TI-EPF ™

Telecommunications Industry
Emergency Planning Forum
Protecting communications

Telecommunications Networks – a vital part of the Critical National Infrastructure

Version 1.0

Telecommunications Networks – A Vital Part of the Critical National Infrastructure

CONTENTS

Executive Summary

This document explains how the UK's telecommunications networks are a vital component of the country's Critical National Infrastructure, the ways in which resilience in both networks and services is achieved and the roles of government and other agencies in the maintenance of this capability.

This document contains information for all those who need to have a basic understanding of the electronic communications environment, ranging from Senior Information Risk Owners (SIRO's), Business Continuity Managers and Emergency Planners in central, regional and local government as well as businesses part of the CNI.

Recently, telecommunications has been going through radical change. Many of these changes are being influenced by the convergence of technologies, particularly computers and telecommunications, as well as broadcast, the internet and other information services. This convergence of technologies, has led to the era of the Information Society. It has always been acknowledged that telecommunications is essential for the economic, social and cultural development of society, but that requirement has become even more evident as the Information Age is increasingly recognised as the future of all societies.

From a regulatory perspective, the European Directives are encouraging a free market approach and the UK regulator Ofcom recognises that this approach will bring new services, technologies and opportunities for increased innovation and potential for competition leading to reduced costs.

There are regulatory obligations on electronic communications providers in relation to resilience and emergency planning; for the wider market there are duties and powers provided through a number of different pieces of legislation. However, the industry has shown its ability to work with government on a voluntary basis to improve emergency planning arrangements. These plans are well developed and regularly tested.

Most central and local government telecommunications systems are today provided by the industry, and there is a requirement for customers of these services to have some form of understanding of how the UK Telecom Network functions. This document aims to fulfil this need.

Introduction

The telecommunications industry contributes around 4-5% of the country's Gross Domestic Product (GDP) and might therefore be considered of relatively minor importance to the country.

However, its own GDP does not reflect the wider importance that telecommunications plays in the economic and social well-being of the country. Almost every UK business is dependent on telecommunications to transact business, as is every branch of central and local government and related public bodies.

The social life of the country is highly dependent on telecommunications too, be it the capability to broadcast TV to every home, for friends to 'text' one another to arrange their appointments or for anyone to summon the emergency services via 999. The defence and security of the nation is also highly dependent on reliable communications. Telecommunications therefore has a 'multiplier' effect and its importance to the overall continuity of life and the democratic tradition of this country is immense. Such is its importance that governments have recognised that the issue often transcends the narrower commercial interests of the companies who supply services and therefore government has some duty to assure the resilience of the country's telecommunications systems and services.

For many years prior to 1984, telecommunications was run by the government as a statutory monopoly. It could ensure that the General Post Office (GPO) took due account of the requirement to serve the country in an appropriate way, with adequate provision for the resilience of the system. Since 1984, not only has telecommunications been provided in an increasingly competitive commercial environment, but also a much wider range of services has become available – and come to be relied on – such as mobile phones and the Internet. Government now has to proceed partly based on supporting statutes, but to a large extent by voluntary cooperation by the industry.

Critical National Infrastructure

The importance of telecommunications resilience is reflected in the fact that government has identified telecommunications as one of the top 10 sectors deemed to be part of the 'Critical National Infrastructure' (CNI). The government views the CNI as those assets, services and systems that support the economic, political and social life of the UK whose importance is such that any entire or partial loss or compromise could:
- cause large scale loss of life
- have a serious impact on the national economy
- have other grave social consequences for the community
- be of immediate concern to the national government

Telecommunications fits with each of these 4 points.

Chapter 1

The nature of the UK's telecommunications networks

1. Before explaining the threats to the UK telecommunications capability and the means of mitigating those risks, it is important to understand the nature of telecommunications networks and the kinds of company that now provide those networks and/or the services running over them. Those familiar with telecommunications networks may wish to skip to Chapter 2.

2. The fundamental principle of telecommunications is the ability to transmit information over a distance. Transmission systems comprise three elements:

   - A Transmitter;
   - A Transmission Medium; and
   - A Receiver

3. The Transmitter converts the information into a form of energy appropriate to the Transmission Medium in use and injects that energy into the Transmission Medium. The Transmission Medium conveys the energy over a path to the Receiver. The Receiver converts the received energy into a form suitable for use at the receiving location, thereby creating a distant replica of the original information. Although TV signals are broadcast one-way out towards viewers, most transmission systems are bi-directional, allowing conversation and interaction between 2, or sometimes more, parties.

4. All forms of telecommunications use different types of electro-magnetic energy and the principle types of transmission media are:

   - Electrical signals over metallic wires;
   - Radio waves through the air and space;
   - Light signals through optical fibres

5. All of these are different forms of electro-magnetic energy, but differ widely in the frequencies of the signals used. The list is not exhaustive, for example, low frequency short range magnetic coupling is used for systems like hearing aid loops for the hard of hearing and infra-red light is used to communicate between our TVs and their remote controls. Though these technologies aren't used for public networks, they are all forms of telecommunication.

6. In order to understand the role that individual transmission systems play within the telecommunications network, it is useful to describe the overall structure and use of the network.

7. A telecommunications network comprises two main parts:

- The core network, comprising a large number of buildings (mostly telephone exchanges) connected together by transmission systems;
- The local or access network comprising copper and some fibre cables connecting individual customer premises into the core network at the local telephone exchange building.

Although BT's network is the largest and serves the entire country' each telecommunications network company has its own core network and its own access network,. However, it is impractical for other competing operators to completely replicate the scale of BT's network, so they may rely on acquiring capacity or facilities from BT or other operators in order to construct their desired network. So a competing operator may construct its own small fibre network connecting the major cities and rely on other means to connect to areas and customers 'off-network'. Many operators start by constructing a 'figure of 8' network connecting, typically, London, Bristol, Birmingham, Manchester and Leeds; paralleling the early deployment of both canals in the 18th century and railways in the 19th century.

A core network of exchanges connected by a mesh of fibre optic cables
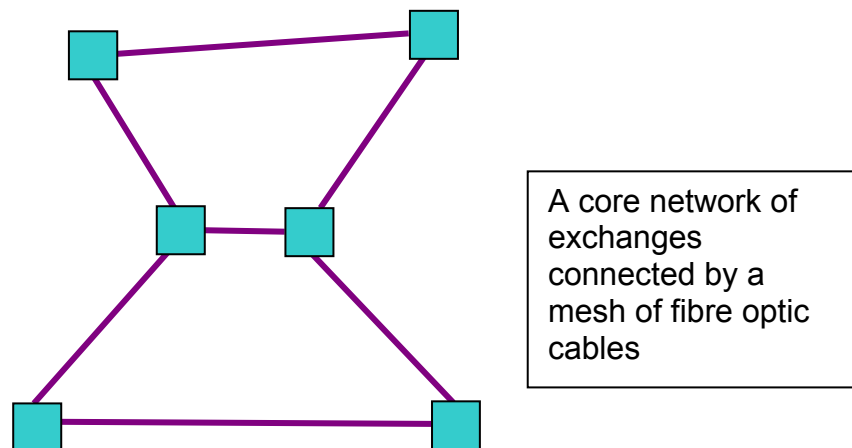
Figure 1: A small core network

The core network

8. In the core network, the most usual transmission medium is optical fibre, which comprises a length of very pure glass, about the thickness of a human hair, capable of carrying light signals over a considerable distance (100s of kms). Other transmission media are sometimes used, such as microwave radio or satellites. In the case of optical fibre, the transmitter consists of a laser which generates a strong pure light source, while the receiver consists of a light detector which indicates the presence or absence of light signals. The fibre optic system works by rapidly switching the light source on and off, many millions of times a second, thereby producing a system capable of conveying a digital information stream, that is, a stream of signals representing the binary states 1 and 0 (on/off). Information, be it voice, video or data is coded into a digital form prior to transmission. Individual fibre strands are protected by a plastic sheath and then bundled together in groups of between typically 24 and 96 to form a fibre cable, with its own outer

sheath and strengthening core. Each strand is isolated from the others and capable of separate use.

