HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTNOTE

Number 584 August 2018

Security of UK Telecommunications

Telecommunications networks are essential for the day-to-day running of UK businesses and public services, but concerns have been raised recently over their security.[1-3] This POSTnote outlines the threats to these networks, the ability of networks to cope with disruption, and possible protective measures.

Overview

- Telecommunications networks face a range of physical and cyber threats that may be malicious, non-deliberate or naturally occurring.
- Concerns have recently been raised about the security of the undersea cables that carry 97% of global communications.[1]
- The Communications Act 2003 requires telecommunications companies to maintain the security and resilience of their networks.
- While there is no mandated security and resilience standard for telecommunications, Ofcom provides guidance on how companies can meet their obligation.
- Resilience methods include investing in duplicates of infrastructure and installing back-up power supplies.

Background

UK businesses, government agencies and other bodies are dependent on telephone and internet services provided by telecommunications (telecoms) networks to carry out daily operations.[4] Telecoms networks also provide services integral to the health and social life of the population.[4,5] The Government has recognised telecoms as one of 13 critical national infrastructure (CNI) sectors – a term signifying infrastructure that is pivotal to the functioning of the UK.[6]

The UK's Chief of the Defence Staff recently highlighted the threat posed by submarines to undersea telecoms cables, following reports of an increase in Russian submarine activity near the cables.[7,8] Undersea cables connect different countries together, transmitting an estimated 97% of all global communications and over $10 trillion of financial transactions every day.[9,10] UK telecoms companies are also increasingly targeted by cyber-attacks, with 66% reporting a rise in attacks targeting personal data between 2016 and 2017.[11] In addition, the CEO of the National Cyber Security Centre confirmed that there have been Russian cyber-attacks against UK telecoms companies.[12]

The Government classifies threats to CNI as physical, cyber or personnel-related.[13] Physical attacks occur when damage is caused by physical means, for example if cables are cut by an attacker. Cyber-attacks occur when a computer system is hacked or disrupted. Personnel threats arise from employees who create opportunities for physical or cyber-attacks through their legitimate access to an organisation's assets. This note focuses on physical and cyber threats to telecoms networks, covering:

- the infrastructure of public telecoms networks and how they are connected internationally;
- physical threats to networks and measures in place to address them; and
- cyber threats and measures to mitigate them.

Telecommunications Infrastructure

Telecoms networks rely on infrastructure to connect users to others in the UK and internationally. Networks comprise two main parts: a 'core' and an 'access' network.[4] A core (or 'backbone') network connects telecoms networks and carries large volumes of communication data across the country. There are several different but interconnected core networks owned by BT, Virgin Media and others (including mobile operators).[4] Core network infrastructure can also be provided by third parties.[14,15] Access networks connect customers to the core network in a local area, either via cables or wirelessly using radio signals.[4]

Fixed-Line Networks

Fixed-line networks provide telephone, TV and broadband internet services (POSTnote 494). Fixed-line core networks (such as those owned by BT and Virgin Media) are made up of telephone exchanges that contain a system of switches to route communications, usually connected by fibre optic cables. Access networks typically use a mixture of fibre optic and copper cables to connect customers' premises to the core network. Openreach (owned by BT) operates the majority of the UK's access network infrastructure, providing connectivity to 30 million UK premises.[16,17] Openreach has a regulatory obligation to share its infrastructure with other companies.[16] Virgin Media operates the UK's second largest fixed-line network.

Mobile Networks

Like fixed-line networks, mobile networks have a core network consisting of exchanges (known as 'mobile switching centres'), normally connected by fibre optic cables.[4] Mobile access networks differ from fixed-line ones, as they comprise base stations (connected to the exchanges) that communicate with handsets using radio signals.[4] Mobile operators use fixed-line (and in some instances radio) infrastructure to connect base stations and exchanges together.[4,18] Base stations provide access to the network over a limited area, so many are required to achieve UK-wide coverage. Mobile network providers must obtain a licence from Ofcom (the UK telecoms regulator) to use certain parts of the radio frequency spectrum.[19,20] There are four UK mobile network operators: Vodafone, EE, O2 and Three. The emergency services currently communicate using a dedicated network, which the Home Office is planning to migrate to EE's commercial network.[5,21,22] The migration has been delayed by 15 months and the Public Accounts Committee is currently conducting an inquiry into its progress.[23,24]

