

UKTIN

Future Capability Paper

Security

Executive Summary

In this paper prepared by the UKTIN Security Expert Working Group (EWG), we set out a view of the UK telecoms ecosystem's strengths, weaknesses, opportunities, and threats around security. In doing so, we explore some of the major threats and risks, and some of the potential enablers, particularly around skills and diversity in building the technical capabilities for the UK to meet its own future telecom's needs. Both the telecoms and cyber-security sectors struggle with skills, and the intersection of these two areas is even more limited in skills.

We recognise that given the nature of this niche intersection, in many cases there is no simple short or medium-term solution to the skills challenges we face, beyond nurturing current talent, and ensuring competent technical leadership in these areas. The worst thing we could do would be to allow ourselves to lose the technical experts with the knowledge needed to secure our telecoms networks, as this will leave the next generation without the guidance and experience needed to become experts.

We also reached several key findings and conclusions, which should inform next steps in this space, and this EWG's subsequent activities. Key evidence-based findings from this EWG are set out below.

This UKTIN Security EWG will work to reach several key recommendations which should inform next steps in this space and will be part of this EWG's subsequent activities.

Key Findings

- The security risks and threats to telecoms are generally well-understood, and existing research and development has produced viable mitigations to many of these issues – the true gap is around driving adoption and uptake of these mitigations and staying "ahead of the curve" of attackers.

- Many of the most impactful vulnerability types are the same year-on-year, and the mitigations available are effective – it is a lack of broad, deep technical knowledge throughout the sector that makes adoption and uptake hard. In particular (and this extends beyond telecoms), adoption is stymied through a lack of technical knowledge of the inner workings of systems, and a culture among operators of outsourcing to vendors, at a time when the UK has a very limited major vendor footprint, meaning the skills and knowledge are located overseas.

- The UK has a real opportunity in certain areas, with an internationally competitive small-scale boutique telecoms consultancy sector – arguably the UK punches above its weight on this front, with many of the early leaders in telecoms being from the UK. This advantage will only last until those individuals retire however, and should be exploited to maximise UK influence, and grow a future generation of industry leaders.

- Given the shift in 5G towards commodity off-the-shelf computing platforms, backed up by IT-based container and virtualisation platforms, telecoms security is now IT/network/platform security. Telecoms security will no longer exist as a separate concept in a vacuum since a significant portion of the attack surface of a 5G (or beyond) telecoms network is based on IT and internet technologies. This means that skills requirements are broadening.

Other Findings

- Security has been (and increasingly is) a cross-cutting enabling function critical to the wider telecoms ecosystem. In the course of this work, the Security EWG was approached to give input to the AI EWG, as well as the Network Management and Semiconductor EWGs. Appendix A – AI Security Summary Note provides the technical input from this Security EWG to the AI EWG around some of the security risks in adoption and use of AI in telecoms.

- Security and resilience are fundamental factors for telecoms in the UK, as well as internationally (as is evidenced by legislation, high risk vendor designations, and similar activities based on threat intelligence of attacks on telecoms networks to gain strategic advantage and cause disruption in the event of conflict, as more and more critical systems rely on them). Similarly, we have set out some examples of how circular resilience dependencies can arise, and how (for example) the energy network is increasingly becoming dependent on telecoms networks to function and recover from blackouts, despite telecoms networks lacking the necessary power autonomy to do this.

- Our work identified the fundamental importance of standards to security, as well as the impact that minor influence and input to standards can have in eroding security, or creating an uphill slope the UK would need to contend with to keep its networks secure. Since telecoms networks are inherently interconnected, international standards drive the attack surface and interfaces we expose, as well as the security architectures around these. Outwardly benevolent influence in standards can be used to undermine or erode our security, and we believe the UK should approach standards with a "security first" approach and make the most of our historical strong influence in standards groups around security topics to deliver on this in a coordinated way, putting security first, and using this to drive maximum influence in standards bodies. We should explore opportunities to work with BSI, our National Standards Body, among others, to grow an international position of leadership in securing standards, and use security to drive and underpin our standards input – in the longer term this will help raise the bar internationally, protecting our allies and partners, as well as in ensuring the UK is best-placed to leverage strategic alliances for wider influence in standards as a result.

- We also discuss a range of other enabling and future technologies and technical changes, although again reiterate our core observation that, in many cases, the primary need is for adoption and uptake of current and long-extant best practice (and practical and applied work to focus on ensuring adoption of best practice and mitigations), rather than more R&D to develop new best practice that will not be adopted and therefore not actually benefit the UK in securing its telecoms networks. Despite mitigations existing, they are not being deployed, resulting in the same avoidable security issues affecting our networks consistently over years.

- Finally, we highlight the strategic challenge posed by the UK not having a long timeframe approach to key security topics (on a cross-party, 20+ year time horizon). The UK and its allies face threats and challenges to their security, posed by adversaries and foreign powers which do not share our common democratic values and respect for fundamental freedoms. These adversaries are able to adopt long-term positions more easily, which give them an advantage in their attempts to undermine our security. An example of a long-term strategy being done well by a key UK partner is South Korea's "Informatization Strategy", taking a long-term 40+ year view on technology (1).

(1) National Informatization Policy in Korea: A Historical Reflection and Policy Implications | Published in Journal of Policy Studies (scholasticahq.com)

CONTENTS

1/ Introduction & Summary

This report provides an insight into telecoms security. It has been drafted with input from Expert Working Group (EWG) members, observers, and guest speakers from related international organisations to bring together collective expertise in specialist areas to explore the opportunities, gaps, and challenges for the security of the UK telecommunications ecosystem.