9. Sometimes the network of cables is organised into sets of discrete hierarchical rings and sometimes in a less structured mesh. At the ends of the fibre systems, including those at points round the ring structures, the light signals are converted back into electrical signals and connected to a multiplexer. The function of the multiplexer is to allow many separate individual circuits (which may be carrying individual telephone calls or private circuits) to share the capacity provided by the individual fibre. This is possible because the fibre cable may provide for, say, 10 Gigabits per second (Gbit/s) to be conveyed, whereas a single telephone call only occupies 64kbit/s. Such a system could therefore convey over 150,000 separate simultaneous calls. This capacity sharing is achieved by the technique of Time Division Multiplexing, whereby each call or circuit is allowed in turn to transmit 8 bits on the fibre every 125 micro-seconds.

10. The BT core network comprises around 5500 telephone exchanges connected together by fibre optic systems. This extensive network then connects to around 350 buildings where regional and trunk networks are focussed.

11. Other core networks are much smaller and may only use about 5-40 exchanges and a few hundred 'points of presence' where connection from customers is made via their own access circuits or by renting circuits from other operators. A diagram of a typical smaller network is shown at Annex 1. Such smaller networks often reflect the company's focus on business customers in major cities.

The local or access network

12. The purpose of the local or access network is to connect individual customers to the nearest suitable point on the corer network, often the local telephone exchange. There are three broad types of access network:

　　a. BT's network, covering virtually every home and office in the country and largely made up of copper cables, but with fibre links for serving larger businesses;

　　b. Competitor networks focussing on business customers, almost exclusively comprising fibre cables, with some use of microwave radio;

　　c. The Cable TV company networks, which also provide telephony and other telecom services, which comprise a hybrid network of fibre cables with final delivery via copper coaxial or pair cables.

13. The BT access network mainly comprises copper cables stretching from the telephone exchange out to individual homes and offices. It is structured in a 'tree and branch' manner, with very large cables, of up to 4800 copper pairs, extending from the exchange Main Distribution Frame (MDF) through underground ducts, to roadside cabinets, known

as Primary Cross-connect Points (PCPs). At the PCP, individual copper pairs are cross-connected to others in smaller cables that then radiate out to many individual Distribution Points (DPs). A DP will typically be sited at the top of a telephone pole or within larger office buildings. From the DP, individual copper pairs are delivered to each home, in the case of a telephone pole sited DP, this will be via a drop-wire, strung between the pole and the home. The pair of copper wires is often called the copper loop. The figures below show how a customer's home is connected to the network and the overall topology of the access network.
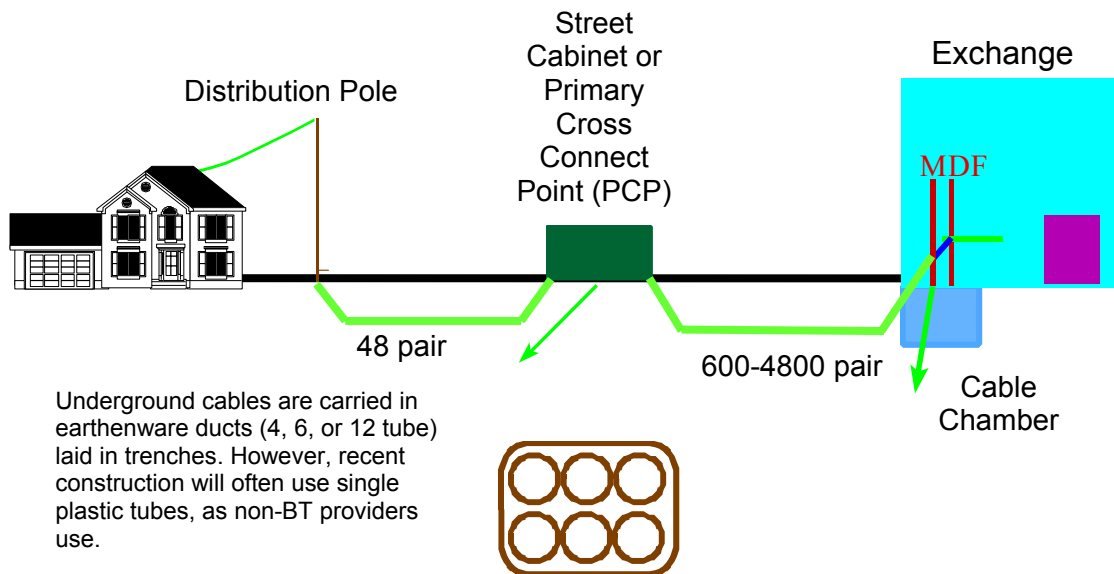
Figure 2: Typical layout of a local access network

14. The outcome of this structure is to provide for every customer a pair of copper wires that act as a single pair of electrical conductors from their abode to the telephone exchange building, where they are terminated on the Main Distribution Frame (MDF). From there, the pairs are connected either to the telephone exchange equipment or to other telecommunications apparatus provided for other types of service, such as data services or private circuits.

15. In the case of large office buildings which have large demands for telecommunication services, fibre cables may be provided instead of copper, as the revenue may justify the higher capital expenditure.

16. An important distinction between the core network and the access network is that the former comprises mainly high capacity transmission systems shared across many types of use, while the latter is mainly low capacity wires, each dedicated to a single customer.

17. The other business focussed companies (e.g. Cable & Wireless, Energis, VERIZON BUSINESS, Thus, COLT, Affiniti, Your

Communications) may have extensive own-build access fibre networks in London and other major cities, but typically will otherwise provide their own fibre access links to customers only where the demand justifies the bespoke construction. Unlike the copper pairs used to deliver a single telephone line, these fibre cables, like those used in core networks, can handle many separate circuits and services and generate much higher revenues, often for corporate data services rather than plain telephony.

18. In March 2006 ntl and Telewest completed a merger creating the UK's largest residential broadband communications company delivering both television, broadband and telephony to about 50% of UK homes (though take-up is less than this, around 12%). Their access networks use a combination of fibre to the street cabinet then a mixture of coaxial cable to carry TV and copper pairs for telephony from the cabinet to the home.

Cable TV Head-End & Exchange
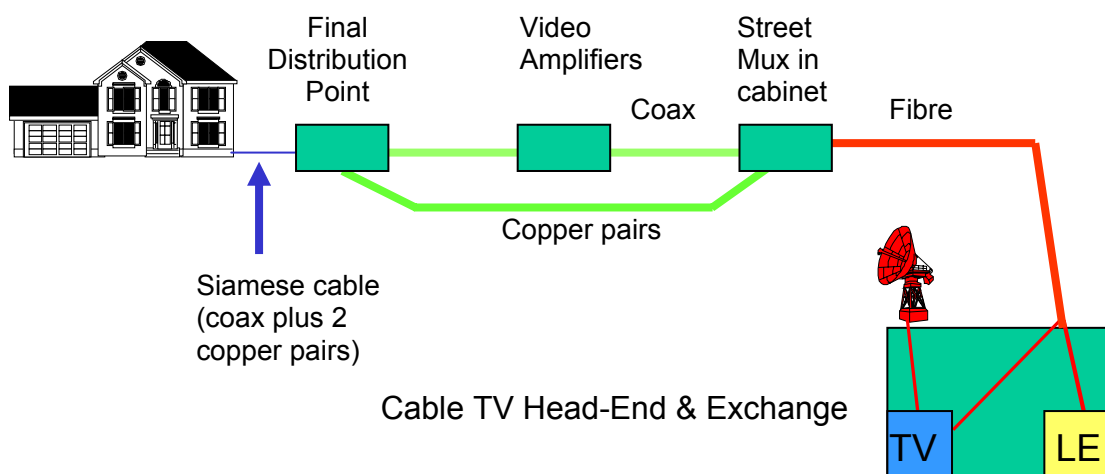
How a telephone call is connected