Undersea Cables

The core networks of different countries are connected using fibre optic cables that run along or are buried in the sea bed. There are around 40 active undersea cables connecting the UK to the rest of the world.[25] Undersea cables come ashore at landing sites that connect the cables to the core network. There are 11 UK landing sites.[26]

Satellites

Satellites can send and receive radio signals over large distances to antennae on the ground, and provide connectivity to remote communities where there is no fixed-line infrastructure.[19,27] The part of the radio frequency spectrum they use and the paths of their orbits are registered by the International Telecommunication Union.[28-30] Telecoms networks also rely on information from global positioning system (GPS) satellites to synchronise with each other.[31] Satellites cannot carry as much communication data as undersea cables since they are limited to a small part of the radio frequency spectrum.[32]

Physical Threats and Resilience

Telecoms companies are required to report to Ofcom security breaches and incidents that have a significant impact on the availability of their network.[33] For an incident to be reported, it needs to be above a threshold related to number of customer-hours lost. This does not take into account unsuccessful attacks. An analysis of the reported incidents is published annually, however, a breakdown of the number of hours lost for each incident is not provided.[34] Of the 678 incidents reported from September 2016 to August 2017, 93% were caused by hardware and software system failures. The 2017 National Risk Register of Civil Emergencies (NRR) details the risks of possible major UK national emergencies.[35] It describes several threats that could impact telecoms networks, including malicious attacks, non-deliberate threats, and natural hazards.[35] These are discussed in the following section.

Threats

Malicious Attacks

Motivations for malicious attacks can include financial gain (e.g. through metal theft) or causing disruption for the purpose of vandalism, espionage or terrorism.[36] In 2007, telecoms infrastructure was the target of an attempted terrorist attack when Al-Qaeda reportedly planned to bomb a key internet exchange in London.[37] Attacks can range from those using sophisticated military weaponry to those that don't use any specialised equipment (Box 1).

Non-Deliberate Threats

Examples of non-deliberate threats to telecoms networks include:

- **System failures** – these can occur in both hardware and software.[38] System failures were identified as the most common cause of network disruption reported by both Ofcom and the European Union Agency for Network and Information Security (ENISA) annually since 2012.[34,39]
- **Power failures** – telecoms infrastructure is dependent on a continuous supply of power.[40] Power failures were the second most common reason for network disruption reported by Ofcom in 2017.[41]
- **Cable damage** – up to 200 faults occur with undersea cables each year globally, two-thirds of which are caused by the anchors of fishing vessels or ships.[42] Excavation machines can cause damage to land-based cables.[43]

Natural Hazards

Of the 678 incidents reported by Ofcom in 2017, 2% were due to natural hazards.[41] Annual reports from ENISA since 2012 show that these lead to the most prolonged disruption (30 hours on average in 2016).[44] Hazards include:

- **Severe weather** – flooding, strong winds, cold weather, and heatwaves have the potential to disrupt telecoms.[35] Severe weather can cause disruption either through direct damage to infrastructure or loss of power.[4,45] In 2015, 61,000 UK homes lost power due to flooding, resulting in the loss of mobile and internet connections.[45]
- **Space weather** – space weather (changes in the near-Earth space environment) can interfere with, or damage, satellites (POSTnote 361).[46] In rare cases, space weather events can also disrupt telecoms and power infrastructure on the ground.[47]
- **Seismic activity –** undersea cables connecting the UK internationally could be damaged by seismic activity. In 2006, an earthquake in Taiwan damaged eight undersea cables, cutting off communication to Hong Kong, South East Asia and most of China.[48,49] Earthquakes can also damage land-based infrastructure, however, this is unlikely to occur in the UK.[35]

Box 1. Malicious Attacks

Examples of malicious attacks include:

- **Cable theft** – copper cabling has been stolen from the access network and disrupted emergency service communications.[50] Metal theft across all sectors is estimated to cost the UK economy £770 million per year, most of which occurs in the rail sector.[36,51]
- **Signal jammers** – signal jammers have been used to disrupt mobile and satellite networks by transmitting radio signals that interfere with them.[52] Handheld signal jammers can be purchased cheaply online and their effects are localised (typically tens of metres).[53,54] More powerful devices can reach up to 750m.[54] The Government's 2014 National Space Security Policy (NSSP) report highlighted signal jamming as a threat to satellite communication.[55]
- **Cable damage** – in shallow waters, ships dragging their anchors could be used to damage cables.[56] The undersea cable network contains 'choke points' (where several cables are routed through the same location) that, if targeted by submarines or ships, could damage multiple cables at once.[1] The locations of almost all undersea cables are publicly available.[25] Malicious attacks on undersea cables are rare.[1]
- **Anti-satellite weapons** – anti-satellite weapons are designed to interfere with or destroy satellites. Anti-satellite weaponry has been tested successfully against satellites in orbit close to the Earth.[57,58] The threat from anti-satellite weapons was highlighted in the NSSP, but only a few states are thought to possess them.[55]

Resilience and Protective Measures

Resilience is defined as the ability of a network to maintain an acceptable service in the face of challenges to normal operation.[59] The Communications Act 2003 requires UK telecoms companies to take appropriate measures to maintain the security and resilience of their networks.[60] While there is no mandatory security and resilience standard that telecoms companies have to meet (Box 2), Ofcom and others produce guidance on what measures are expected from telecoms companies in order to meet their obligations under the Communications Act (Box 3). Ofcom can issue fines if companies do not take sufficient measures.[61]

Fixed-Line and Mobile Networks

Physical security measures protect sites hosting telecoms equipment from theft or damage. The Centre for the Protection of National Infrastructure (Box 3) recommends using several different protective measures to achieve the best physical security, including controlling access to infrastructure using defences around site perimeters and detecting intruders with CCTV.[62-64] Openreach use a range of methods to prevent cable theft, including marking cables with SmartWater, an invisible solution that fluoresces under ultra-violet light and is difficult to remove, allowing cables to be traced to the street of origin.[17,50]

The Government's 2016 National Flood Resilience Review (NFRR) identified telecoms as a sector with infrastructure vulnerable to extreme flooding.[65,66] Following this review, telecoms companies have been working on putting in place plans to improve flood defences.[65] Portable infrastructure, such as base stations, can be deployed temporarily to mitigate the effect of infrastructure damage.[67,68] The exact procedures companies follow in the event of a flood are detailed in confidential emergency flood plans that vary between organisations.[76] One challenge identified in the NFRR is that telecoms companies make use of infrastructure located on sites owned by others, making it difficult to implement resilience measures.[65] For example, base stations may be located on leased property.

Box 2. Standards Available

Telecoms services procured by public sector organisations in the UK may be certified under the National Cyber Security Centre assurance scheme for telecoms, CAS(T), which is based on an internationally recognised standard (ISO 27001).[69-71] CAS(T) includes the requirement that certain physical and cybersecurity measures are in place.[69] Many telecoms providers, including BT and three of the UK's four mobile network operators, have services certified under CAS(T).[72] There are a number of other, international standards that telecoms companies can adhere to.[73-75]

Undersea Cables

According to the European Subsea Cables Association (ESCA), there is no noticeable effect when undersea cables around the UK are cut in fishing accidents, as communication is rerouted via other cables.[77] There are conflicting views on the scale of the threat of a malicious attack on undersea cables. Policy Exchange concluded that a coordinated attack on multiple cables would pose a major threat to the UK.[1] The UK's Chief of the Defence Staff also highlighted the risk of submarines to undersea cables.[7] Conversely, cable operator organisations, including the ESCA and the International Cable Protection Committee, have stated that the primary risk to cables is fishing accidents.[78,79]

If a cable is cut, the ease with which communication can be rerouted depends on the capacity available on other cables.[79] Cutting multiple cables at once, such as those in a choke point, may lead to a slowing down of the services that depend on those cables.[79] Cable operators monitor undersea cables and any attempts to cut or interfere with them is expected to raise an alarm at a monitoring station.[80] Cable operators typically deploy cable repair ships within 24 hours of a fault being reported.[81] The repair may take several days to complete, depending on factors such as the complexity of the repair and sea conditions.[82,83] To increase resilience, cables are laid to minimise the risk associated with natural hazards. For example, cables are positioned carefully in areas near the mid-Atlantic ridge.[84]