This report presents a set of findings designed to advance recommendations that can support telecoms security policy development by the Department for Science, Innovation & Technology (DSIT), based on expert insights. This release of the paper focuses on the security of today's telecom solutions, and gaps in adoption and uptake of the outputs of R&D activities, to understand how R&D can better have an impact on improving the security of the UK's networks. To do this, we review past security problems, since many of these remain as today's problems; then we take a forward-looking view of likely issues into the future. The intent is to produce a second report to propose recommendations and a roadmap for security in telecoms, based significantly on the solid evidential foundation generated by this report.

References in this paper to security-related incidents are provided through press releases from media, government announcements, or global reports from across the world. This presents the best available view of what is happening in a rapidly evolving ecosystem, based on real insights from ever-evolving security threats, as, for commercial or other reasons, security incidents are not always reported in full technical detail from primary sources.

The remainder of this section provides a summary of current telecom security problems and challenges for this sector.

Introduction & Summary

1.1/ Telecoms Security Today – the extent of the problem

In the context of security, telecoms vendors and operators are faced with new legislation, a shortage of skilled people, gaps in education and attainment in in-depth digital skills (on which the future of the economy depends), and regular headline security incidents from across industry, healthcare, government, academia, and charities alike. Perhaps most worryingly, there is a general and fundamental lack of understanding that along with the great benefits of the internet, it has also brought about a great decentralisation of power and an exponential increase in security risk. This means that it is now equally possible for a state-sponsored actor or lone individual using a vulnerability to compromise a national telecoms operator. While state-sponsored actors will have more resources available, such attacks are not resource-constrained.

There is a perpetual challenge in security, in that cyber security breaches are often explained or rationalised as being of high sophistication and complexity, to attempt to excuse the breach having occurred. Often this may be part of a strategy around crisis communications or deflecting scrutiny from the real reason for a successful and preventable attack (2,3). This presents a harmful and challenging narrative to Government and other stakeholders, by suggesting that the attackers' sophistication makes the problems highly intractable and requiring further research to address. This is not necessarily the case – as was a recurring theme of public presentations given by Ian Levy as then -Technical Director of NCSC (4):

"The context in which you judge something also influences how you interpret it," he told the audience at WIRED Security in London. Media coverage of cyberattacks is crammed full of scary buzzwords. Cyberattacks – invariably represented by a lone hooded teenager in a dark room – are described as 'sophisticated' and 'unprecedented.'

Indeed, in 2017, Ian Levy, then-Technical Director of NCSC, said (5) of the incident where a telecoms operator was compromised, "exploiting a vulnerability that was patched in 2012 is not advanced", and that "I do not believe there was a telco in the UK that got done by a SQL injection attack by a fifteen-year-old, allegedly – sorry, it hasn't gone to court yet [...] I don't believe you get to call it sophisticated or advanced when the vulnerability is older than the perpetrator".

(2) Cyberattacks: Just How Sophisticated Have They Become?, Article by Leonard Kleinman Forbes Councils Member
(3) FullFact.org Article: How sophisticated was the "sophisticated" cyber attack against Labour?
(4) Hackers are 'not as sophisticated as they think they are', Wired Article by Matt Reynolds
(5) Nation Scale Cyber Security, Abstract by Dr Ian Levy

Introduction & Summary

This is a real “code red” situation, and yet it seems we are not improving, even with many years of experience of these issues.

The telecoms sector, in particular, faces a unique problem, in that its networks must inherently be exposed to the entire world, to facilitate the global connectivity that users and businesses expect. Without this inter-connectivity, there would be no global internet. It does not take much to look at moves in other countries and regimes, which do not share our democratic values and support for rules-based order, to see what can happen when the security and integrity of telecoms networks is deliberately undermined in order to, for example, support control of access to information by domestic populations; as well as to gain influence over their overseas adversaries, including the UK and its allies.

Since telecoms networks are inherently exposed to every other country, we cannot take an isolationist approach, simply unplugging the cables, or closing our eyes and blindly hoping we will remain secure. We must instead embrace the challenges head-on and take (and continue to take) meaningful technical steps (specifically including driving adoption and uptake of the outputs of existing R&D) to improve the security of our networks. This needs to be a multi-sector initiative – neither government(s) nor industry alone can solve these problems. They must instead work together to solve them, using both technical progress, and policy along with legislation where appropriate.

Another risk arises from the requirement to implement international standards in telecoms, in order to interoperate with other telecoms networks, while those who wish to gain access to our networks covertly or illicitly are also heavily engaged in the development of international standards, with the same (or a louder) voice than ourselves.

1.2/ Key Challenges for the Sector

There are several key challenges that this report highlights, although, perhaps unexpectedly, we believe that they are already identified and well-understood problems – rather than requiring "new" innovation or research to deliver; the tools and technical capability to solve most of these already exist. For example, while many point to the rise of "generative AI" tools as a threat, these simply just produce "output", which could be provided as "input" to a system. If a system is vulnerable to the application of arbitrary/invalid input, then it was vulnerable in the first place, regardless of the rise of generative AI – for example, SQL injection and XSS attacks illustrate why user input cannot be trusted. Tools to modify and tamper with inputs already exist today (i.e. fuzzing tools) – the underlying problem there is a well-understood issue of relying on untrusted user input. Similarly, the risks of quantum computing to asymmetric cryptography are real, however have been talked about since 1994 (6).

Instead, we need to focus on how to deliver adoption and uptake of these extant solutions, which is more a challenge of skills, technical capability, knowledge, incentives, and policy. Many of these challenges are ultimately driven by a pressure to reduce costs, rather than invest in infrastructure and security.

This presents significant opportunities for the UK, but it also means that we must approach these challenges in a far more "joined-up" way than we have to date. Many of these are not newly identified challenges, but ones which have been systemic for many years. Since technical solutions to many of the problems plaguing telecom networks already exist, many key relevant standards already exist that we will have to work with into the future, and telecoms is generally an adopter of technologies developed in the IT sector, the reality is that we already possess much of what we need to solve these problems. The particular challenges we have identified are:

- Skills, talent, leadership, and role models for the telecoms industry, to attract and retain the most technically competent people, and create a "tech-first" telecoms sector (where technical knowledge and expertise guides and steers organisations) with the capabilities needed to defend the UK, its allies, and their critical infrastructure. This also includes retaining the experienced talent needed to manage the security of legacy telecoms equipment (such as the early signalling defined for telephony in the 1970's and still in force through ITU, known as SS7 (7) and other legacy signalling systems).