19. The following brief description is given of how a telephone call is established..

20. The call is initiated by the caller lifting the handset which causes current to flow round the copper pair loop and this is detected at the telephone exchange. The wanted number is dialled and the exchange analyses the dialled digits to determine which direction the call is to be routed. The call will be extended by the exchange providing a cross-connection, for the duration of the call, from the local copper loop to a digital channel amongst many on a multiplexed fibre cable connected to the next exchange. Successive exchanges repeat the routing until the call reaches the local exchange of the wanted customer, where it will be connected to that customer's local copper loop and the bell rung. Different calls will take different paths through the network, but the routing through the local access network is always fixed, as each customer has a dedicated copper loop from his premises to a local exchange.

About 740 local exchange 'host' units in about 300 buildings

Approx 100+ tandem exchanges in about 80 major locations

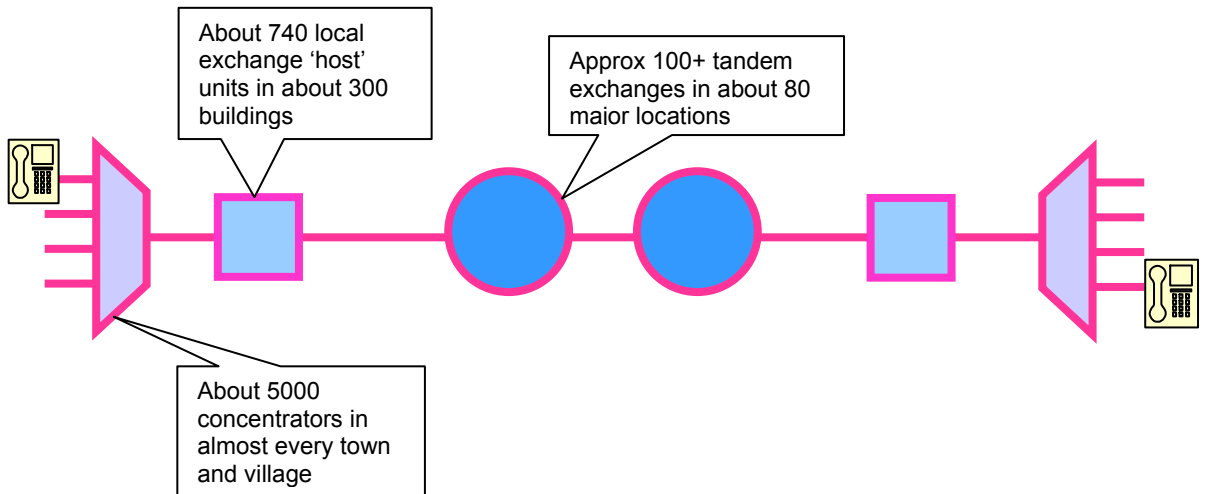About 5000 concentrators in almost every town and village

Figure 5: Telephone network architecture

21. In practice, the network is a little more complicated than this simple description. The local exchange to which customers are connected actually comprises two parts, a remote concentrator with limited functionality to which the copper loops are connected in over 5000 towns and villages and a more complex computer-controlled 'host' exchange located in the nearest principal town. The ~740 local exchanges are connected via a network of over 100 trunk or tandem exchanges located in around 80 major locations across the country.

22. Some operator's networks have far fewer telephone exchanges and in general do not use remote concentrators. The smallest companies have only a single switch 'layer'. Customers are connected via fibre or hybrid fibre/copper networks. However, the principle of stage by stage call establishment is the same.

Private Circuits

23. As well as providing a telephone network, the transmission network can be used to provide business customers with Private Circuits. A Private Circuit, unlike a telephone call, is not designed to connect from one point to any other; rather it provides a permanent connection between two specific end points, such as two branch offices. A private circuit is formed by connecting, on a semi-permanent basis, the local access circuit at one end to a path through the core network of multiplexed fibre cables until it reaches the distant exchange building, where it will be connected to the local access circuit of the far-end point. Unlike a telephone call which disconnects when the caller finishes the call, this connection remains held all the time, as long as the customer continues to rent the Private Circuit service. However, like a telephone call connection, while the routing through the access network is fixed, the routing through the core network can vary and may rapidly change in response to faults in the network or other planned rearrangements. This re-routing is performed by using electronic cross-connect equipments situated in exchange buildings. Furthermore, the Private

Circuit will be occupying capacity on the core network of multiplexed cables and sharing these cables with many thousands of other Private Circuits or channels used in the telephone network.
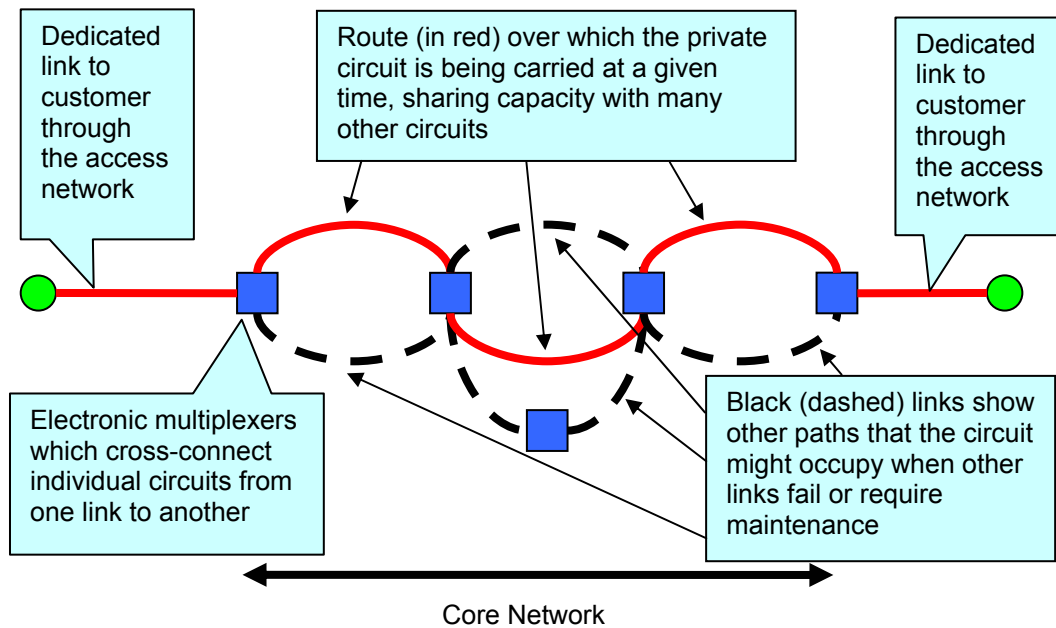
Figure 6: Typical arrangement and routing of a Private Circuit

Supporting others' infrastructure needs

24. Because Private Circuits provide transparent capacity between end-points, a telephone company may rent a Private Circuit service from another telephone company in order to provide the underlying transmission it needs to build its own network. For example, a mobile telephone company will rent Private Circuits in order to connect its radio base stations to its network of exchanges.

25. Alternatively, a company may acquire the right to use individual fibre strands in another company's cable. This is known as a 'dark fibre' lease.

26. Hence, many telecommunications networks are dependent on others and resilience may depend on the performance of several operators.

