

RESILIENT TELECOMMUNICATIONS: STRATEGY FOR ENHANCING THE RESILIENCE OF EMERGENCY RESPONDERS' TELECOMMUNICATIONS

INTRODUCTION

1. Telecommunications are a fundamental enabler to the effective response to any emergency. But experience during a number of recent emergencies in the UK (e.g. the BT plc tunnel fire in Manchester, April 2004; floods in Boscastle, August 2004; flooding at Carlisle, January 2005; the bombings in London, July 2005) showed that there were potentially significant weaknesses in current arrangements which needed to be better understood, the implications evaluated and remedies proposed. This paper summarises the current position and sets out the strategy for putting in place telecommunications capabilities that are resilient in the face of the most severe civil emergencies.

THE CURRENT POSITION

2. There is no coherent approach across the emergency responder community to enhancing the resilience of telecommunications provision. Likewise, knowledge of the issues involved and the alternatives available varies considerably between responder organisations. Among some Category 1 responders under the Civil Contingencies Act, particularly outside the blue light services, there can be limited ownership of the problem despite the statutory responsibility on all Category 1 responders to ensure that they are able to deliver their key functions in an emergency, with resources most frequently cited as the reason.

3. The three existing privileged telecommunications services (Airwave; ACCOLC; and GTPS) are managed independently of each other with little or no read-across between them and limited awareness of, and transparency over, entitlement to access. There is significant concern over the utility of GTPS, the take up of ACCOLC and the capacity of Airwave.

4. There are known capacity limitations on some systems, especially mobile telephone networks, which place limits on their ability to handle the significantly higher levels of traffic that might be expected in a major emergency. And other systems are not, or not yet, resilient against some of the expected impacts of severe emergencies, especially the widespread loss of electricity or of core circuits.

5. At a strategic level, we cannot therefore be confident that in an emergency key decision makers in COBR could communicate with the Police gold commander, relevant Regional Director in England and / or lead ministers in the Devolved administrations.

AIM

6. The Aim of this Strategy is to:

Ensure that emergency responders at all levels can communicate and share information effectively in a major emergency.

OBJECTIVES

7. This Aim is supported by the following Objectives:

- a. *Encouraging a diversity of telecommunications provision, so that emergency responders are not reliant on a single system.*
- b. *Making telecommunications networks likely to be used by emergency responders more resilient against the anticipated impacts of major emergencies, including by exploiting those networks which have the highest degree of embedded resilience.*
- c. *Ensuring that emergency responders know about privileged telecommunications services, and that such services function effectively in a way which meets their operational needs.*
- d. *Making information available on the take-up of privileged services.*

PLANNING ASSUMPTIONS

8. This Strategy draws from the National Risk Assessment and associated National Resilience Planning Assumptions a set of tailored planning assumptions to inform the range of consequences (at Annex A) which emergency responders' telecommunications should be resilient against. The underpinning Resilient Telecommunications Programme to deliver this Strategy will reflect a key judgement that the likelihood of all these consequences combining is comparatively relatively small.

DELIVERY

9. There is no one simple solution. Experience suggests that, however much is spent on enhancing its resilience, reliance on any one telecommunications system carries a significant inherent risk. It is principally for this reason that this Strategy is founded on the principle of diversity, and the adoption of a layered fall-back approach.

10. Telecommunications are rapidly becoming a commodity. There is a wide choice of physical infrastructures and services run over them, offered by a large number of private providers. That said, the apparently wide choice disguises much inter-dependency on basic infrastructures and services which works to the detriment of resilience. Because of the close integration between telecommunications infrastructures, those that are truly independent of commercial core infrastructures

command a premium. When the risk of wide-scale unavailability of commercial infrastructures is taken into consideration, it is difficult to justify significant expenditure on duplicate systems that may only rarely, if ever, be used.

11. The key to enhanced resilience is thus founded on encouraging and supporting a better understanding among responders of the systems available to them and their respective strengths and weaknesses; enhancing the resilience of existing systems wherever possible, ensuring that where high-integrity infrastructure is warranted it is regularly used; and greater inter-agency planning to enhance mutual aid and interoperability.

12. The Strategy therefore comprises four broad strands:

- a. Working with providers and responders to **enhance the resilience of every-day commercially-available telecommunications**.
- b. **Improving the management, take-up and resilience of privileged telecommunications schemes** that are accessible only to emergency responders.
- c. **Delivering a high-integrity telecommunications backbone infrastructure** providing connectivity and services between the main multi-agency co-ordination centres at the UK, national, regional and local levels.
- d. Developing a means for **securely sharing information between all local, regional and national responders** both in preparing for and in response to a major emergency.

Strand 1 - Enhancing the resilience of everyday telecommunications

13. Arguably the most important step in enhancing resilience is to help ensure that emergency responders avail themselves of the best possible value from commercial telecommunication services. This strand is itself made up of three elements:

- a. Awareness raising among responders.
- b. Working with service providers.
- c. Promoting inter-agency co-operation.

14. Steps have already been taken to raise awareness through newsletters, workshops and interim guidance. Comprehensive advice has also widely distributed amongst responders, and published on the *ukresilience* website. Relevant courses at the Emergency Planning College have been reviewed and extensively revised. In view of the importance of communications in responding to emergencies, and to bring all this together, each Local Resilience Forum has been advised to establish a communications sub-group, responsible for considering all aspects of communications, including the technical means, and how resilience might be

enhanced within its area. Finally, the Electronic Communications Infrastructure – Resilience and Response Group (ECI-RRF) has an arrangement in place, referred to as NEAT (the National Emergency Alert for Telecommunications), for responding to emergencies affecting telecommunications in the UK. These arrangements are tested annually.