(6) IEEE Document - Algorithms for quantum computation: discrete logarithms and factoring
(7) ITU Q.700 : Introduction to CCITT Signalling System No. 7

- Culture, business models, and "over-financialisation" of the telecoms sector resulting in a lack of investment in security capabilities (8,9), and the treatment of security as an intangible non-differentiator, rather than as a "cost of entry" ("A lack of commercial drivers because consumers of telecoms services do not tend to place a high value on security compared to other factors such as cost and quality" (10). This also includes the concerning differences in culture between telecoms and other Critical National Infrastructure (CNI) sectors.

- For a variety of reasons (including, but not limited to, information asymmetry between vendors and buyers; a historical lack of incentive and expectation to manage security risks as technical priorities; and a focus on price/cost, as opposed to quality and security), there is and has been a general failure to implement and apply existing technical best-practice and tools to mitigate security vulnerabilities, and to better design infrastructure to be inherently secure against attack, and create a meaningful step-change towards all infrastructure being "secure by design and default". To some extent, this is due to a cultural difference between the IT world, which favours regular patching, at the expense of resilience and reliability, and the telecoms world, which favours system stability and change control, rather than rapid software deployment. This approach no longer works as telecoms networks deploy and depend on the security of full-scale IT stacks for their infrastructure.

- Modern telecoms networks are heavily adopting IT technologies, i.e. commodity off-the-shelf (COTS) hardware, software, operating systems, hypervisors, and container orchestration platforms such as Kubernetes, significantly widening the attack surface and critical technologies whose risks need to be managed in telecoms networks.

- In the wider UK economy, businesses (large and small alike) often fail to recognise the enabling power of IT and telecoms technology, and therefore what they stand to lose if they fail to invest appropriately to secure these technologies that enable their businesses to grow successfully. Few businesses wish to revert to a 1980s pre-internet economy without online sales, but few have invested significantly in securing and protecting the infrastructure which has grown their turnover immensely. There are also challenges in suitably encouraging/incentivising companies to adequately invest in security more generally (11,12).

(8) Bert Hubert Article, How Tech Loses Out over at Companies, Countries and Continents
(9) Bert Hubert Article, 5G: The outsourced elephant in the room
(10) DCMS, UK Telecoms Supply chain review report
(11) The Conversation Article, Why companies have little incentive to invest in cybersecurity, by Benjamin Dean
(12) Tech.co Article, Less Than Half of Large US Businesses Investing in Cybersecurity Despite Major Concern, by Jack Turner

- A loss of influence and at-scale presence in international standards fora, through a decline in the number of relevant telecoms vendors in the UK (due to acquisitions), to the extent that the UK no longer has any major telecoms equipment vendor left. This makes it harder for UK innovators to follow the direction of travel and makes it more difficult for us to gain influence in standards in future, through a reduction in people familiar with and respected in standards development organisations. These standards set the norms for the technologies we deploy, and how our networks interconnect with overseas networks, and therefore effectively dictate the security posture of our networks.

The task for this UKTIN EWGs was and is to look at R&D questions and come to conclusions as to what the future direction of R&D should be, along with relevant recommendations (these recommendations will be the focus of our second paper). As this paper makes clear, the UK already has much advanced R&D, but in Section 6.7 (Learning from systemic threats) we have identified a gap around a general failure to adopt best practices and take heed of the security recommendations and best practice set by government and industry alike.

1.3/ Telecoms Security and its impact on wider critical infrastructure

Another key factor when considering the security of telecoms networks is the extent to which telecoms networks are also key underpinning enablers of wider critical infrastructure, and therefore how the supply chains of telecoms operators become the implicit supply chains of other critical infrastructure users who rely on telecoms networks.

Currently telecoms operators are focused on implementation and compliance with the Telecoms Security Act (TSA)(13), which currently sets out a holistic level of expectation around security from telecoms operators, and goes much further than other security legislation (such as NIS) in having the facility to designate high risk vendors, require their removal, and also stipulate specific expectations around measures taken by operators to secure their networks, including their upstream equipment supply chains. Other CNI sectors, however, began this process five years ago, with the passage of the NIS Regulation (2018). While the initial position of the NIS Steering Group was that telecoms should be covered, in the final version, telecoms was expressly excluded (14), because of industry lobbying.

While the adoption of the TSA means that telecom no longer sits outside of the scope of modern cyber-security regulations, a key finding and conclusion of the second post-implementation review of NIS highlighted the importance of securing "the supply chains of operators of essential services, where the supplier is critical to the provision of that essential service." The telecoms sector increasingly is a critical component of the supply chain of our wider economy, and other NIS-covered critical infrastructure sectors. It therefore likely makes sense for telecoms to be recognised as the key enabler (that it is in providing control and information communication capabilities for other critical sectors), which may merit a more "hands-on" approach to Government setting regular expectations of operators, to ensure that they deliver appropriate levels of security that meet the needs of the UK.

To understand the challenges surrounding supply chains it is useful to consider the results of a study undertaken by Topping et al (2021)(15), which identified that there are different interpretations of what is classified as a supply chain. The researchers undertook a review of advice and guidance about Cyber Supply Chain Risk Management (C-SCRM) provided to authorities in the UK, US, and EU, alongside sector specific guidance for chemical, energy, and water sectors.

