Written evidence submitted by Dr Greig Paul (Lead Mobile Networks & Security Engineer on 5G RuralFirst), Electronic & Electric Engineering, University of Strathclyde

Acknowledgement:

This response was prepared with the assistance and input of Dr James Irvine (a Reader in the Department of Electronic & Electrical Engineering, University of Strathclyde).

Author Bio:

Greig has been a consultant working with international mobile network operators, working on projects with small operators on their network design and technology. More recently, a Cyber-Security Lead working in the utilities sector (critical national infrastructure), and Chief Information Security Officer for a pre-launch UK start-up bank. He bridges the technology and executive divide in a range of fields, having advised at board level on cyber-security, foreign governments on spectrum policy and mobile auction design, FinTech start-ups on security and strategy in the banking and payments sectors, to name a few.

Since then, he has led the architecture & design, deployment and operation of the 5G RuralFirst end-to-end cellular network, including network security considerations.

Executive Summary

- 5G networks will see significant changes from 4G networks. While today we see only early stages of 5G adoption, we can see that these changes will impact security in network design.
- 5G will increasingly bring **"core" functions towards the edge** (nearer the radios) of the network – the distinction of "core" and "non-core" is blurring already with new technology.
- In light of this, we **must** ensure our networks are designed with this in mind – our networks should be designed to be "**intrinsically secure**" without relying on equipment vendors.
- There is momentum behind 5G enabling "Industry 4.0" and associated increases in productivity, with businesses encouraged to take advantage of 5G. This means security issues in 5G networks will **directly impact the economy**, and NCSC may need **to prepare for advising non-telecoms providers** about security of private mobile networks.
- Some applications, such as connected vehicles, will require increased **inter-connectivity between different telecoms networks at the edge of their networks** (where core functions will move to), for **low-latency** safety-related communications. This is a change compared to the current approach, where networks only inter-connect at the core, and has security implications around vendor equipment and **exposure of telecoms companies to the vendor selections of other telecoms operators**.
- The O2 outage in late 2018 has highlighted the harm to the country by disruption to service, and the lack of resilience in place. There are **legislative gaps** around telecoms

operators, compared with other utility operators. Telecoms networks **should be considered as essential services**, and **regulated under NIS regulations**. This has implications for other CNI, including energy utilities, which do not consider public mobile networks to have **suitable power autonomy** in the event of a "blackstart" incident.

- The risks of **widespread outsourcing** within the telecoms sector (and other utilities and infrastructure sectors), as well as "sell-and-lease-back" models, should be considered by the committee.
- Government policy around connectivity shows a move towards **convergence of industrial/business focused networks and public 5G networks**, as shown in the Rural Connected Communities competition, with a vision of **new, smaller entrants into the telecoms market**. As government policy envisages new entrants into this market, it is important to consider what the security implications will be, and how to support them.

Key Recommendations:

- Telecoms operators should be designated as **Operators of Essential Services** under NIS, in light of their importance in day-to-day life and the economy, and exposed to the same penalties for disruption as other OES, ensuring **investment in security and power resilience.**
- Parliament **should reduce the weight it places on distinction between "core" and "non-core"** functions of networks – networks should be secure **without relying on vendors**. Inter-connection at the network edge for low-latency vehicular communications means **vendor choices can impact on other network operators, and cause cascading security issues**.
- Parliament should consider whether a culture of **buying "cheapest"** puts the UK's national interests at risk, among telecoms companies**. Operators, not government, should bear the costs of suitable security, as they enjoy the profits from operating these networks**.

Challenges and Opportunities for the UK's Telecoms Sector

(1) One particular challenge for the UK's position in the global telecoms market is that it, for the most-part, doesn't have a major domestic offering in the equipment used to build mobile networks. There is significant potential for export of this equipment, particularly if the UK were to build a reputation for building and selling high-quality, secure equipment around the world. This would also help the UK to ensure the security of critical components of its own telecoms infrastructure. The costs of verifying the security of third-country vendors' equipment properly may be significant, and some of this cost may perhaps be better spent developing and securing domestically-developed equipment for telecoms networks.

