigation Unit, to Praed Street.		✘	
9:01 AM				
9:02 AM	Further appliances were mobilized, responding to reports of smoke in a tunnel. Two fire engines and a senior officer were sent to <b>Aldgate</b> , and an additional fire engine was sent to <b>Liverpool Street</b> . <b>King’s Cross</b> The London Fire Brigade received its first 999 call, reporting smoke issuing from a tunnel at King’s Cross.		✘	
9:03 AM	<b>Aldgate</b> The first ambulance arrives at Liverpool Street,			
9:04 AM	<b>Edgware Road:</b> The first London Fire Brigade units arrived at Praed Street.	Praed Street turned out not to have been the site of any incident	The Metropolitan Police were called by the London Fire Brigade and	

Time/ Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
	<b>King's Cross</b> At 9.04 am, a 'split attendance' was mobilized, with three fire engines sent to Euston Square and one to King's Cross.		were on the scene at 9.12 am.	
9:05 AM				
9:06 AM	Emergency planning manager arrives at Liverpool Street.			
9:07 AM	The London Ambulance Service Emergency Planning Manager advised Central Ambulance Control to place hospitals on major incident standby, identify safe rendezvous points in case of a Chemical, Biological, Radiation or Nuclear (CBRN) risk, and mobilize equipment vehicles. Edgware Road Fire Control received a call alerting them to the location of the incident on the Hammersmith and City Line at Edgware Road station. Fire engines arrived at Euston Square (which turned out not to be one of the sites where passengers were emerging from tunnels).	There are 25 walking wounded, some of whom were badly injured.	☒	
9:08 AM	The British Transport Police at the scene reported that there had been a train accident, and declared a major incident.			
9:09 AM				
9:10 AM	The City of London Police recognized that there had been an explosion caused by a bomb, and declared a major incident.			
9:11 AM	Additional Fire engines arrived at Euston Square (which turned out not to be one of the sites where			

Time/ Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
	passengers were emerging from tunnels).			
9:12 AM	<b>Edgware Road</b> The first ambulance arrives at Edgware Road. <b>Edgware Road</b> Metropolitan Police on the scene.	Communication between the control rooms of the emergency services in the event of a major incident takes places through a ‘first alert’ system. This is done through a ‘first alert’ call, which is in effect a conference call involving the emergency and transport services. The ‘first alert’ system was activated at 9.12 am.	☒	
9:13 AM	<b>King’s Cross</b> The first fire engine arrived at King’s Cross station. Fire Control – four vehicles were mobilized to Edgware Road. Only one of these was a redeployed vehicle from Praed Street.		☒	
9:14 AM	<b>Aldgate</b> An ambulance crew reported that the incident had been an explosion, and that there were five fatalities. <b>Edgware Road</b> Ambulance corps confirmed that there had been an explosion and requested ‘as many ambulances as you can muster’. The crew reported back to the control room that there had been an explosion with up to 1,000 casualties <b>King’s Cross</b> A London Ambulance Service Fast Response Unit arrives at King’s Cross		☒	
9:15 AM	The London Fire Brigade declared a major incident. <b>Kings Cross:</b> A major incident was declared at King’s Cross by	The London Ambulance Service was initially called to seven separate sites, and ambulances were being deployed to ‘various places that ended up not	☒	

Time/ Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
	the Metropolitan Police Service.	<p>being the main incident sites'. For some time, it was thought that there may have been up to five separate incidents on the Tube, and the emergency services were being deployed accordingly to five separate Tube station.</p> <p>A 'leaky feeder' cable that enables the British Transport Police's radios to function was damaged by the blast. Emergency and transport services personnel were therefore unable to communicate with their colleagues at ground level without making the 15-minute journey back down the tunnel to the platform.</p> <p>The decision was taken at 9.15 am to declare a network emergency and evacuate the entire Tube network.</p>		
9:16 AM	<p>On arrival at the affected trains, emergency services personnel sought to establish what had happened, and needed immediately to communicate this information to control centres. The British Transport Police is the only emergency service equipped with radios that can function underground. All the other emergency services had to rely on individuals running back and forth from the train to the platform and from the platform to ground level, or use British Transport Police radios.</p>			
9:17 AM				
9:18 AM	<p><b>Edgware Road</b> The first fire engine arrived at Edgware Road.</p>	<p><b>Russell Square.</b> The British Transport Police reported that there</p>		