(13) Telecommunications (Security) Act 2021
(14) Recital 7 of Directive (EU) 2016/1148
(15) Topping, C., Dwyer, A., Michalec, O., Craggs, B. and Rashid, A., 2021. Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Computers & Security, 108, p.102324

They explained that the differences in interpretations "resulted in a diversity in the quantity and quality of advice offered", which was "exacerbated by a lack of common taxonomy to support supply chain procurement and risk management". Following this study, the researchers concluded that there is a need (and desire) for a common taxonomy and are proposing that an initial framework be divided into four categories: ownership, risk, services, and end-to-end. These four areas capture and reflect the breadth of challenges surrounding the supply chain security.

Indeed, in the summary of NCSC's security analysis for the UK telecoms sector (16), it noted that (emphasis added):

- "The trend in the telecoms industry is increasingly to outsource and/or centralise functions, into international locations. This approach may be applied to business decisions, technical decisions, management processes and security processes. Business decisions, such as procurement decisions, are increasingly taken within an operator group HQ.

- The most significant risks due to this trend are that business decisions may be taken without an understanding of the local threat to the environment and without full consideration of the local context or local risks.

- One business decision is to operate UK networks from outside the UK. Networks are increasingly designed, operated, maintained and secured from lower cost international 'hub' locations – this is likely to be further exacerbated as network functions become more cloud-based, and potentially no longer hosted in-region. This presents network availability concerns should there be an international connectivity issue and it increases the complexity of securing the network."

(16) Summary of NCSC's security analysis for the UK telecoms sector

2/ Scope of Paper and Interdependencies

Our focus in this paper is the security of telecommunications networks, recognising that telecommunications networks and services are now built on the same technology and platforms that underpin wider off-the-shelf business IT systems, albeit with highly specialist and customised telecoms-specific applications running on them to support business, society and people.

Consideration of security is part of a policy mix that needs to include many other ingredients to be successful (e.g. skills, scale, long-term strategic planning, standards, regulations, adoption, best practices, targeting and etc). UK Government reviews the situation regularly for security (17).

We provide our perspective on standards (section 3), the SWOT on UK's position (section 4), skills (section 5) and regulation (section 10).

Security has a dual role: i) the technologies that support and enable telecom security capabilities; and ii) the technologies, systems, applications, and people (human error being the source of 95% of security problems (18)) that use security and communication capabilities in their own ways. The former, is covered in sections 7 (security evolutions) and 9 (R&D and adoption). The latter is covered in sections 6 (the security toolbox) and section 8 (Critical National Infrastructure).

Other UKTIN EWG domains also have this dual role for technologies under their studies while there may be multiple interdependencies between them. Security is unique, however, in spanning all domains and having a wide range of basic capabilities that assure security of domain-specific functions such as: the control plane, management plane, and user plane of a telecom system. It also provides a rigorous approach to using those functions to better protect all types of users. We highlight AI as a particular example of this. The impact of security failures is also unique in the extent of their consequences on the users due to flawed implementation, failure to adopt mitigating measures (Section 9.1 Barriers to Adoption explains this in detail), or poor risk assessment, validation, and maintenance (hence the toolkit – Section 6).

(17) UK Gov't, "2022 cyber security incentives and regulation review", 19 January 2022.
(18) World Economic Forum Report 2022, 17th edition, p45

Scope of the Paper

The “security toolbox” approach is a key element, that seeks to identify key topics (or tools) that would be of greater or lesser relevance to other EWG’s and other stakeholders, such as policymakers, depending on their particular subject. We believe this will also make our output clearer and more digestible and actionable, in a sector that is often anything but. We are mindful that policymakers will not always have complete sight of the finer detail of a security landscape that changes continually, and the intention is that by using this topic-based approach it is possible for them to revert with questions on any topic that grabs their attention and/or where they seek a deeper understanding.

3/ Security and the link to standards

An important consideration around the security of telecoms networks is the extent to which potential solutions already exist to some of the systemic and underlying challenges in security, but our ability to implement these may be restricted by the need to deploy equipment in line with international standards - to preserve global interoperability and enable features like roaming (as well as achieve economies of scale for operators). Otherwise, our telecoms networks simply would not work. Section 6.7 (Learning from systemic threats) sets out examples of the top vulnerabilities in software, and demonstrates that effective controls and mitigations to these issues are already known. In this section, however, we explore the impact that standards have on our ability to operate secure and resilient telecoms networks in the UK.

It is important to note that security, particularly in the context of telecoms equipment, is an ever-moving battleground, and one that effectively entails a recursive set of activity to manage and reduce risks, and mitigate or control for new risks as those emerge – "security is a process, not a product." (Bruce Schneier, 2000). In telecoms, a new "G" emerges roughly every 10 years, and there is generally a mid-generation equipment refresh cycle after around 5 years. This leads to continual evolution and roll-out of new products and features. With 5G becoming increasingly software-based, and with vendors seeking to deliver new software releases more rapidly and iteratively (perhaps monthly rather than annually), this will require more rapid iteration and evolution of defensive measures to keep up. In other words, every time a new generation of network equipment, based on the latest release of 3GPP, is deployed in the field, this introduces a change to the process and hence a potential new set of security vulnerabilities.

The term “standards” is a broad one, with a wide range of potential interpretations and meanings in different contexts. In the context of telecoms and security, the following definitions are relevant:

- Formally ratified “de-jure” international standards (for example, standards from ETSI ; IEEE; ISO; standards committees). Note: The Internet Engineering Task Force (IETF) is not a de-jure body but its specifications, (so-called Requests for Comment – RFCs) and security RFCs in particular, are the basis of the 3GPP introducing 4G LTE flat architecture based on IP networking. Many industrial applications that use telecoms also use these security RFCs.

- Informal “de-facto” standards (which gain their recognition through industry adoption and uptake).

- National guidance and best practice (usually issued by Government National Technical Authorities, such as NCSC, and previously CESG, or Government departments)

It is important to understand how these layers work together.