Satellites

The impact of space weather on satellites depends on factors such as the satellites' orbit.[85] Measures to reduce this impact are built into the design of the satellite, for example by using components that can withstand large amounts of radiation.[86] Organisations, including the Met Office, provide advance notice of solar activity so that satellite operators can take steps to mitigate damage.[87,88] The Government's NSSP report outlines the UK's approach to improving satellite resilience.[55] It includes measures such as improving the forecasting of solar weather and ensuring that relevant authorities have the power to prohibit the use of jammers.[55]

Box 3. Responsibility for Telecommunications Security

There are a number of Government and regulatory bodies in the UK that are responsible for the security of telecoms networks:

- Ofcom produce guidance for telecoms companies to set out an expectation of the measures they should take to meet their security and resilience obligations under the Communications Act 2003.[33]
- The Electronic Communications Resilience and Response Group (EC-RRG) was established in 2002 and comprises representatives from Ofcom, the Government and all major UK telecoms providers.[89] The EC-RRG issues guidance to telecoms providers on how to maintain resilience to a range of threats.[40,89] The EC-RRG is responsible for the maintenance of the National Emergency Plan for Telecommunications, which details the roles of Government and industry in the event of a civil emergency affecting telecoms.[90] It also enables the organisation of a response through the National Emergency Alert for Telecommunications (NEAT). NEAT is a conference call between EC-RRG members and allows them to share information.[90]
- The Department for Digital, Culture, Media and Sport (DCMS) is the lead department for telecoms and is responsible for responding to concerns about the security and resilience of UK networks.[91]
- There are several UK Government bodies that are responsible for security of CNI more broadly. These include: the Civil Contingencies Secretariat, which is responsible for emergency planning and response; the Centre for the Protection of National Infrastructure (CPNI), which is the Government authority on physical and personnel security; and the National Cyber Security Centre (NCSC), the Government authority on cybersecurity.[92-94]

Power Resilience

Generally, important parts of the network, such as telephone exchanges, have back-up batteries and diesel generators that can provide power for several days in the event of an outage.[95-97] A telephone connected to an exchange via copper cabling can draw power from the exchange and continue to operate.[98] A phone connected via fibre optic cabling is unable to do this. Ofcom are currently consulting on new guidelines to ensure customers with a fibre optic connection are still able to access emergency services in the event of a power cut.[99] Mobile base stations have no obligation to provide back-up power.[95] Ofcom has expressed concern at the dependence of mobile networks on mains power and plans to work with industry and Government to find options for improvement.[41]

Cyber Threats and Resilience

Telecoms companies underpin many vital services in the UK and hold their customer's personal data, making them a cybercrime target.[100] Ofcom stated that due to the growing threat from cybercrime, cybersecurity is a major concern.[41] Cybercriminals can target telecoms companies directly or target customers through the network (Box 4).

Threats

The cybersecurity of critical national infrastructure, including details of the different types of cyber-attack, is discussed in POSTnote 554. Additional cyber threats to telecoms include:

- **Device compromise** – devices used in telecoms networks (such as home routers) can be targeted in cyber-attacks. Once they are compromised, hackers can launch anonymous attacks or access services.[101-103] Vulnerabilities in devices can arise in the supply chain.[113] The NCSC have raised concerns about products produced by the Chinese manufacturer Huawei (POSTnote 554 Box 5) and Chinese state-owned supplier ZTE.[3,114,115]
- **Man-in-the-middle attacks** – communication between two parties may be covertly intercepted, recorded, and even altered by an attacker. Information collected may then be used for identity or data theft.[116] The NCSC recently reported that Russian state-sponsored actors used compromised routers to conduct man-in-the-middle attacks on UK networks.[117,118]
- **Legacy protocols** – protocols describe the software that telecoms networks use to communicate with each other, such as the SS7 protocol that enables calls to be connected between different operators.[119] Some protocols are decades old and were designed without considering future security issues.[119] The NCSC is working on improving the security of legacy protocols.[120]

Box 4. Cyber-Attacks on Telecommunications Companies

There have been multiple successful cyber-attacks against telecoms companies in the UK:

- In October 2015, TalkTalk was hacked and the personal data of 157,000 customers was stolen. The hack cost the company £60 million and resulted in the loss of 95,000 customers.[104,105] The Information Commissioner's Office fined TalkTalk £400,000.[106]
- In 2016, UK mobile provider Three was hacked, resulting in the theft of personal data from 134,000 customers.[107] The hackers accessed information using employee login details.[108]
- In 2016 it was reported that malicious software known as the 'Mirai Worm' had infected around 100,000 Post Office routers in the UK.[109,110] The hacked routers were used to route internet traffic to popular websites including Netflix and Twitter.[111] An independent testing body suggested that this could have arisen from a weakness in some of the routers' software.[112]