Mobile Networks

27. Mobile phone networks represent a special type of network which shares many attributes of fixed networks but several critical differences.

28. Like a fixed network, the core network comprises a network of telephone exchanges connected by fibre-optic cables. However the access network is quite different, comprising a set of Base Station Controllers and the many Base Stations themselves (the antenna sites) which then communicate with handsets using radio. Additionally, the core network has several databases, known as Location Registers which keep track of the location of handsets as they move around.
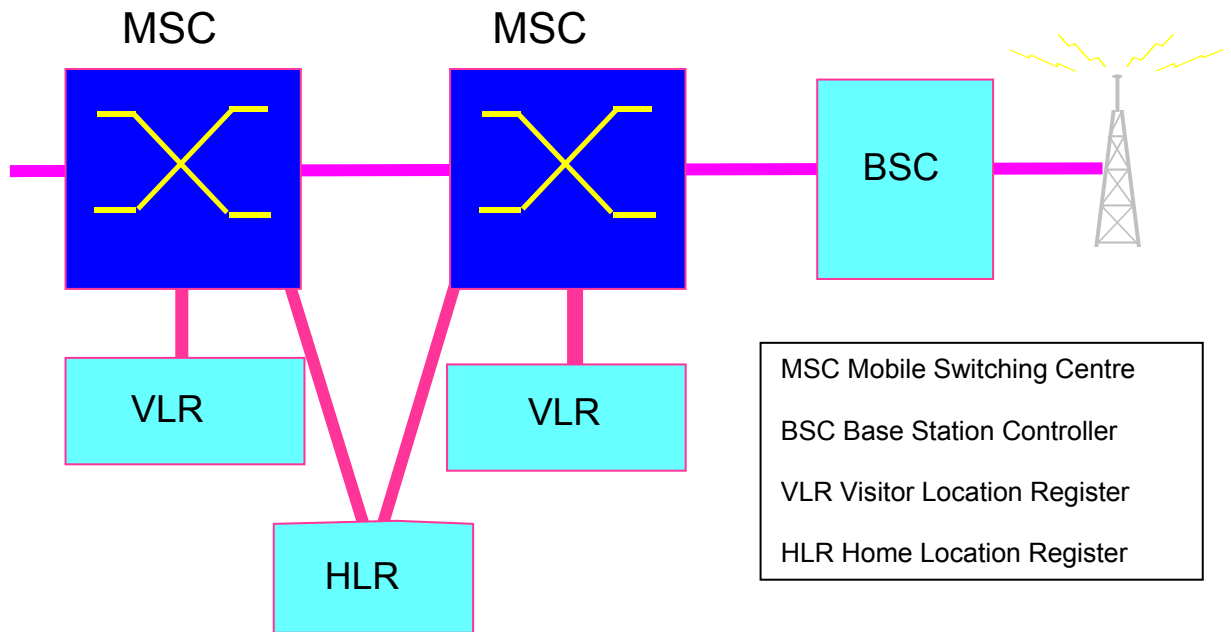
Figure 7: Typical mobile network

Internet

29. The Internet represents the other dominant form of network in use today. Since the 1970s there have been many types of data network deployed using a wide range of technologies and acronyms (e.g. X25, Frame Relay, ATM, SMDS, FDDI…). However, the development of the Internet, especially since its commercial exploitation from the early 1990s, has been dramatic and now IP (Internet Protocol) is not only the data network protocol of choice, but is likely to become the technology over which almost all forms of future network are built, including the traditional public telephone network.

30. It is important therefore to distinguish between the public Internet, which is a 'network of networks', all interconnecting with the same set of protocols and the use of IP technology to build entirely private networks ('intranets') and other managed IP networks which might be used for the provision of more robust public telephone services.
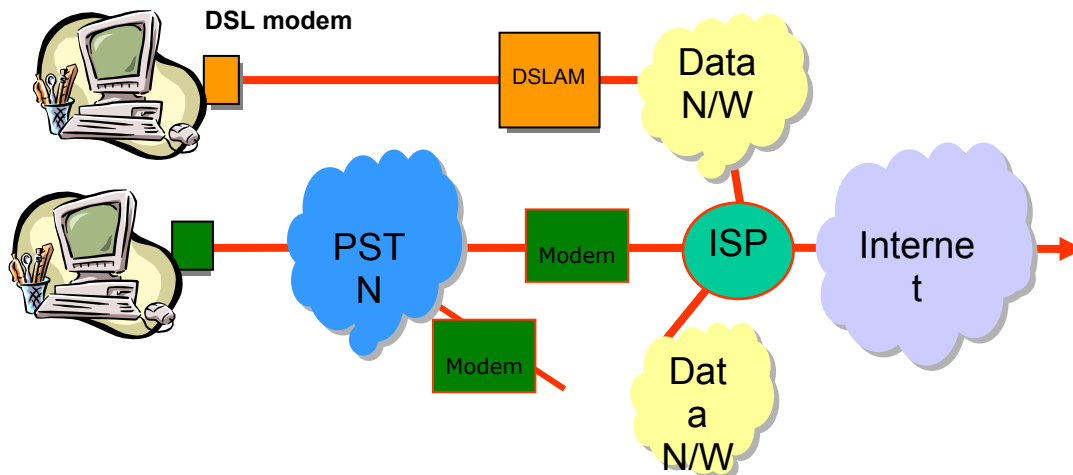
Figure 8: Accessing the Internet

31. Figure 8 shows how the Internet is accessed. The traditional narrowband method is shown at the bottom. The user dials up via the Public Switched Telephone Network (PSTN) to the customer's Internet Service Provider (ISP) via a modem. Data transfer rates of up 56kbits per second can be achieved in this way. A faster means of accessing the Internet, using a broadband connection, is shown at the top. Using either a Digital Subscriber Line (DSL) broadband modem or a Cable Modem, the customer is connected to the ISP via a DSL Access Multiplexor (DSLAM) at the exchange. Data transfer rates of 8Mbits per second are possible over a standard line operating alongside normal telephone use of the same line.

32. The Internet itself is a set of ISP networks and non-commercial IP networks which connect to one another, sometimes directly, but more often via so-called Neutral Access Points (NAP), the main UK NAP being the London Internet Exchange (LINX). Some smaller ISPs, which lack the connectivity of others, buy access from larger ISPs, but the bigger ISPs continue to interconnect by free mutual 'peering'. Some ISPs have no network of their own and resell the services of others. Such 'virtual ISPs' include names like Virgin and Arsenal Football Club.

Chapter 2

Types Of Telecommunications Companies In The UK

1. Since opening up the telecommunications markets to competition in the 1980s, a wide range of companies have entered the market and many have chosen to specialise in the kinds of network they have built and services they offer.

2. The largest telephone network remains that run by BT which reaches everywhere in the country (save for Hull, where Kingston Communications operates). BT and Kingston have the Universal Service Obligation, requiring them, in their respective areas, to provide telephone service on request to anyone who wants it.

3. Many of the other networks use the BT network to connect with each other, so they are still involved in the vast majority of calls made in the UK, even if they start on a cable or mobile network.

4. Since their emergence in the 1980s/90s, there has been considerable consolidation amongst the cable companies. Since 1991, the cable companies have exploited their right to offer telephone service as well as cable TV over their networks. There is one other cable company that provides telephone service. Tweedwind provides service in the Isle of Wight and parts of Cumbria, under the trading names of Isle of Wight Cable and Omne.

5. There are 5 mobile networks in the UK, run by Vodafone, O_2, Orange, T-Mobile and the new 3rd generation network operator known as '3'. There is also a specialist network operated by O_2, known as Airwave, which is used by the police, the fire service and in the future by the ambulance service (and in principle other essential public services) for their own internal radio communications.