Time/ Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
		were at least 200 casualties.		
9:19 AM	The British Transport Police formally requested assistance from the Metropolitan Police Service (which is the lead police service in the event of a major or catastrophic incident, even if it takes place within the jurisdiction of the City of London Police or British Transport Police). <b>King's Cross</b> First ambulance on scene. <b>King's Cross</b> Further fire engines were requested to King's Cross.	It is unclear precisely when the London Fire Brigade became aware that there had been an explosion at King's Cross. However, we do know that the ability of the London Fire Brigade to establish what had happened at King's Cross was hampered by the fact that hand-held radios did not work effectively between the platform and a control position at the top of the escalator, nor between the top of the escalator and outside the station. The Fire Brigade therefore had to use runners – individuals running up and down escalators – to communicate from below ground to the surface.	✘	<b>Network extension for coverage &amp; reachback</b> (see Section 4.3.1)
9:20 AM	The Metropolitan Police was in fact already aware of the incident, and the first officer arrived at the scene			
9:21 AM	<b>King's Cross</b> A major incident was declared at King's Cross by the London Ambulance Service.		✘	
9:22 AM				
9:23 AM				
9:24 AM	<b>Russell Square</b> The London Ambulance Service dispatched a Fast Response Unit.		LAS dispatched Fast Response Unit.	As part of the analysis performed for this document, it is noted that similar information arrived at the BTS and the LAS command centers at significantly different times. After considering potential cognitive capabilities to improve the timeliness of information flow, we concluded that the issues primarily command and control issues (procedural environment) rather than

Time/Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
				communications issues. Cognitive capabilities could support real-time changes in the network environment to support changes in command structure.
9:25 AM			The first conference call on the 'first alert' system took place.	
9:26 AM				
9:27 AM				
9:28 AM				
9:29 AM				
9:30 AM	<b>Russell Square.</b> A Fast Response Unit arrived at the scene.			
9:31 AM				
9:32 AM	<b>Edgware Road</b> The Metropolitan Police Service declared a major incident		✘	
9:33 AM				
9:34 AM	<b>Edgware Road</b> The Fire Brigade declared a major incident at Edgware Road station.		✘	
9:35 AM				
9:36 AM	<b>King's Cross</b> Further fire engines were requested to King's Cross.		✘	
9:37 AM	<b>Edgware Road</b> The Fire Rescue Unit that had been sent to Praed Street re-deployed to Edgware Road		✘	
9:38 AM	<b>Russell Square</b> A major incident declared at Russell Square by the London Ambulance Service (note: this is 45 min after the explosion).	<b>Russell Square</b> The Ambulance Service Professional Standards Officer at the scene was reporting 6-15 fatalities and 50+ casualties fatalities - and stated that there was only one ambulance at the scene, along with the Fast Response Unit. Note: This was a full 20 minutes after the British Transport Police received	✘	

Time/Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
		reports of loss of life and limbs.		
9:39 AM		<b>Kings Cross.</b> The ambulance crew reported that there was still no officer at the scene, but that there were 400 casualties and 15 ambulances were needed.	✘	
9:40 AM		<b>Russell Square.</b> The Metropolitan Police Service requested the London Ambulance Service to ‘send every unit that you have got’.	✘	
9:41 AM				
9:42 AM				
9:43 AM				
9:44 AM				
9:45 AM				
9:46 AM		<b>Kings Cross.</b> The first LAS manager was sent to the scene, almost an hour after the explosion.		
9:47 AM Fourth bomb detonated	<b>Tavistock Square.</b> It was immediately apparent what had happened, and the first 999 call was made, within a minute of the explosion. Twelve further 999 calls were made, all before 9.56 am. A number of medics were on the site before that time: the bus was located outside the headquarters of the British Medical Association and doctors and other trained first-aid personnel came out of the building to care for the injured.		✘	<b>Interface to non-first responders</b> (see Section 4.3.4).
9:48 AM	<b>Russell Square.</b> One ambulance was dispatched from University College Hospital.		✘	
9:49 AM				



Time/ Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
9:50 AM	Fire engines dispatched to Tavistock Square.		☒	
9:51 AM				
9:52 AM				
9:53 AM				
9:54 AM				
9:55 AM				
9:57 AM	<b>Tavistock Square.</b> The Metropolitan Police Service happened already to have an officer at the scene. The first ambulance arrived on the scene at Tavistock Square, having come across the explosion (as opposed to having been specifically dispatched there).			
9:58 AM				
9:59 AM				
10:00 AM				
10:01 AM				
10:02 AM	<b>Russell Square.</b> A request was made for five ambulances and a bus.		☒	
10:03 AM				
10:04 AM				
10:05 AM				
10:06 AM				
10:07 AM				
10:08 AM				
10:09 AM				
10:10 AM				
10:11 AM				
10:12 AM				
10:13 AM		<b>Kings Cross.</b> duty officer reported that there were still more than 50 casualties in the train, and requested a further ten ambulances and an	☒	