Resilience and Protective Measures

There are many cybersecurity schemes that telecoms companies may follow.[121] Ofcom recommend that all telecoms companies obtain 'Cyber Essentials Plus' certification from the NCSC's 'Cyber Essentials' scheme.[33] The scheme sets out basic technical controls to mitigate cyber threats.[122] It includes guidance on updating devices, using anti-virus software, and keeping internet connections secure.[123] Many UK telecoms companies hold this certification.[124] In addition, the Information Commissioner's Office provides guidance on preparing a data breach response plan; 58% of UK telecoms companies have a tested data breach plan.[125,126]

The NCSC, DCMS and Ofcom are partnering to launch a cyber vulnerability testing framework that will assess telecommunication companies' cyber resilience by carrying out realistic cyber-attacks on their systems.[41,127,128] This is based on the existing 'CBEST' framework, which carries out a similar exercise on UK financial organisations.[129]

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to Alison Tully for researching this briefing, to the Science and Technology Facilities Council for funding her parliamentary fellowship, and to all contributors and reviewers. For further information on this subject, please contact the co-author, Dr Lorna Christie. Parliamentary Copyright 2018.

Endnotes

1 ‘Undersea Cables: Indispensable, insecure’, Policy Exchange (2017)

2 ‘Cyber security: fixing the present so we can worry about the future’, NCSC (2017)

3 ‘ZTE: NCSC advice to select telecommunications operators with national security concerns’, NCSC (2018)

4 ‘Telecommunications Networks – a vital part of the Critical National Infrastructure’, EC-RRG

5 ‘Public Private Partnerships: Airwave’, NAO (2002)

6 ‘Public Summary of Sector Security and Resilience Plans’, Cabinet Office (2017)

7 ‘Russia a ‘risk’ to undersea cables, defence chief warns’, BBC News (2017)

8 ‘Russian submarines are prowling around vital undersea cables. It’s making NATO nervous.’, The Washington Post (2017)

9 ‘Economic Impact of Submarine Cable Disruptions’, APEC (2013)

10 ‘Reliability of Global Undersea Communications Cable Infrastructure’ Seminar, U.S. Federal Reserve (2011)

11 ‘Cybersecurity in the United Kingdom – Views from the C-Suite’, FICO (2017)

12 ‘Cyber security: fixing the present so we can worry about the future’, NCSC (2017)

13 ‘Advice’, CPNI (accessed June 2018)

14 ‘Telehouse’, Telehouse (accessed July 2018)

15 ‘Telecoms’, SSE Enterprise (2016)

16 ‘Infrastructure Report: The first Communications Infrastructure Report’, Ofcom (2011)

17 ‘Your guide to Openreach’, Openreach (2017)

18 ‘Report on the convergence of fixed and mobile networks’, BEREC (2017)

19 ‘United Kingdom Frequency Allocation Table’, Ofcom (2017)

20 ‘Mobile coverage obligation’, Ofcom (2018)

21 ‘Upgrading emergency service communications: the Emergency Services Network’, NAO (2016)

22 ‘Emergency Services Network: overview’, HM Government (accessed June 2018)

23 ‘Emergency Services Network: progress review inquiry’, Public Accounts Committee (accessed June 2018)

24 Third Annual Report of the Chair of the Committee of Public Accounts, House of Commons Committee of Public Accounts (2018)

25 ‘Submarine Cable Map’, TeleGeography (accessed June 2018)

26 ‘Undersea Cables’ Debate, Lord Ashton of Hyde (2018)

27 ‘Extending Mobile Networks into Rural Areas via Satellites’, Gilat (2015)

28 ‘Satellite Regulation: An introduction for new entrants’, Ofcom/UK Space Agency (2017)

29 ‘Procedures for the Management of Satellite Filings’, Ofcom (2016)

30 ‘Satellites & Spectrum: The Right Wavelength’, ESOA (2010)

31 ‘Satellite-derived Time and Position: A Study of Critical Dependencies’, Government Office for Science (2018)