3.1/ De-Jure Standards

In telecoms, the underlying infrastructure is generally built around 3GPP standards - each "G" refers to an IMT specification within ITU-R Working Party 5D. In general terms, a "G" corresponds to a point in time where a given release of standards is ratified to meet the IMT specification – for example, 5G generally refers to 3GPP-Release 15 or above, and corresponds to the IMT-2020 requirements).

These standards define the physical interfaces, network architectures, features, security measures, and similar that create interoperable global networks – and explains why standards is a cross-cutting topic. It is essential for interoperability that telecoms networks implement these standards correctly. Vendors also do not want bifurcation of standards for individual markets, and seek to deliver better value products through international economies of scale, that arise because of international harmonisation of standards.

This also means that the security of our telecoms networks is fundamentally set by the standards that are ratified and adopted. It is often difficult (or impossible) to raise security beyond that covered by the standard, while preserving interoperability with the global market.

3.2/ De-Facto Standards

There will also be informal de-facto standards that overlay on top of this – examples of this in the UK market could include mobile number portability (MNP) procedures for conveying information about ported numbers across operators (19) - this is effectively an agreed de-facto standard for how number portability works in the UK market, and operators adhere to this to deliver a functional number porting system to meet their obligations under Ofcom's General Conditions of Entitlement (General Condition B3). Beneath this system sits the exchange of Microsoft Excel documents over SFTP or ISDN to communicate information about ported numbers, and the provision of onward indirect call routing to the new network. This is a good example of a UK market specific standard, adopted by the market, to meet an obligation.

(19) MNPOSG Mobile Operator Guide Version 8

3.3/ National Guidance

Finally, there is national guidance and best practice, which can become a form of de-facto standard, but which is often issued by Government on security grounds. An example of this is that NCSC has previously issued guidance to telecoms operators around the use and management of security risks posed by high-risk vendors (20), which states that operators should not deploy equipment from more than one High Risk Vendor (hereafter "HRV"), as NCSC's assessment is that it is not possible to manage the risk posed by equipment from multiple HRVs in one network. This guidance becomes an effective form of a lightweight standard, in that it becomes an expectation and constraint in the operation of a network. Similarly, NCSC guidance also expects operators to use two vendors' equipment in their radio access network for resilience purposes (21).

This illustrates the extent to which either formally ratified or de-facto standards and guidance influence and ultimately steer and drive what is deployed.

3.4/ Standards and Interoperability drive telecoms

Nonetheless, there are important factors to note here – even where we may have the R&D capability to solve security problems in telecoms infrastructure, unless it can be deployed in a manner that is in line with standards, it will be difficult or impossible for the UK to benefit from its R&D. Doing so may break interoperability and compatibility with other markets, and inhibit roaming, international calling, or cross-market handset compatibility. This would have significant economic impact on the UK, restricting international trade and communications, as well as significantly increasing the costs of communications services, and likely also attracting significant international criticism, including from both UK operators and vendors.

UK-based vendors would also be less competitive, as their products would struggle to gain international adoption, given the UK would develop a reputation for "going it alone" and not following international standards (so their products would likely not work overseas). This would be detrimental to the national interest, and further, a failure to engage with the security standards process in particular might limit our ability to make the most of standardised features that help to keep the public safe (such as lawful intercept capabilities).

(20) NCSC advice on the use of equipment from high risk vendors in UK telecoms networks
(21) NCSC The future of telecoms in the UK

As such, this means that international standards committees become a core critical path component of the telecoms security landscape, and it is relatively futile to consider telecoms security without also considering the standards development, evolution and ratification process as part-and-parcel of this. Otherwise, UK activity and strength in improving telecoms security will ultimately struggle to gain adoption internationally, and therefore we will not see the benefits of these changes that DSIT seeks to deliver.

While not every improvement in security will require international adoption and uptake, and there are many areas where the barriers to uptake of better security practices are not dependent on international standards but rather on organisational culture, mindset and incentives (See Section 6.5 on Adjacent factors surrounding attitudes to security i.e. culture, mindset etc), some of the most fundamental aspects of security postures require international cooperation – for example, the encryption and authentication algorithms implemented and used on handsets and SIM cards, cryptographic parameters and key schedules used in infrastructure, downgrade and backwards compatibility support, and protocol version negotiation protocols, as well as deprecation schedules for legacy or null authentication and encryption modes, etc.

As a hypothetical example, if certain actors were to advocate at international standards committees for continued default support for EIA0 and EEA0 (i.e. null integrity checking and encryption schemes), this would aid and facilitate the execution of ciphering downgrade attacks against devices internationally. While arguably some handset manufacturers could introduce optional user-facing options to change this behaviour (as some Android devices have done to enable disabling of 2G network support on handsets) (22), this needs to be opt-in (meaning it will not be secure by default), to avoid users unaware of the feature from returning their handset as non-functional.

(22) Electronic Frontier Foundation Article, VICTORY: Google Releases “disable 2g” Feature for New Android Smartphone by Cooper Quintin

To materially benefit the security of our telecoms networks, as well as to enable the UK to make use of any influence and capability it grows in this area, it will be essential for work in security to evolve hand-in-hand with standards. Given the extent to which standards and security are inherently interconnected, we make an early recommendation that DSIT considers how best to enable security and standards work to be connected, as is the case in wider Government, both in the UK and our overseas allies. At a recent ETSI security event, UK NCSC and DSIT, German BSI (Federal Office for Information Security), and US NIST all spoke about the inherent interrelations of standards and security. We are clearly not alone on this point, and it is important that the UK is not left behind.

Furthermore, DSIT is already working on such a strategy, as the PSTI Regulations 2023 (about IoT security and coming into effect 29 April 2024) prove. Its main aims are to:

- Ban universal and easily guessable default passwords
- Ensure manufacturers have a point of contact for reporting vulnerabilities
- Ensure consumers are told how long products will be supported for

“The UKs new product security regime will be the first in the world to require minimum cybersecurity requirements before consumer connectable products are made available for sale to UK customers,” (23) as DSIT proudly claims. They also state that the work is rooted in the ETSI EN 303 645 standard. It is clear that DSIT already understand the importance of working to international security standards.