Time/Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
		equipment vehicle <b>Russell Square.</b> The manager at the scene reported that there were 40-50 walking wounded and 100 stretcher cases still in the tunnel. There was still only one ambulance on the scene at that point.		
10:14 AM				
10:15 AM	London Bus Control centre called to request that walking wounded be sent to Bart's			
10:22 AM	<b>Russell Square.</b> An equipment vehicle was requested.	<b>Kings Cross.</b> Four busloads of casualties were taken (by bus drivers who had taken the impressive individual initiative of offering their services) to The Royal London Hospital. They were directed to the Royal London Hospital, despite a call to the control centre seven minutes earlier requesting that walking wounded be sent to Bart's instead.		<b>Interface to non-first responders</b> (see Section 4.3.4).
10:27 AM	<b>Russell Square.</b> The manager at the scene requested an estimated time of arrival of the ambulances that had been requested. There was no reply from Central Ambulance Control.	<b>Kings Cross:</b> No further information was recorded about the Ambulance Service's response at King's Cross, other than the time at which the scene was cleared of casualties – 2 hours and 26 minutes after the explosion.	<b>Kings Cross:</b> The London Ambulance Service manager at the scene reported that there were still 50 people trapped in the train.	
10:30 AM		A system exists to restrict mobile phone network access to the emergency services within a specified area. This system, called the Access Overload Control (ACCOLC) is seen very much as a last resort. It is expensive to implement and can cause public distress or panic. The decision to activate ACCOLC can		Several possible CR-based approaches to improve response: <ul style="list-style-type: none"> <li>○ <b>Temporarily reconfigure responder radio priorities</b> (see Section 4.3.2).</li> <li>○ <b>Dynamically access additional spectrum.</b>(see Section <b>Error!</b> <b>Reference source not found.</b>).</li> </ul>

Time/ Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
		<p>therefore be taken only at the highest level of command: the Gold Coordinating Group.</p> <p>The first meeting of the Gold Coordinating Group, considered whether to close down mobile phone networks to the public at any of the sites where the emergency rescue effort was being mounted. The London Ambulance Service told us that problems with mobile phones and radios led them to ask the Gold Coordinating Group to activate ACCOLC in the area around Aldgate station, and that their request had been refused by the Gold Coordinating Group. It was decided that ACCOLC should not be activated, because of the risk of public panic and also because it was not clear that the right personnel would be carrying ACCOLC-enabled telephones.<sup>18</sup> If they were not carrying this equipment, ACCOLC could have made matters worse. As it was, at least some mobile telephone calls were getting through some of the time. Had ACCOLC been activated, key personnel who were not carrying specially-enabled telephones would not have been able to make or receive any calls. This is clearly a major flaw in the system: there is no point in having the technology to enable key people to</p>		

<sup>18</sup> Transcript of Committee meeting, 3 November 2005, Volume 2, pages 24-25

Time/Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
		communicate with each other if the relevant authorities do not make sure that the right people are in possession of that technology.		
10:45 AM				
11:00 AM				
11:15 AM				
11:30 AM				
11:31 AM		<b>Tavistock Square.</b> The tactical, or 'Silver', officer at Tavistock Square reported that they had enough vehicles. It turned out that this was the result of ambulances destined for Russell Square being directed to the same muster point as those dispatched to Tavistock Square.	☒	
11:45 AM				
12:00 AM		ACCOLC had been activated, by the City of London Police, on the O <sub>2</sub> network in a 1km area around Aldgate Station. This was a response to the fact that the City of London <b><u>Police were experiencing serious communications difficulties in the area</u></b> , and this was hampering their response. Despite the Gold Coordinating Group decision, the City of London Police made a request to O <sub>2</sub> to shut down the O <sub>2</sub> network to the public in a 1km area around Aldgate station. O <sub>2</sub> carried out the appropriate validation procedures, but these procedures, set by the Cabinet Office, do not include verifying the request with the Gold Coordinating Group. The O <sub>2</sub> network was	☒	<p><b>Dynamically access additional spectrum.</b>(see Section 4.3.2<b>Error! Reference source not found.</b>).</p> <p>Not clear what was causing problems, but improved spectral efficiency possible through cognitive techniques could alleviate congestion.</p>

Time/ Event	PS Response	On-scene Problems / Situation Awareness	Communication Activity	Potential Cognitive Capability
		<p>therefore closed to the public – outside the command and control structure - at about noon, and remained closed down until 4.45 pm. During that period of time, O<sub>2</sub> estimates that ‘<i>Several hundred thousand, possibly maybe even more than a million</i>’ attempted calls by members of the public were lost.<sup>19</sup> Tavistock Square. The London Ambulance Service manager at the scene reported that the remainder of the casualties still needed to go to hospital.</p>		
12:12 PM	<p><b>Russell Square.</b> The scene was clear of casualties.</p>			<p><b>Switch protocols to balance load or allow additional access</b>          As part of the analysis performed for this document, it is noted that the other protocols such as WiFi, WiMax were unavailable so this use case is not being addressed at this time.</p>

1

<sup>19</sup> Transcript of Committee meeting, 1 December 2005, Volume 2, page 88