6. There are a number of business-focussed telecommunications companies that have, to varying extents, built their own fibre networks. These include Cable & Wireless, Energis, VERIZON BUSINESS, Thus, COLT, Affiniti, Your Communications, Fibrenet and many other smaller enterprises.

7. Recognising that it's easier to build a core network, but harder to replicate an access network, a range of companies have entered the market providing so-called Indirect Access services. In its simplest form, a BT customer dials an access code of the form 1xxx followed by the wanted number. BT routes the call to the core network identified by the access number and the other company completes the call, including billing for it. A development of this service which has become very popular in the last few years, is Carrier Pre-Selection (CPS). With CPS, a BT customer opts to have all (or some) of his calls routed via a stated indirect access company, so that no access code has to be remembered or dialled. In case of problems, a CPS customer can use the access code 1280 to have BT route the call. With both Indirect Access and CPS, the customer still has to be a BT customer and pay

the BT line rental. Companies like Centrica (under both their British Gas and OneTel brands) are active in this market.

8. A further development of telephony competition is also now emerging, using 'Wholesale Line Rental'. This is often structured like CPS, but in this case, the competing company takes over the BT line and rents it on behalf of the customer, so that the customer only has a single relationship with the company.

9. The Internet service provision market has been competitive since it emerged in the early 1990s – the pioneers being Pipex and Demon (now owned by Thus). There are still hundreds of small ISPs in the UK, including many 'virtual ISPs', but there has been considerable consolidation and concentration in the market serving domestic customers. The main players are now AOL (whose network serving the UK is almost entirely in the USA), Wanadoo (mainly a virtual ISP running on the Energis network and now owned by France Telecom), BT, NTL and Telewest.

10. Broadband Internet is currently growing rapidly. Aside from NTL and Telewest's cable modem service on their own cable networks, most customers' broadband access is via their BT telephone line, using Digital Subscriber Line technology. BT carries the broadband connection over its own data network before handing over to the ISP serving the customer.

11. A few ISPs have invested in 'Local Loop Unbundling' (LLU), whereby they take over the BT line and use their own DSL equipment and data network to provide service. The most successful operator to exploit LLU is Easynet, although they only serve business customers.

12. A few companies offer Internet access via 'Fixed Wireless Access', notably Pipex and UK Broadband. 'Wifi' radio technology has also been used in a few rural locations to provide Internet access on a community self-help basis, though this technology has primarily been used for in-building networking (increasingly within the home) and for 'hotspot' services in airports, hotels and coffee shops.

13. As mentioned before, IP is becoming the dominant technology. Whereas in the past we dialled up over the telephone network to reach the Internet, some Internet companies are now realising that broadband Internet access can be used to provide voice services, though in many cases in a form quite unlike the traditional PSTN. Companies already well-known in this market include Skype and Vonage, but many more are now entering the market.

14. However, even mainstream telephone companies are expected to convert their public telephony networks to IP technology in the next decade. They won't use the Internet as such to route calls, but their own, more robust, managed IP networks. Such networks are often described as Next Generation Networks (NGNs) and their development will have implications for the resilience of the UK network.

Chapter 3

Threats To Continuity Of Service

1. We have become accustomed to the fixed telephone network always being 'up and running', even when our local electricity supply is lost. Indeed, this expectation creates frustration with the more recent mobile and Internet networks which have been built on a more commercially oriented basis.

2. All the major telephone companies have invested heavily in ensuring the reliability of their networks and the continuity of services running over them.

3. In this chapter, we will consider the many threats to continuity of service that companies need to take into account. In summary, they can be grouped into 5 headings:

   - Physical
   - Loss of key inputs
   - System/Logical failings
   - Software failures
   - Electronic 'interference'

Physical Threats

4. These include:

   - Natural phenomena (Extreme weather, earthquake, flood and lightning);
   - Fire
   - Explosions, in particular those caused by gas leaks;
   - Damage caused by accidents, vandalism, internal sabotage and terrorism.

Loss of key inputs

5. Telecommunications depends on the continuous availability of many 'key inputs', amongst which the most critical are:

   - Electrical Power
   - Fuel (for backup generators and vehicle fleet)
   - Human access (to operational installations)
   - Materials

6. Electricity, in particular, is the most critical input. Not only is the telecoms industry wholly dependant on electrical power, but the electrical power industry depends on telecoms to manage their extensive network of generators and grid distribution.

System/Logical failings

7. To prevent being vulnerable to the failure of a single part of the system, telecommunications companies will invest, where practical, in duplicate or triplicate back-ups for their equipment (redundancy) and diverse transmission routings. Thus the 'logical' architecture of the service will be more resilient than the simple physical layout. But sometimes, due often to human error, these logical configurations can themselves fail to provide the expected level of resilience. The key is to avoid, wherever possible, 'single points of failure'.

8. However, not all parts of the network can be made resilient and in these cases, the complementary processes of restoration and repair have to be strengthened.

Software failures

9. All telecommunications networks are reliant on software controlled equipment, and no software is immune from errors and operational failings. Unlike personal computers, it is not acceptable for a telecommunications network to crash and stop responding altogether.

10. A particularly worrying form of software failure is called a 'systemic' or 'common-mode' failure, where a software error in one network node causes the same fault to occur in other connected nodes, leading to a 'runaway' failure of an entire network.

Electronic 'interference'

11. Telecommunications networks, especially those increasingly using IP technology, can be vulnerable to conditions entering the system via the network itself. Increasingly, these can be malicious in intent.

12. A wide range of types of threat fall into this category, including:

- Inappropriate signals injected by users, either too high a voltage or at the wrong frequency;
- Similar signal pickup problems caused by radio interference, e.g. from amateur radio transmissions;
- Traffic overloads, often stimulated by advertising campaigns and TV based promotions;
- Denial of Service attacks – malicious attempts to damage a service, sometimes by traffic overload, sometimes by the transmission of 'malware' (malicious software);
- 'Malware', such as viruses, worms and Trojans;
- Hacking, including attempts to subvert the proper operation of the billing system in networks;
- The transmission of specifically crafted signalling messages, designed to cause misoperation of the network

Chapter 4

Resilience Measures Taken By Telecommunications Companies

1. Despite the long list of threats to which a telecommunications network is exposed, as described in Chapter 3, in practice, there are many mitigation measures that can be taken to reduce the risk that these threats can pose. Although no network can ever be totally 'non-stop', the performance of the UK telecommunications networks, especially the public telephone networks, are very high.

2. This is not the appropriate document in which to record all the possible and desirable counter-measures that can be taken, but the following gives a flavour of the typical ways in which the telecommunications networks are secured. Some residual difficulties are also mentioned.

3. Physical Threats: Exchange buildings are fitted with smoke, gas and flood detectors. Some buildings will be physically hardened and be fitted with CCTV monitoring. Building access is controlled by door entry systems which can record who have entered the building. Internal cellular security, as well as perimeter security may be used. Radio masts are designed to cope with high wind and ice-loading.

4. Loss of key inputs: Equipment will be secured against loss of electricity both by having a battery backup (which might support service for about an hour) plus a diesel generator designed to cut in when the public mains supply fails. Because the large majority of home telephones are powered by the telephone line itself, service can be provided even when the domestic electricity is cut off. (Some domestic phones, such as cordless phones and answering machines do need local mains power, however).

   Generator back-up is not practical to secure most mobile network base stations or street cabinets in cable networks. This means that in an extended electrical power outage, the mobile phone networks may become subject to failure. Equally, the phones themselves rely on battery recharging from the mains supply.

   The Fuel Crisis showed how vulnerable telecommunications operators are to loss of fuel, especially now that they no longer hold large bunker stocks of fuel. However, priority provision of fuel, alongside other essential services should suffice.