(23) ETSI Cybersecurity International conference presentation by DSIT 17/10/23

4/ Sectoral SWOT Analysis on the UK's position in telecoms security

The EWG met in-person in late October 2023, amongst other things, specifically to carry out a SWOT analysis for this paper. Although we were able to identify a wide range of factors, the scale of change required concerned us. Critical is the need for a longer-term strategic vision – by which we mean an adequately resourced "20-year plan and not a 20 minute one." (24) Just as the Far East has learned from us, so can we learn from them. What we have in mind is the adoption of an "Informatization" type strategy as was so successfully done in South Korea (25).

4.1/ UK Strengths

1. Impressive track record and still internationally "rated" in telecoms.
2. Regulatory clarity (though TSA impact yet to be felt and might not deliver as expected?), and the potential for the UK TSA to drive overseas security standards via adoption of similarly worded measures.
3. Historic reputation for world-leading research globally, but with a need to close the loop on innovation to adoption.
4. A strong base of innovative companies, with the rise of alternative network providers (130 to 150 small and large regional providers), competing with the incumbents, and winning.
5. As an island, we have opportunities for R&D with slightly reduced interference and frequency coordination requirements with neighbours, making it possible to innovate and move faster.
6. A potentially unique amount of thriving competition in the infrastructure layer of telecoms.
7. A very strong set of skills in our "niche/boutique" telecoms consulting industry, which is used to advise operators globally.
8. A strong legacy from the 5G Testbed & Trials programme creating an ecosystem of innovators and private network system integrators.
9. The UK's proactive stance on HRVs is forcing a greater "willingness to pay", while reducing risk to networks, and also creating incentives for new entrants.
10. Telecoms is the second largest infrastructure investment in the UK – second only to HS2.
11. We have the researchers and applied R&D to answer many of the security problems we face – the UK is a nation of SMEs (small and medium enterprises). Our challenge is in getting these into deployment quickly.

(24) Comment overheard at launch of DSIT Open Networks Ecosystem launch day 14th September 2023
(25) National Informatization Policy in Korea: A Historical Reflection and Policy Implications, Changhee Lee

4.2/ UK Weaknesses

1. No long-term cross-party strategy on telecoms and technology, as is evident in other countries such as South Korea and China.
2. The UK no longer has "critical mass" in the sector as either a manufacturer or large customer.
3. No major UK telecoms vendors left, so limited visibility of standards that drive security, and limited influence on standards.
4. Complex funding landscape that funds in a piecemeal manner (i.e. part-funding some R&D, but not funding standards participation, etc.)
5. Academics forced to compete not cooperate (while other countries benefit from near-unlimited R&D funding and backing) there must be a better way.
6. Lack of clear ownership and accountability for the Government risk-holder in CNI (such as telecoms) – NCSC as NTA; DSIT as lead government department, CO as lead on resilience.
7. A mature financial market for infrastructure investment leads to a short-term focus on regular returns (leading to market consolidation), and asset "sweating", rather than on ongoing investment into security (which would erode on those returns on investment). We see our telecoms infrastructure as an investment vehicle, rather than as a piece of long-term critical infrastructure.
8. Skills and people – many of the technologies we have available to protect our networks require a deep understanding of how things work, in order to use and configure them correctly, and this knowledge is often lacking, or in very short supply.
9. A "certification mindset" – industry love certifications as a point-in-time stamp of compliance (which introduces the risk of compliance-washing of certifications, where they are eroded to the point they are ineffective). This leads to compliance theatre, where everyone defers to the certification scheme rules, regardless of their relevance, efficacy, or appropriateness.
10. A lack of risk-taking capital investment for businesses making the UK less attractive for innovators than the US market, due to lower early-stage valuations and a desire for investment propositions to be "de-risked" while still priced at venture levels of equity.

4.3/ UK Opportunities

1. Rebalance the UK government's R&D portfolio to focus on better exploiting the impact, synergies and innovation in areas of known commercial interest to get better progress.
2. The Standards problem could be fixed but this would require a longer-term cross-Government strategic vision, which we believe is currently missing.
3. User awareness and skills could be improved using new methods (old have failed).
4. Still seen as a "trusted partner" internationally, although our soft power is eroding – there are however recent examples of good practice, such as around ETSI EN 303 645 (Consumer IoT security).
5. Improved cross-government cooperation to bring about the changes needed – including in government – at pace.

4.4/ UK Threats

1. Lack of appetite. The on-going "Standards Explosion" requires "fixes" that necessitate a radical departure from existing ways of working and higher costs – including in government. Is the will there?
2. The speed at which threat landscape changes is constantly accelerating as networks and capabilities improve.
3. Our historic international influence is declining – no longer seen as "leaders".
4. UK Drive for Open Networks increases available attack surface, increases risk of "faux interoperability" and lower barriers to entry for attackers.
5. No layered secure mapping solutions yet in place – though some data freely available. Let's not make it easy for attackers!
6. New approach to skills gap still not adopted.
7. A lack of credible available "exit" strategies for innovative start-up businesses – the options are generally to publicly float through an IPO, go through a corporate acquisition (M&A), or have a private equity buy-out.

We have heard much talk of the UK's technology position being weak, and this seems justified. We no longer have any manufacturing at scale and consequently have lost visibility and influence of the standards driving key areas where they used to participate in the key relevant working groups. We have a long history of world class R&D, yet we have not managed to translate that into economic benefit at scale, we were pioneers in GSM, now we lag other developed economies. We have for decades had a skills problem, yet it remains unresolved.