Strand 2 - Improving the management, take-up and resilience of privileged telecommunications schemes

15. Privileged communication schemes are those where access is restricted to those with a role in the response to a major emergency. Work to implement this Strategy will seek to introduce a common framework for entitlement to and management of these schemes:

- a. Privileged access to the fixed-line telephone system.
- b. Privileged access to mobile telephone networks.
- c. Access by those outside the Emergency Services to mobile communications using TETRA-based systems (i.e. Airwave and possibly other similar services if these become available).
- d. Commercially-available satellite communications equipment made available to responders through a Cabinet Office-negotiated catalogue of services.

16. Access to these schemes will be managed through a master entitlement list setting out those responders who are, in principle, entitled to access privileged services. Narrower criteria will be laid down for specific privileged services where there may be capacity or other factors limiting the numbers able to take up particular services. Arrangements will be put in place with relevant service providers to ensure that management information is provided regularly to the responder community so that take-up can be monitored and emerging gaps identified and addressed.

Strand 3 - Delivering a high-integrity telecommunications backbone infrastructure

17. While it is difficult to justify substantial expenditure on the installation and maintenance of fall-back systems for what are very low probability (or combined probability) events, this needs to be balanced against the risk that key decision-makers are unable to communicate in the most catastrophic emergencies.

18. The armed forces have dedicated, resilient telecommunications capabilities that could be deployed to support civil authorities. This Strategy includes a delivery strand based on the installation of a limited infrastructure offering a high degree of assurance of the continued ability to communicate and share information at up to RESTRICTED level even against the planning assumptions listed at Annex A. It is intended that such a network should connect:

- a. COBR and its alternates (3 locations).
- b. The main government departments likely to have a significant role in an emergency (13 locations).
- c. Regional co-ordination centres in England (9 locations).
- d. Primary Strategic Co-ordination Centres (42 locations) in England.
- e. The Devolved Administrations in Scotland, Wales and Northern Ireland (3 locations).

19. Such a network (shown schematically at Annex B) could, subject to available funding, be extended to cover fallback locations, taking the total to some 200 locations. Connection would be dependant on individual sites meeting criteria for their ability to sustain operations in a severe emergency, including standards on the availability of back-up power supplies and geographic location away from flood plains.

Strand 4 - Sharing information between all responders

20. The effective preparation and response to an emergency is currently hampered by limitations on the ability of the wider responder community to share information effectively. Some local responders have already implemented multi-agency extranet-like systems at a local level. But the coverage of such systems is far from comprehensive and there are no agreed standards in place covering their functionality. The inability to seamlessly share protectively marked information is a significant constraint.

21. To meet these needs, this Strategy includes work to develop a '*Resilience Extranet*'. This would be a web-based system to facilitate the sharing of information (to RESTRICTED level) by those preparing for, and responding to, major emergencies at and within local, regional, national and UK levels. It is intended that it should be accessed over a secure, GSI-accredited network, thus allowing it also to provide a common repository for key documents (i.e. it acts as a secure equivalent to the *ukresilience* website) and optional functionality such as GIS mapping. The Extranet will be hosted on a resilient server in line with best practice for physical and data security. As far as possible, it will be administered by each organisation taking responsibility for its designated users. Essential central administration will be undertaken, as appropriate, by an appointed administrator or, in the case of Devolved Administrations, by the relevant Administration. Technical administration and support will be provided by the supplier.

Civil Contingencies Secretariat,

April 2007

RESILIENT TELECOMMUNICATIONS PLANNING ASSUMPTIONS

Arrangements ultimately need to be resilient against:

- a. **Large-scale, temporary absence of staff.** Up to a cumulative total of 25% of staff absent across an organisation for a 3-4 month period, with levels of absence from work peaking at 15%, perhaps double this level for small teams. These figures may increase if, during a flu pandemic, schools close or if a large proportion of staff care for dependants.
- b. **Permanent or long term absence of staff.** Loss of several hundred staff through death or serious injury resulting from damage to key sites.
- c. **Denial of access to site or geographic area.** Up to 40,000 properties inaccessible in a single geographic area for seven days due to widespread flooding. Smaller numbers of properties may be inaccessible for much longer as a result of, for example, industrial accidents or terrorist activity.
- d. **Disruption to transport.** Significant disruption to domestic road and / or rail transport for 10 days; significant disruption to localised networks and / or infrastructure for up to 1 month.
- e. **Loss of mains water.** Mains water supply denied across a substantial part of the country for up to three days due to a failure of the electricity supply.
- f. **Loss of mains electricity.** Complete UK-wide loss of mains electricity, taking three days to restore power in all areas to the national grid. There may under other scenarios be widespread loss of power within a region for up to 10 days.
- g. **Loss of availability of oil and fuel.** Complete cessation of fuel distribution within the UK, which would exhaust current supplies after 48 hours. After the incident is concluded, it may take up to 10 days to fully restore supply.
- h. **Loss of telephone / mobile communications.** Regional unavailability of the PSTN. Loss of the PSTN and dependent systems for 100,000 customers for up to three days.

- i. **Non-availability of IT services.** Loss of IT services, including loss of access to the GSI for up to three days with possible corruption of data not backed up in a resilient manner

SCHEMATIC REPRESENTATION OF THE HIGH INTEGRITY TELECOMMUNICATIONS INFRASTRUCTURE