(2) The UK does have strong technical knowledge and expertise in telecoms, and could provide a strong, compelling offer that exports worldwide, using some of our world-class innovation and technical expertise to provide another option for secure telecoms

equipment. At a time where major vendors' offerings suffer regularly from embarrassing security flaws and poor design practices[1], there is an opportunity for a new entrant. The biggest challenge that would be faced in attempting to grow a UK mobile telecoms equipment sector would be the culture of "cheapest over all else." In pursuit of maximum profits for shareholders, telecoms companies both domestically and internationally focus on **cost reduction** as one of their top priorities, as well as elimination of capital assets. This needs to be balanced with the serious responsibility of securing the UK's infrastructure, and suitable penalties put in place to ensure there are economic incentives to invest in security. This conclusion is also highlighted by the Government's own Telecoms Supply Chain Review Report[2].

(3) For example, one UK mobile network operator is currently planning to **sell off 60,000 mobile masts** across Europe for €20bn, driving their share price up as a result of an expected dividend or "windfall" to shareholders as a result of the sale[3]. The committee and wider parliament should question **whether it is in the strategic national interests of the UK** for operators of mobile networks, now effectively critical national infrastructure**, to sell these assets**, and whether suitable regulatory levers are in place to ensure mobile network operators manage and operate this critical infrastructure with the UK's national security interests at heart. Consumers may remember Woolworths, a major UK retailer, which collapsed partly as a result of a sale-and-leaseback arrangement carried out by its owners, to liquidate profits from the business[4].

(4) Some international suppliers are heavily subsidised by their respective national governments[5], and this kind of subsidy makes these suppliers hard to compete with purely on price. This would also potentially pose challenges in establishing a vibrant domestic-based telecoms sector. Nonetheless, consideration should be given as to how to **ensure a well-funded vendor is not able to use subsidised pricing to gain entry to a market**, and the potential legal remedies available through the Competition Act 1998 and other relevant legislation.

Opportunities and Risks Involved in Purchasing Equipment and Services from Foreign Suppliers

(5) When considering the security of suppliers' offerings, it is firstly important to remember that, even with equipment manufactured domestically or in neighbouring countries, **the supply chain of modern electronics equipment and devices can be problematic for security**. Indeed, equipment sold by major US vendors can arrive "double-boxed", where the inner box contains the box labelled from the factory where the product was made. This raises the importance of supply chain security. **There is a significant risk around**

[1] https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

[2] https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference

[3] https://www.theguardian.com/business/2019/jul/26/vodafone-standalone-mobile-mast-business-towerco-europe

[4] https://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/3527448/Woolworths-failure-could-trigger-high-street-collapse.html

[5] https://news.yahoo.com/huawei-key-beneficiary-china-subsidies-us-wants-ended-021607000--finance.html

the lack of supply chain diversity in electronics and other devices. The UK Telecoms Supply Chain Review report addresses this.

(6) One of the main challenges for MNOs and those purchasing equipment and services is a lack of cyber-security awareness throughout organisations. Often, formal procurement processes are used to purchase goods and services – these generally result in a business-minded decision to select the cheapest credible option, particularly in some utility sectors. There has been, and is, an ongoing drive to cut costs within this sector and reposition businesses' financials – as mentioned earlier, one UK mobile network operator has announced its plans to sell off its tower business in the next 18 months, for example.

Telecoms are critical infrastructure, but are not held to that standard

(7) Our telecoms networks are now **part of the fabric of society**, and **becoming critical to the economy**. As payments increasingly move towards debit and credit card transactions, cash use reduces, and our dependence on telecoms networks for daily commerce increases. During the O2 outage in late 2018, **an example of what the future holds** was seen[6] - Uber drivers and food delivery drivers using the O2 network were **struggling to find work** and had to hop between WiFi hotspots unaffected by the mobile network outage. London buses were unable to communicate their progress for bus stop timing screens, and journey planning websites. Pay-as-you-Go access to the London rental bikes was unavailable, as payments depended on the O2 network. Small businesses were unable to plan work, take bookings, or handle payments, as these were dependent on mobile network access.

(8) It is generally accepted that **electricity, gas and water are utilities** which are critical to the functioning of society – they are viewed as **critical national infrastructure**, and must conduct their operations accordingly, even where their operation is franchised out to privatised operators – expected standards of availability and safety remain. In the energy sector, for example, **penalties** are applied on the basis of "**customer minutes lost**". There are, for the most-part, not similar systems in place for telecoms networks, aside from 999 outages.