We are also familiar with the narrative, heard even within UKTIN, that the UK has pockets of excellence "that we need to link them all up better". We already know via DSIT of plans for the UK to explore a possible Future Telecoms Institute, that may seek to address this, and about which we hope to learn more detail from DSIT in due course. We would, based on this SWOT and our experience, make the following remarks:

1. If this is done then it needs to be done at scale to have impact.
2. Why would the UK even want to be active in all sectors anyway – some are low value? We are a high-wage economy and cannot realistically compete with low-wage economies, so must be strategic in where we add the most value and benefit most from influence.
3. The resulting R&D ecosystem will inevitably involve more Universities than today, ideally specialising in different areas so there is less overlap and need for "competition to allocate funding".

We will be looking at our conclusions in a second paper that follows this one and makes a series of specific evidence-based recommendations.

5/ Skills

To ensure long-term resilience of the UK's security capabilities it is vital to embed an appreciation of skills requirements, challenges, and opportunities. This section of the report considers these three components to develop a better understanding of the current situation, which will then be built upon in our recommendations paper. When considering the situation with skills and security, it is necessary to focus on the diversity and inclusivity of the cybersecurity sector, and it is widely acknowledged that there is currently a lack of adequate diversity and inclusion. This section of the report therefore also examines the current context of cybersecurity diversity, why diversity is important, and examples of good practice across the cybersecurity sector. Here we combine consideration of diversity and inclusion because those who hold different identities must feel valued, able to be themselves, and able to access equal opportunities and resources.

Operationally, a more diverse and inclusive sector will inevitably provide wider insights into R&D problems than would otherwise be the case. That will in turn lead to better research outcomes than would otherwise be possible. We are particularly mindful in the security world of the appalling treatment of one of Britain's most brilliant minds, Alan Turing. What might he additionally have been capable of had society at the time been more diverse and inclusive? Given that the internet is global, never has it been more important to ensure that the way we approach security is also as wide-ranging as possible, and that we approach problems with a "hive mind" mentality that values inputs from whenever they might come, so long as they add value.

5.1/ Skills requirements, challenges, and opportunities

The skills shortage is often cited challenge across the tech sector, but especially within discussions about cybersecurity. A 2023 report featuring research undertaken by IPSOS on behalf of DSIT identifies that "a high proportion of UK businesses continue to lack staff with the technical skills, incident response skills and governance skills needed to manage their cyber security" (26). This lack of skills has a significant impact across society and within companies, notably, findings from this research from IPSOS highlight that "half (50%) of all private sector businesses identify a basic technical cyber security skills gap" (27).

(26) Coutinho, S., Bollen, A., Weil, C., Sheerin, C., Silvera, D., Donaldson, I.S. and Rosborough, J., 2023. Cyber security skills in the UK labour market 2023. Department for Science, Innovation and Technology (DSIT). Accessed Oct. pp1
(27) Ibid (in the same source)

Whilst the skills shortage is often presented as an issue, we wish to take a more optimistic approach and highlight the opportunities surrounding skills. Key to the development of cybersecurity skills is a strategy with breadth. The increasing interconnections of telecoms with multiple sectors and societal dependence means that cybersecurity skills also need to be broad. Skills development activities therefore need to work across the STEM and non-STEM divide to help develop the talent pool. This is already occurring with initiatives pushing for broader engagement, including the Cybersecurity Council's Cyber Career Framework, which provides ideas and guidance across and between 16 different cybersecurity specialisms.

5.2/ Skills, Diversity, and Inclusivity

Considering the skills requirements, challenges, and opportunities necessitates an examination of diversity and inclusivity. The more diverse the cybersecurity sector is, the wider the talent pool working to develop secure networks, and thus the more resilient networks will be. In discussions about diversity, it is important to identify why diversity within the cybersecurity sector is important. When diverse groups work on cybersecurity, challenges and opportunities can be more effectively and efficiently identified and evaluated. As then Ciaran Martin, the CEO of NCSC, identifies, diversity provides a "mix of minds and fresh perspectives" and "we have a moral duty" to ensure there is diversity (28). The wider the talent pool of individuals engaging, working on, and understanding cybersecurity needs, the more resilient the networks, and country will be. Ensuring that the cybersecurity sector is diverse thus embeds digital resilience across the sector.

In order to have enough suitably qualified and skilled people to secure our networks, we must embrace diversity. It is also important to ensure that we make telecoms security workplaces attractive compared with other options – including recognising technical excellence and establishing technical leadership chains throughout the organisation (since technical leadership chains are likely to be more attractive to many individuals than more traditional managerial leadership chains).

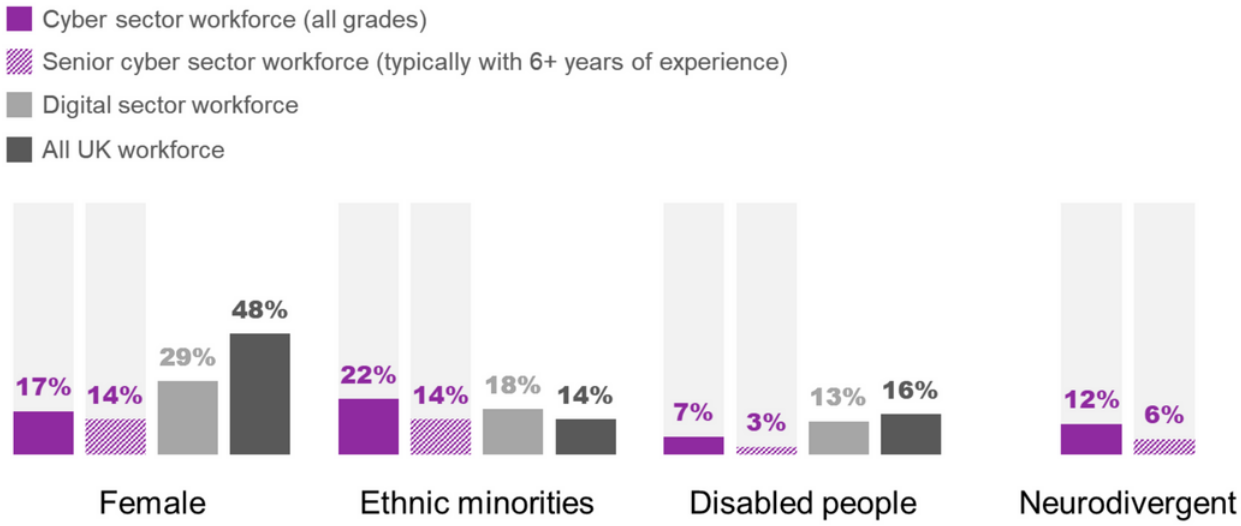
(28) NCSC & KPMG (2020), Decrypting Diversity PDF Report