   Similarly, the Foot & Mouth crisis and events following city centre bombings have shown that if telecommunications staff are denied access to their installations, then they may be unable to assist the repair of equipment needed by other essential services. Again, recognising priority of access is needed.

   Many telecommunications companies hold as little stock of material as they can, according to modern 'just-in-time' provisioning principles. However, many make arrangements with their suppliers to hold emergency stocks on their behalf.

5. System/Logical failures: This is an issue that has to be designed-in from the start. For example each concentrator can have diverse routings to its host local exchange. Each local exchange is then typically connected to 3 tandem/trunk exchanges. Each trunk exchange is connected to every other. The result of this is that any two local exchanges have a multitude of possible paths over which calls can be set up, so the resulting network is extremely resilient to the loss of either individual trunk exchanges or the transmission systems connecting them. But any given customer will still be vulnerable to the loss of his concentrator or local exchange. For this reason, BT maintains a group of strategically positioned trailer-mounted exchanges which can be deployed where necessary for fast restoration. Similarly, replacement power equipment and generators can be deployed. All telephone exchanges also use duplicated computers and switch paths internally.

6. The UK Internet has not been planned as a single logical entity, which is both a strength and a weakness. The Internet can often reconfigure itself in times of outage. On the other hand, many parts of the Internet rely on just a few buildings (most in East London) where different Internet providers both site their equipment and make connections with one another.

7. Mobile networks are highly reliant on the fixed network operators to connect their base stations and exchanges together. Hence, the mobile network cannot be seen as a separate and alternative network to the regular public fixed network. A similar situation arises with the Internet, where the many smaller Internet Service Providers are dependant on others for their transmission. Hence the whole UK telecommunications infrastructure has significant elements of mutual dependency.

8. Software failures: Exchange equipment is designed to detect software which is not working properly, contain the problem and restart the offending sub-system. If all else fails, the entire exchange will automatically restart. So unlike personal computers, they never stop entirely. To avoid 'common mode' failures, some companies will deliberately use two types of equipment in their network from different suppliers, to avoid any 'domino failures'.

9. Electronic 'interference': It has to be realised that no network has enough spare capacity to cope with the increased demand for calls which occur during major incidents. Traffic overloads in telephone networks can cause major problems which can be avoided by invoking traffic management techniques, such as 'call gapping' which reduces the load on the system to one that can be safely managed. In some circumstances, priority access to the networks can be provided to ensure that appropriate public authorities can continue to function.

10. The Internet poses special threats because its original design concept was to provide a very open and transparent form of network. This means that all sorts of threats arise from inappropriate use or access of the Internet. Unlike the telephone network, which has physical separation of its customer connectivity and its control circuits, IP networks have only a logical form of separation and this is vulnerable to

'hacking'. Increasingly, IP networks are being protected by extensive 'firewalls' and progressively new protocols are being deployed to avoid the threats caused by the originally highly open nature of the Internet.

11. IP networks do have their own strengths, however. For example, because of the packetised nature of transmission and the fact that these packets may traverse different paths across the network, it is far harder to 'eaves-drop' on an Internet connection. Additionally, it is very easy to encrypt messages before they pass over the Internet.

12. Not all parts of the network can be secured and the single access line from the customer to the exchange is not capable of being protected from failure economically. So customers are encouraged, where they need higher than normal levels of security, to invest in two separated paths from their building, perhaps to two different telephone exchanges.

13. Telecommunications operators will invest in resilience commensurate with the risk to their commercial interests, including their reputations. In a competitive environment, where prices are constantly falling, companies will often switch from competing on price to competing on quality. Good resilience therefore becomes a competitive imperative. and many of the desirable resilience features that government will wish to see are often delivered by the operation of the market itself. But not always. In particular, the mobile and Internet industries have arisen from a quite different commercial culture than the telephony providers. The Internet is commonly described as a 'best efforts' network.

14. There are particular risks as telephone companies move towards the adoption of Next Generation Network IP technologies. The diversity of the present network may be reduced and switching will be concentrated in fewer nodes than at present. The telephone network could start to suffer some of the weaknesses described above relating to the wider Internet. Added to that, the introduction of any new software driven technology is likely to cause some instability before the inevitable software bugs are driven out.

Chapter 5

Statutory Provisions Concerning Telecommunications Resilience

There are a range of statutes that touch on telecommunications and in particular the issues of resilience, emergency planning and wider national security. Few of these provide clear powers to require all telecommunications providers to maintain the resilience of their networks and services. Furthermore, legal opinions within government are, to a degree, divided. Some measures have been put in place by the industry on the understanding that national security legislation could in the last resort be used to require it. Others, however, believe that such legislation can only be used for reasons directly relating to national security, i.e. the maintenance of public order and the democratic rule of law. While the loss major Critical National Infrastructure could in extremis become a matter of national security, it is less clear that national security legislation could be used to require all features that assist the maintenance of the commercial and social activities of the country.

The Communications Act 2003

This Act, which replaced almost all of the former Telecommunications Act 1984, is the primary legislation that set up Ofcom as the regulator for the broader communications industry and implemented the new European regulatory framework which came into force in July 2003. Instead of the former licensing regime of the Telecommunications Act, the new Act regulates communications providers by means of general authorisations which are required to be complied with as a condition of operating in the market.

In particular, Section 51 defines the subject matter that can be included by Ofcom in the general Conditions of Entitlement. Section 51(1)(c) specifies "conditions making such provision as OFCOM consider appropriate for securing the proper and effective functioning of public electronic communications networks" and thereby empowers Ofcom to implement Article 23 of the Universal Service Directive, entitled Integrity of the Network. It has done so through Condition 3 of the Conditions of Entitlement:-

---

3. PROPER AND EFFECTIVE FUNCTIONING OF THE NETWORK

3.1 The Communications Provider shall take all reasonably practicable steps to maintain, to the greatest extent possible:

> (a) the proper and effective functioning of the Public Telephone Network provided by it at fixed locations at all times, and

> (b) in the event of catastrophic network breakdown or in cases of *force majeure* the availability of the Public Telephone Network and Publicly Available Telephone Services provided by it at fixed locations, and

> (c) uninterrupted access to Emergency Organisations as part of any Publicly Available Telephone Services offered at fixed locations.

3.2 The Communications Provider shall ensure that any restrictions imposed by it on access to and use of a Public Telephone Network provided by it at a fixed location on the grounds of ensuring compliance with paragraph 3.1 above are proportionate, non-discriminatory and based on objective criteria identified in advance.

3.3 For the purposes of this Condition, "Communications Provider" means a person who provides a Public Telephone Network at a fixed location and/or provides Publicly Available Telephone Services at a fixed location.

Condition 3 only applies to providers of fixed telephony. It does not therefore provide for any regulation of the resilience of mobile or Internet services.

Condition 3.2 goes slightly beyond the requirements of Article 23, but continues a similar regulation contained in the old Condition 20 of the former licence for Public Telecommunications Operators which was in force until July 2003.

Oftel, the predecessor of Ofcom, produced guidance for the industry on what issues it expected should be considered when assessing whether companies were complying with Condition 20. These are known as the "Essential Requirements Guidelines" (published in October 2002) and while Ofcom no longer wishes to act as author of such guidance, the material is currently being revised as part of the Tripartite arrangements between the Cabinet Office, DTI and Ofcom.

In practice, while Condition 3 impacts all telephony providers, as with most regulation, there is no pro-active compliance checking. Compliance action has been restricted to events following a major network failure, for example, the Southampton outage of 2002 and the Manchester fire of 2004.

However, compliance to the 'Essential Requirements' Guidelines was made part of the voluntary elements within the National Emergency Plan for the UK Telecommunications Sector (see Chapter 7).