(9) The potential reach on impacts of a mobile network outage should be considered – **the vulnerable and the elderly** (particularly those who are mobile and able to leave the home) may rely on cellular-based **fall detection and alert systems**. Lone working alarms and monitoring systems utilise mobile connectivity for staff not based at a single location. The rise of tele-health and similar technologies presents similar concerns, particularly with an aging population and elderly care crisis. Mobile telecoms based healthcare and medical solutions offer simple "fit and forget" solutions to help ensure the welfare of the elderly as they choose to grow old in their own homes. Many consider **tele-medicine** as one of the opportunities enabled by **5G networks**. This situation will become more critical with the **PSTN switch-off**, an area Ofcom is exploring[7].

[6] https://www.bloomberg.com/news/articles/2018-12-08/o2-s-all-day-outage-caused-havoc-in-ways-consumers-didn-t-expect

[7] https://www.ofcom.org.uk/consultations-and-statements/category-2/access-emergency-organisations-power-cut

(10) Ofcom's 2017 Connected Nations report highlights that the majority of security incidents related to voice services (including access to 999 services), and that "the majority of incidents are caused by the failure of hardware components, the loss of power supply, or by software bugs". They highlight in particular that "The resilience of mobile networks, in particular to major power disruption, remains a key concern". With 70% of calls to 999 made from mobile phones in 2017, mobile telecoms are now essential services, and save lives.

(11) To ensure value for money for the taxpayer and billpayer, it is important to ensure that all sectors of industry are able to take make the most of telecoms networks. As electricity distribution network operators increasingly look to improve connectivity in their networks to create a "**smart grid**", suitable for the **mass adoption of electric vehicles** and other **low-carbon technologies**, the ability to avoid **reinventing the wheel** using billpayer money by using infrastructure is clearly advantageous for all concerned. The ability for utilities to utilise public mobile network infrastructure would therefore be beneficial for all concerned. Due to the **lack of power resilience in mobile networks**, as identified by Ofcom in the 2017 Connected Nations report, this is currently not possible. A network capable for use in control of would have to meet the requirements for "black start" resilience – the ability to still be operational throughout, after power was lost nationally for a period of several days. Otherwise, such a network would not offer sufficient resilience to be used in this way.

(12) Even if meeting full black start resilience standards was not deemed feasible by operators, **enhanced power resilience is clearly necessary**. People **depend on telecoms networks** to be operational, and the systematic lack of power resilience in mobile network cell sites is a relatively "hidden" problem the committee should explore further, given the growing importance mobile networks have in daily life.

(13) The business pressures on those operating critical telecoms infrastructure sometimes create challenges and conflicts – in 2008, an Ofcom spokesperson confirmed they **were not aware of any requirement** for mobile operators to provide **backup power to mobile base stations**[8].

(14) Ofcom's 2017 Connected Nations report highlights that the majority of security incidents related to voice services (including access to 999 services), and that "the majority of incidents are caused by the failure of hardware components, the loss of power supply, or by software bugs". They highlight in particular that "**The resilience of mobile networks, in particular to major power disruption, remains a key concern.**"

(15) Ofcom's 2018 Connected Nations report notes that fixed exchanges and core network nodes would typically have backup power to support normal operation for between 2 and 7 days, with refuelling of generators able to continue this on an ongoing basis. "Hub" sites, usually base stations which other base stations use to connect through to the network would usually have 4 to 8 hours of battery protection, with on-site or temporary generators used if a longer outage were experienced. **The majority of mobile cell sites have around 10 minutes of battery runtime**. This effectively allows for a "graceful shutdown", rather than providing any level of resilience.

[8] https://www.networkworld.com/article/2284316/backup-power--not-required--in-u-k--base-stations.html

(16) This issue was highlighted clearly during the "blackout" over large parts of the UK on 9th August 2019, with the Telegraph reporting mobile phone and internet connectivity going "dead" as masts seemingly lost power.

(17) In terms of power resilience, Street cabinets or other fixed nodes in the network would usually have battery backup of 2 to 24 hours. Ofcom has noted the risk that in some areas, **"service, including the ability to call the emergency services, could fail immediately"**. This has significant public safety and national security implications.

(18) In the major 2015 power outage in Lancaster, the Royal Academy of Engineering's "Living Without Electricity"[9] report documents that "**Most mobile phone coverage was lost within an hour**", and also reported that "**many people who had replaced their traditional handsets with cordless phones were unable to connect". Internet services were mostly unavailable**, and home routers were obviously unpowered, leading to an effective outage for most people. **Electronic payment systems were non-functional**, and "**most ATM machines did not work**". The ability to get access to fuel was also hindered, as "garages could not sell petrol or diesel as pumps are driven by electricity". This may present challenges for operators planning to fuel generators without their own power-resilient plans for fuel supplies.