32 ‘Submarine Communication Cables – The Backbone of Worldwide Communications’, Internet Access Guide (accessed June 2018)

33 ‘Ofcom guidance on security requirements in sections 105A to D of the Communications Act’, Ofcom (2017)

34 ‘Connected Nations and infrastructure reports’, Ofcom (accessed June 2018)

35 ‘National Risk Register Of Civil Emergencies: 2017 edition’, Cabinet Office (2017)

36 ‘Metal Theft Taskforce: Identification Booklet’, Openreach (2015)

37 ‘Al Qaeda plot to bring down UK internet’, The Times (2007)

38 ‘Guideline on Threats and Assets: Technical guidance on threats and assets in Article 13a’, ENISA (2015)

39 ‘Incident Reporting’, ENISA (accessed June 2018)

40 ‘EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure’, EC-RRG (2006)

41 ‘Connected Nations 2017: Data analysis’, Ofcom (2017)

42 ‘Submarine Cables: The Handbook on Law and Policy (2014)’, Brill (2013)

43 ‘Quick Guide: Duct Laying’, Openreach (2017)

44 ‘Annual Incident Reports 2016’, ENISA (2017)

45 ‘Living without electricity: One city’s experience of coping with loss of power’, RAE (2016)

46 ‘Extreme space weather: impacts on engineered systems and infrastructure’, RAE (2013)

47 ‘Solar flare eruptions set to reach Earth’, BBC News (2011)

48 ‘Submarine Cables Cut after Taiwan Earthquake in Dec 2006’, Submarine Cable Networks (2011)

49 ‘Under the Sea: The Vulnerability of the Commons’, Foreign Affairs (2015)

50 ‘Report cable theft’, Openreach (accessed June 2017)

51 ‘Metal Thefts (Electricity Industry)’ Debate, Graham Jones (2011)

52 ‘Report on GNSS Vulnerabilities’, Sentinel (2014)

53 ‘GPS chaos: How a $30 box can jam your life’, New Scientist (2011)

54 ‘Jamming and radio interference: understanding the impact’, IET

55 ‘National Space Security Policy’, HM Government (2014)

56 ‘Undersea cable break: Four things you wanted to know’, BBC News (2016)

57 ‘Concern over China’s missile test’, BBC News (2007)

58 ‘Worldwide Threat Assessment of the US Intelligence Community’, Office of the Director of National Intelligence (2018)

59 ‘ResiliNets: Multilevel Resilient and Survivable Networking Initiative’, ITTC (2006)

60 ‘Communications Act 2003’, HM Government (2003)

61 ‘Penalty guidelines’, Ofcom (2017)

62 ‘Physical Security’, CPNI (accessed June 2018)

63 ‘Physical Defences at the Perimeter’, CPNI (accessed June 2018)

64 ‘Intruder Detection, Tracking, Monitoring and Lighting’, CPNI (accessed June 2018)

65 ‘National Flood Resilience Review’, HM Government (2016)

66 ‘Flood risk management and funding’, HoC Library (2017)

67 ‘EE shows off helium balloon mobile masts’, BBC News (2017)

68 ‘Ubi-Tech involved in the Ericsson/EE launch of Rapid Response Vehicles’, Ubi-Tech (2017)

69 ‘Security Procedures: Telecommunications Systems and Services’, NCSC (2016)

70 ‘ISO/IEC 27001:2013’, ISO (2013)

71 ‘Apply for a Public Services Network (PSN) connectivity service compliance certificate’, Cabinet Office (2016)

72 ‘Organisations’, NCSC (accessed June 2018)

73 ‘ISO/IEC 27001:2013’, ISO (2013)

74 ‘NICC ND1643: Minimum Security Standards for Interconnecting Communications Providers’, NICC (2015)

75 ‘Introduction to the NIS Directive’, NCSC (2018)

76 ‘The UK’s Core Digital Infrastructure: Data Centres, Climate Change Adaption and Resilience’, TechUK (2016)

77 ‘Submarine Telecommunications Cables’, ESCA

78 ‘Let us put the record straight on ‘Submarines, Sharks and Spooks’ (and other submarine cable myths)!!!’, ESCA (2016)

79 Private communication, ICPC (2018)

80 ‘Undersea Fiber Communication Systems’, Academic Press (2002)

81 ‘Submarine Cable Services’, ACMA (2018)