Emergency Planning

Section 51(1)(e) specifies "conditions requiring or regulating the provision, availability and use, in the event of a disaster, of electronic communications networks, electronic communications services and associated facilities" and thereby empowers Ofcom to implement conditions requiring providers to assist central and local government in times of emergencies. This is specifically allowed (though not mandated) by paragraph 12 of Annex A to the Authorisation Directive and continues previous obligations on Public Telephone Operators in their former licences.

---

5. EMERGENCY PLANNING

5.1 Subject to paragraph 5.3, the Communications Provider shall, on the request of and in consultation with:

> (a) the authorities responsible for Emergency Organisations; and

> (b) such departments of central and local government as Ofcom may from time to time direct for the purposes of this Condition,

make arrangements for the provision or rapid restoration of such communications services as are practicable and may reasonably be required in Disasters.

5.2 Subject to paragraph 5.3, the Communications Provider shall, on request by any person as is designated for the purpose in any such arrangements, implement those arrangements in so far as is reasonable and practicable to do so.

5.3 Nothing in this Condition precludes the Communications Provider from:

> (a) recovering the costs incurred in making or implementing any such arrangements; or

> (b) making the implementation of any such arrangements conditional upon being indemnified by the person for whom the arrangements are to be implemented for all costs incurred as a consequence of the implementation.

5.4 For the purposes of this Condition:

> (a) "Communications Provider" means a person who provides a Public Telephone Network and/or provides Publicly Available Telephone Services; and

> (b) "Disaster" includes any major incident having a significant effect on the general public; and for this purpose a major incident includes any incident of contamination involving radioactive substances or other toxic materials.

Oftel published under 5.1(b) a list of emergency planning bodies in county and unitary authorities, plus those central government departments with emergency planning responsibilities.

Providers are not expected to seek out such departments, but will be expected to respond appropriately when approached, either in advance, to plan for some future contingency, or at the time of an event, such as a local flood, storm etc.

The existence of this condition has assisted the voluntary production of the National Emergency Plan for the UK Telecommunications Sector (see Chapter 7).

Given that the previous licence condition only affected Public Telephone Operators, it was deemed appropriate to limit the class of provider to whom

this condition applies. However, by limiting it to telephone providers, it was realised after the event that it does not apply to the two major suppliers of transmission services to the broadcasters.

Section 132

Section 132 of the Communications Act provides powers for the Secretary of State to direct Ofcom to suspend, in whole or in part, the authorisation of a provider to provide networks or services, where he has reasonable grounds for believing that it is necessary to do so to protect the public from any threat to public safety or public health, or in the interests of national security. This is permitted by Article 3 of the Authorisation Directive and flows from over-arching powers of Member States under Article 46(1) of the European Treaty.

Powers to restrict or limit providers' services on the grounds of national security have existed since the very beginning of telecommunications. Prior to the new European regulatory framework, similar powers were included in SI 98/1580. As early as 1848, the Secretary of State used such powers to prevent Chartists from coordinating their nationwide protest activities using the telegraph system, which at the time was in private hands, using powers under the Electric Telegraph Act of 1846.

Cutting off communications in times of national crisis is quite common following coups and rebellions in other jurisdictions, but in today's society, with its loathing of censorship, it is difficult to see such powers ever being used in peace time. Additionally, the powers are of their very nature restrictive and do not provide for making orders for providers to provide positive assistance to the government in times of emergency.

Telecommunications Act 1984

As mentioned above, the Communications Act repealed almost all of the former Telecommunications Act of 1984, which had introduced competition, privatized BT and set up Oftel.

However, paragraph 70 of Schedule 17 of the Communications Act 2003 amended Section 94 of the Telecommunications Act and this remains one of the few sections of the former Act still in force. Section 94 allows the Secretary of State to give directions to providers of public electronic communications networks, or Ofcom, in the interests of national security, or of relations with a foreign country. The directions are to be laid before Parliament, unless the Secretary of State considers that disclosure is against the interests of national security, or of relations with a foreign country, or the commercial interests of some other person.   The Secretary of State has power to defray costs incurred in complying with any direction.

Civil Contingencies Act 2004

Part 1 of the Civil Contingencies Act establishes a clear set of roles and responsibilities for front line responders at the local level. Section 22 of Schedule 1 of the Act defines all network providers who supply telephone services to be "Category 2 responders". Such responders are required to

provide information to other emergency bodies and cooperate with them on making contingency plans for all kinds of emergency. There has been some concern that given the number of local committees to be set up to do this at a local level, that it would represent an undue burden on a large number of providers. In practice, providers are likely to represent one another so that the burden is shared and minimised. There have been other concerns that the duty to cooperate partly overlaps the obligations under Condition 5 as described above. Condition 5 does go further however, in that it requires that network providers not only plan but implement planned services on request.

See definition and list of Category Two Responders in ANNEX 2.

Other Statutes

Although outside the primary scope of this document, it should be noted that there are other Acts which impinge on communications providers and that the above does not therefore represent the totality of the statutory or regulatory burden on providers. In particular, in relation to national security and law enforcement for serious crime, there are two Acts that relate to obligations on lawful interception and the retention of communications data. Policy on these matters rests with the Home Office.

The Regulation of Investigatory Powers Act 2000 (RIPA)

Lawful interception can only be carried out through warrants issued by a Secretary of State to one of the 9 intercepting agencies listed at Section 6(2) of the Act. Communications Providers are required to provide assistance to these bodies when requested, subject to the request being reasonably practicable (Section 11).

The Anti-Terrorism, Crime and Security Act 2001

Implemented in the wake of '9/11', this statute, in Part 11, requires Communications Providers to retain communications data. However, it has not been formally implemented and data retention continues to be promoted and governed by a voluntary code of practice. Steps are currently being taken to seek a harmonized European approach to data retention requirements.

Limitations

It is important to recognise that some threats to the telecommunications network are global or external in character, so national legislation alone cannot solve everything. However, there is extensive cooperation amongst UK agencies with those in other countries with sympathetic objectives in respect of national security.

Chapter 6

Roles of Government Departments, the Regulator and other Agencies

Department for Trade and Industry (DTI)

The DTI has the primary policy responsibility for the telecommunications industry, including regulatory matters. The Cabinet Office, while being the main department for coordinating government policy on emergency planning, relies on a system of lead government departments to oversee the delivery of resilience within their areas of competence. In particular, DTI takes that lead role for telecommunications and ensures that appropriate resilience arrangements are in place. In practice, this is delivered through a Tripartite arrangement between DTI, the Cabinet Office and Ofcom, with support from specialist agencies such as NISCC and NSAC (see below).

Cabinet Office, Civil Contingencies Secretariat (CCS)

The CCS was set up in July 2001 to improve the UK's resilience against disruptive challenges through working with others to anticipate, assess, prevent, prepare, respond and recover. It defines resilience as the ability at every level - national, regional and local - to detect, prevent and if necessary handle disruptive challenges. These could range from floods, through outbreaks of human or animal disease, to terrorist attacks.

Its objectives are to:

- lead horizon scanning activity to identify and assess potential and imminent disruptive challenges;

- lead the delivery of improved resilience across Government and the public sector;

- ensure that the Government can continue to function and deliver public services during crisis; and

- improve the capability of Government and other stakeholders to prepare for, respond to and manage potential challenges.

Cabinet Office, Central Sponsor for Information Assurance (CSIA)

The CSIA works with partners in the public and private sectors, as well as its international counterparts, to help safeguard the nation's IT and telecommunications services.

Its broad focus is on safeguarding IT systems but also has a specific remit within the telecommunications area to identify and address vulnerabilities of national telecommunications systems and progress their resolution in conjunction with other government departments and organisations. CSIA also coordinates a range of services and facilities for use in emergencies, such the

Government's Emergency Communications Network, the Government Telephone Preference Service and its mobile counterpart ACCOLC (Access and Overload Control).