The Risk of Complex Third-Party Dependencies

(19) Ofcom's 2018 Connected Nations report highlights the general lack of long-term runtime of mobile cell sites, as well as the **external dependency of O2 on an Ericsson network component**, where a certificate expired. This reflects one of the main challenges for mobile networks when purchasing equipment – **the need to verify that it operates independent of the supplier or vendor's own operations.**

(20) It is unclear the extent to which mobile networks have outsourced their capabilities to operate and maintain their own networks,

(21) When considering the impact of cyber-security threats, it is important to also consider the implications of availability impacts by more conventional or passive routes. With availability an important consideration in the running of telecoms networks, it is now more important than ever to **ensure our infrastructure can run with full autonomy, even in the absence, or lack of cooperation of, external vendors and suppliers**. Were Ericsson not to have promptly responded and resolved the issue, it is unclear how this situation would have played out; namely **whether or not O2 was able to issue a new valid certificate itself in replacement for the expired one**.

(22) With a drive to outsource support costs from networks, many functions in the operation of telecoms networks have been outsourced. Ofcom is aware of these, and has issued guidance to this effect. In a document entitled "Updating Ofcom's guidance on network and service security", obligations under 105A(4) of the Communications Act are clarified to **not be excused where a communications provider outsources work**, and the telecoms operators are required to **regularly ensure these continue to be met**[10].

[9] https://www.raeng.org.uk/publications/reports/living-without-electricity

[10] https://www.ofcom.org.uk/__data/assets/pdf_file/0028/108856/Statement-review-security-guidance.pdf

From the perspective of national infrastructure resilience, however, the **prevalence of outsourcing**, as well as the adequacy of controls in place should be considered. In particular, attention should be paid to any situations where outsourcing takes place across national boundaries, to avoid scenarios like that seen in Sweden, where information which was highly sensitive to national security (including identifies of undercover operatives) was transferred to a third country by an outsourced provider seeking to reduce costs of their operations[11].

(23) By looking at operators overseas, we can see the extent to **which outsourcing of critical functions** of telecoms operators' businesses has occurred[12]. Outsourcing providers or **vendors** are **a major route of compromise into networks and businesses**[13] , with on average 59% of organisations having been **breached as a result of a vendor[14]**. Where telecoms infrastructure is relied upon to the extent it is today in the UK, this risk should be carefully monitored and managed by regulation, and this is an area the committee may be wise to explore.

(24) When this is considered in line with the UK Telecoms Infrastructure Review Report's observations about "insufficient incentives to internalise the costs and benefits of security", it should be particularly concerning for the committee to note the potential for widespread outsourcing to result in reductions in security for the UK's telecoms networks.

Regulation, Legislation & Collaboration

(25) Concerns around security and resilience can be, to some extent, addressed by way of carrying out technical investigation, like GCHQ/NCSC currently do via the Huawei Cyber Security Evaluation Centre. This is an area for potential collaboration and cooperation with other like-minded countries, since detection of vulnerabilities within vendor-supplied telecoms products is an area where "more eyes" help to reduce the number of undetected vulnerabilities. Nation state actors already look for vulnerabilities in telecoms and other infrastructure equipment, therefore cooperating with others on detection of these vulnerabilities may help to improve the security of UK telecoms assets.

(26) There is a complex landscape for cyber-security, in particular around telecoms companies. While there are clear needs for separation of responsibilities, it appears questionable how effective this regime is for UK telecoms companies. **Telecoms companies**, for example, are **not currently subject to NIS**, despite operators of "radio and telecommunications systems, computer systems and networks" in the water transport sector being covered, due to recital 7 excluding those providing public communication networks or publicly available electronic communication services governed by other regulations around security[15]. EC Directive 2002/21/EC (March 2002) sets out the framework for regulating providers of telecommunications networks. It is worth noting

[11] https://www.nytimes.com/2017/07/25/world/europe/ibm-sweden-data-outsourcing.html
[12] https://ultra.news/s-e/32708/wipro-wins-5-year-outsourcing-deal-telenors-bangladesh-unit
[13] https://www.beyondtrust.com/blog/entry/wipro-breach-how-to-stay-protected-when-your-managed-services-provider-gets-hacked
[14] https://www.apnews.com/556444d2cc114ea9a8ceda8f747b329c
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

that this regulation does not specifically address cyber-security, and the UK's Communications Act, namely Sections 105A to 105D, appears to provide the cyber-security regulation around telecoms providers[16], but caps the penalty to £2 million**, far below penalties in the NIS directive for operators of essential services**. Telecoms services are **essential** to day-to-day life, business, economic activity, and societal function in the UK.