82 ‘Maintainence/Repair Operations’, KIS-ORCA (accessed June 2018)

83 ‘How undersea fibre-optic cables are repaired’, Deccan Chronical (2016)

84 ‘Submarine Cables and BBNJ’, ICPC (2016)

85 ‘Space Weather Prediction Center Topic Paper: Satellites and Space Weather’, NOAA/Space Weather Prediction Center (accessed June 2018)

86 ‘Space Weather’, Intelsat (accessed June 2018)

87 ‘Space Weather’, Met Office (accessed June 2018)

88 ‘Solar storms and their impacts on power grids – Recommendations for (re)insurers’, SCOR (2014)

89 ‘Terms of Reference: Electronic Communications Resilience and Response Group (EC-RRG)’, HM Government

90 ‘National Emergency Plan for the Telecommunications Sector’, HM Government (2010)

91 Letter to Rt Hon Norman Lamb MP, DCMS (2018)

92 ‘Preparation and planning for emergencies: responsibilities of responder agencies and others’, Cabinet Office (2013)

93 ‘About CPNI’, CPNI (accessed June 2018)

94 ‘About us’, NCSC (accessed June 2018)

95 ‘Connected Nations 2016’, Ofcom (2016)

96 ‘Response to Ofcom Review of Digital Communications’, Chaltel (2015)

97 ‘Telecoms resilience’, Cabinet Office (2013)

98 ‘Will your landline telephone work during a power cut?’, Ofcom (2015)

99 ‘Consultation: Proposed guidance on protecting access to emergency organisations when there is a power cut at the customer’s premises’, Ofcom (2018)

100 ‘Global Cyber Executive Briefing: Telecommunications’, Deloitte (accessed June 2018)

101 ‘Threat intelligence report for the telecommunications industry’, Kapersky Lab (2016)

102 ‘SYNful Knock – A Cisco router implant – Part 1’, FireEye (2015)

103 ‘Cisco Talos VPN Filter malware findings’, NCSC (2018)

104 ‘TalkTalk hack affected 157,000 customers’, BBC News (2015)

105 ‘TalkTalk loses 101,000 customers after hack’, Telegraph (2016)

106 ‘TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack’, ICO (2016)

107 ‘Data on over 130,000 Three mobile customers compromised in breach’, The Guardian (2016)

108 ‘Three Mobile hack affected 76,000 more customers than thought’, Telegraph (2017)

109 ‘TalkTalk and Post Office customers hit by Mirai worm attack’, Wired (2016)

110 ‘The Botnet that broke the internet isn’t going away’, Wired (2016)

[111] ‘Dyn reveals details of complex and sophisticated IoT botnet attack’, Computer Weekly (2016)
[112] ‘TalkTalk router hack. Consumers, what should you do?’, Pen Test Partners (2016)
[113] ‘Supply chain security collection’, NCSC (2018)
[114] ‘Huawei cyber security evaluation centre: oversight board annual report 2018’, Cabinet Office (2018)
[115] ‘Cyber security watchdog warns UK telcos against using equipment from Chinese supplier ZTE’, Financial Times (2018)
[116] ‘Man-in-the-middle attacks: Is your organisation vulnerable?’, SME (2018)
[117] ‘Additional information: Russia’s malicious cyber activity’, NCSC (2018)
[118] ‘Advisory: Russian state-sponsored cyber actors targeting network infrastructure devices’, NCSC (2018)
[119] ‘Legacy technologies as a threat to EU’s telecommunications infrastructure’, ENISA (2018)
[120] ‘Active Cyber Defence – tackling cyber attacks on the UK’, NCSC (2016)
[121] ‘UK Cyber Security Standards’, BIS (2013)
[122] ‘Cyber Essentials’, NCSC (2015)
[123] ‘Cyber security for your organisation starts here’, NCSC (accessed June 2018)
[124] ‘Certified Organisations’, IASME (accessed June 2018)
[125] ‘Guidance on data security breach management’, ICO (2012)
[126] ‘Cybersecurity for Telecom – Views from the C-Suite’, FICO (2017)
[127] ‘Department for Digital, Culture, Media and Sport single departmental plan’, DCMS (2018)
[128] ‘Review of Security Guidance’, Ofcom (2017)
[129] ‘Financial sector continuity’, Bank of England (accessed June 2018)