National Infrastructure Security Coordination Centre (NISCC)

Within the Government's broad role to promote the protection of the Critical National Infrastructure, NISCC's role is to minimise the risk to the CNI from electronic attack.

NISCC has no regulatory, legislative or law enforcement role; it seeks to achieve its aim through four broad work streams:

- Threat Assessment. Using a wide range of resources to investigate, assess and disrupt threats.

- Outreach. Promoting protection and assurance by encouraging information sharing, offering advice and fostering best practice.

- Response. Warning of new threats; advising on mitigation; managing disclosure of vulnerabilities; helping the CNI investigate and recover from attack.

- Research and Development. Devising the most advanced techniques and methods to support efforts across all work streams.

NISCC was set up in 1999 and is an inter-departmental centre drawing on contributions from across government. Defence, Central Government Policy, Trade, the Intelligence Agencies and Law Enforcement all contribute expertise and effort.

National Security Advice Centre (NSAC)

NSAC is part of the Security Service and contributes to the protection of key Government assets and the UK's Critical National Infrastructure (CNI), including telecommunications, and to the reduction of their vulnerability to terrorism and other threats. NSAC works with telecommunications providers identifying those parts of their systems which represent a significant risk to the CNI and can provide advice on physical and personnel protective security.

Office of Communications (Ofcom)

Ofcom is the regulator for the communications industry and assumed the powers of the former regulators (such as Oftel) in December 2003. Unlike Oftel, it is not a Government department, but a Public Corporation.

Ofcom's role includes ensuring compliance by providers to their Conditions of Entitlement, including Conditions 3 and 5 as described in Chapter 5. Ofcom investigates major failures within the telecommunications system and provides advice to DTI and the Cabinet Office as part of the Tripartite arrangements.

Chapter 7

Emergency Plans And Response Measures

However well telecommunications providers build their networks and systems, the investment in resilience will always reflect the perceived risks, the known vulnerabilities and the practicality of trying to protect assets against the increasingly uncertain modes of attack by malicious parties. It is therefore important that as well as building in resilience and other mitigating measures against risks, there should be clear plans and response measures should emergency situations arise.

Telecommunications providers have always worked with Emergency Planning organisations in both central and local government to deliver support for emergencies in the community.

Under CSIA's chairmanship, the Telecommunications Industry Emergency Planning Forum operates to two key documents:

- The National Emergency Plan for the UK Telecommunications Industry; and

- The Memorandum of Understanding for cooperation in emergency situations

There is also a non-disclosure agreement which protects any shared information from being passed outside the emergency planning community.

The Emergency Plan contains information on emergency contact points (which are regularly exercised), emergency scenarios (both those identified within the industry and those communicated from Government), management processes for handling emergencies and priority customers & services.

The Memorandum of Understanding allows the sharing of human and material resources amongst providers when required in an emergency.

The Emergency Planning Forum continues to oversee the maintenance of these documents and is working on further activities to identify risks and improve resilience.

Annex 1 – Typical core network of a smaller operator

This kind of network could be provided either by self-build or by acquiring dark fibre leases. In contrast, BT's core network reaches every city, town and many villages in the entire country and their access network serves almost every building.

Civil Contingencies Act 2004, Definition of Category Two Responder

22   (1) A person who provides a public electronic communications network which makes telephone services available (whether for spoken communication or for the transmission of data).

     (2) In sub-paragraph (1)-

      (a) the reference to provision of a network shall be construed in accordance with section 32(4)(a) and (b) of the Communications Act 2003 (c. 21), and

      (b) "public electronic communications network" shall have the meaning given by sections 32(1) and 151(1) of that Act.

List of Telecoms Category 2 Responders[1]

Company	Type of Service
Affiniti[2]	Fixed
BT	Fixed
Cable & Wireless	Fixed
COLT	Fixed
Global Crossing	Fixed
3	Mobile
Kingston Communications	Fixed
Level 3	Fixed
NTL[3]	Fixed
O_2	Mobile
Orange	Mobile
T Mobile	Mobile
Telewest	Fixed
Thus	Fixed
Vodafone	Mobile
Verizon Business	Fixed

---

[1] Comprising major companies that (as defined under the CCA) provide a public electronic communications network which makes telephone services available (whether for spoken communication or for the transmission of data).

[2] Affiniti is part of the Kingston Communications Group.

[3] NTL and TeleWest are in merger discussions.

Glossary

ACCOLC	Access and Overload Control, a system designed to give priority access to mobile networks in times of stress.
AOL	America On Line – a major US-based Internet Service Provider
ATM	Asynchronous Transfer Mode, a system for high speed data transmission.
Base Station	The part of a mobile telephone network where the radio antenna is sited.
CCS	Civil Contingencies Secretariat, part of the Cabinet Office which coordinates civil emergency matters.
CCTV	Closed Circuit Television
CNI	Critical National Infrastructure, the key assets, services and systems that support the economic, political and social life of the UK.
CPS	Carrier Pre-Selection, a service whereby telephone customers can have their calls routed via another network without having to dial a specific code.
CSIA	Central Sponsor for Information Assurance, part of the Cabinet Office, which has a coordinating role in telecoms resilience matters.
DSL	Digital Subscriber Line, a technology which allows a normal telephone line to carry broadband data.
DP	Distribution Point, the final part of the local access network where connections are made to individual homes, often mounted on a telegraph pole.
FDDI	Fibre Distributed Data Interface, a system for high speed data transmission over fibre, typically across campus sites.
Frame Relay	A medium speed system for data transmission, often used within corporate networks.
Gbit/s	Gigabits per second, that is, a data transmission rate of 10^9 bits per second.
GTPS	Government Telephone Preference System, a facility whereby priority can be given to public authorities on the fixed telephone network.

Head End	The central building in a cable network where the TV signals are distributed.
Internet	A global system of Interconnected Networks, using a common technical basis.
Intranet	An internal, corporate network using the same IP protocols as the Internet.
IP	Internet Protocol, the base protocol used for data transmission on the Internet.
ISP	Internet Service Provider
LINX	The London Internet Exchange, were ISPs connect their networks together to exchange traffic.
LLU	Local Loop Unbundling, a facility whereby a telecoms provider can use the copper loops of the BT network to provide their own competing broadband data services.
MDF	Main Distribution Frame, an arrangement of connections assembled on a large gantry which allows the external copper circuits to be cross-connected to any piece of internal equipment in an exchange building.
NAP	Neutral Access Point, such as the LINX, where ISPs connect their systems together.
NGN	Next Generation Network, a multi-service network mainly based on IP technology which is set to replace the present telephone network.
NISCC	National Infrastructure Security Coordination Centre, a cross-departmental agency which focuses on electronic security of the CNI.
NSAC	National Security Advice Centre, part of the Security Service that specialises in physical security.
Ofcom	Office of Communications, the UK communications regulator.
Oftel	Office of Telecommunications, the former telecoms regulator 1984-2003.
PCP	Primary Cross-Connect Point, typically a green roadside cabinet where local copper cables are cross-connected.
Private Circuits	Sometimes called Leased Lines, these are point-to-point un-switched telecoms circuits, used by businesses and other providers to link sites together on a permanent basis.
PSTN	Public Switched Telephone Network, the ordinary phone

	network.
SMDS	Switched Multi-Megabit Data Service, a system of high speed data transmission, a precursor to ATM.
WiFi	Wireless Fidelity, a radio system used for connecting computers together over short distances, in homes, offices or at public 'hotspots'.
WLR	Wholesale Line Rental, a service whereby a competitor to BT provides telephone service by reselling the BT network, in a similar way that 'airtime providers' provide service over mobile networks.
X25	A system of medium speed data transmission which has now largely been replaced by IP.