Closing Remarks

(27) I particularly welcome the publication of the UK Telecoms Supply Chain Review Report (July 2019), and in particular highlight its recognition of the **need for the UK to deliver a strong policy response**, the challenges around a **limited number of foreign-based suppliers**, and the tensions between commercial factors and cyber-security, which currently allow short-term financial thinking to outweigh the important duty to the nation's security that telecoms operators hold.

(28) I would add that there is inherent supply-chain centralisation and concentration around a number of regions of the world, and that the committee should explore the implications of these – continued availability in an era of increased international tensions and volatility should be considered, as well as the cyber-security considerations around low-level components being sourced from these countries.

(29) With reference to the statement around "the complexity of delivering, monitoring and enforcing contractual arrangements in relation to security," I suggest that the committee not take this into consideration – while absolutely correct, **telecoms operators operate profitable businesses delivering services which government recognises to be essential to the economy and growth**. If telecoms operators struggle to enforce contractual arrangements around cyber-security, arguably they **should not be outsourcing such activities**.

(30) When providing **critical infrastructure**, it is important for Government to recognise its mandate and right **to regulate in the national interest**, even if this were to mean increased costs, or barriers in the path to the wholesale outsourcing of network operations which we are seeing. The **responsibility lies with the operator** to ensure the security of their network. Challenges in contracting others to carry this out mean the operator should consider taking on these tasks internally. This is backed up by Ofcom guidance on the subject, namely their document titled "Updating Ofcom's guidance on network and service security", which clarifies that **obligations under 105A(4) of the Communications Act are not excused where a communications provider outsources work**, and the telecoms operators are required to regularly ensure these continue to be met[17]. From the perspective of national infrastructure resilience, however, the prevalence of outsourcing, as well as the adequacy of controls in place should be considered.

(31) The complexity and potential **interdependency of telecoms networks and other critical infrastructure (including power networks)** should not be overlooked, particularly where there is potential for circular dependencies to form – if power network

[16] https://www.legislation.gov.uk/ukpga/2003/21/section/105A

[17] https://www.ofcom.org.uk/__data/assets/pdf_file/0028/108856/Statement-review-security-guidance.pdf

operators depend on mobile infrastructure to reach remote assets, and a power outage prevents connectivity, this could hamper the UK's ability to respond to a blackstart incident.

(32) The rise of mobile network-based payments handling should be considered by the committee, particularly for the UK's economic resiliency. As cash usage falls, and card usage consequently rises, there is a risk of the economy becoming over-reliant on technology which is not legally deemed essential under the NIS directive. Other infrastructure (such as transport) depending on fixed and mobile networks (such as TFL buses) should not be overlooked. The **impact of a widespread mobile network failure has now been partially seen during the O2 outage** in December 2018, and the committee should look at this example to consider the UK's **ability to resist a targeted, deliberate attack** by a belligerent party or actor.

(33) When considering 5G, it is important to note that we are **unlikely to see a 6G in the same form of nationwide roll-out** of an entirely new generation of network, with new equipment, at significant capital expense. Mobile network operators are already looking at ways to monetise their existing fixed assets and infrastructure, meaning it is **questionable whether there would be sufficient money to fund another roll-out in the future**. Site and asset sales show that we may be reaching the point of inadequate returns on nationwide infrastructure deployments for mobile networks. It is therefore essential to ensure that 5G is architected and deployed with a view to the future, and ensuring it remains secure going forwards, since supply chain or vendor decisions taken today will have **lasting repercussions** into the future.

(34) An effective focus on the development and growth of new, smaller entrants, is particularly welcomed, and mention of the DCMS **5G Testbeds and Trials** program is important – these trials have made considerable progress, and it is worth policy-makers engaging with those who have been involved in these trials. **I would be happy to participate in follow-up on this topic**.

13 September 2019