The question of diversity expands across multiple identities, from ethnicity to gender, from sexual orientation to neurodiversity, and from disability to socioeconomic background (and others). A crucial point when discussing diversity is an appreciation of intersectionality which foregrounds how different identities may intersect, for example, someone who is a black woman, or someone who is a neurodiverse transgender person. The lived experiences of these people are shaped by both (or more) of their identities; it is not possible to neatly categorise people. Indeed, it is also important to be aware that some of these identities may not be visible, for example, disability, sexual orientation, and neurodiversity. The need to take an intersectional approach is increasingly being called for within the cyber industry, as Dr Anne-Marie Imafidon MBE (Co-founder and Head of STEMettes via NCSC and KPMG, 2020: 33) articulates: "Talent, irrespective of protected characteristics, is so required by the cyber industry... I'd like to see a more intersectional approach taken swiftly, to ensure that we're not losing people faster than we can recruit and promote them. There is work to be done to break entrenched habits, ensure competent handling of incidents and rebuild social norms. How can talent that is, for example, black, female, lesbian or a combination reach their senior leadership potential?" (29).

Despite, the difficulty in categorising identities, to understand the current context within the cybersecurity industry (and therefore the need for action) it is necessary to focus on specific identities as this is where the data currently lies.

(29) NCSC & KPMG (2020), Decrypting Diversity Page 33

Percentage of cyber sector workforce that come under the following diverse group (via Ipsos and DSIT, 2013, page 19)



Bases: c.150-180 cyber sector businesses for all workforce estimates
(in each case excluding those that were not able to answer these questions, or refused)

The above graph from a report by IPSOS and DSIT (2023) (30) includes reference to senior cyber professionals, which they define as someone who has 6+ years of experience. Notable within this graph is the percentage of women within the cyber sector (17%) versus the number in the UK workforce (48%). This is also not confined to the UK with only 25% of cybersecurity jobs globally held by women in 2022. The gender diversity disparity is repeatedly cited as an issue facing the cybersecurity sector whereby much needed talent and skills remain untapped, and thus must be taken seriously (31). A lack of diversity in senior cyber professionals can also create a self-perpetuating problem, as it means young people looking at career options may not see role models they can identify with.

(30) Coutinho, S., Bollen, A., Weil, C., Sheerin, C., Silvera, D., Donaldson, I.S. and Rosborough, J., 2023. Cyber security skills in the UK labour market 2023. Department for Science, Innovation and Technology (DSIT). Accessed Oct. pp19
(31) Cybersecurity Ventures, (2022), Women in Cybersecurity 2022 Report

Although lower socioeconomic status is not a protected characteristic and is difficult to define, it is increasingly being recognised and considered within surveys about diversity within the cyber sector. Findings from NCSC and KMPG (2020) (32) indicate that those working in the cyber sector tend not to be from lower-socioeconomic backgrounds. Activities surrounding skills development are also increasingly engaging with people from lower socioeconomic backgrounds, for example, working with state school children and children who receive free school meals. It is also important to consider the intersection of lower socioeconomic status with other identities and how that may introduce extra barriers to engagement with cybersecurity.

Fundamental to an examination of diversity is an attention to inclusivity. A good way to understand this differentiation is via a report from NCSC and KPMG (2020) (33) which indicates that there is a similar level of ethnic diversity within the cybersecurity industry and the UK population, however, people not identifying as White or Asian have reported feeling less confident in being themselves within the cyber security sector. This highlights a need to consider more than numbers indicating diversity, but people's experiences of inclusivity.

Indeed, the report from NCSC and KPMG (2020) argues that "without an inclusive industry, the cyber security industry will not benefit fully from the diverse workforce today and in future" (34). The group agrees with this statement as a diverse and inclusive industry is needed for the full benefits and talents to be realised. Inclusivity is built from the culture within organisations and the wider sector, norms and expectations about how people act and engage with ideas, situations, and the world around them. Inclusivity is also built from the structures in place within organisations – are systems in place for identifying needs, accessing support, and reporting incidents? A focus on the culture and structures shifts the focus from the individual to the community (whether the department, wider organisation, or sector as a whole).

Inclusive working environments enables people to work more effectively and efficiently, as they are not having to navigate so many obstacles, and it can also foster a sense of community which in turn benefits people's work. A more inclusive working environment also enhances the chances of retention within the cyber sector, when people feel safe, supported, and able to be themselves at work it means they are more likely to stay working in that organisation and sector. Discussions about upskilling people within the cybersecurity industry must also address how to retain people once they have developed these skills, and therefore one part of that is considering how to create an inclusive sector.

(32, 33) NCSC & KPMG (2020), Decrypting Diversity Report
(34) NCSC & KPMG (2020), Decrypting Diversity Report Page 41

Fortunately, there are wide-ranging organisations and individuals working to address the skills, diversity, and inclusivity needs of the cybersecurity sector and shifting the focus towards opportunities. There are too many examples of good practice to list here, but we wish to draw attention to some which are making an important impact including:

- STEMettes, which is a social enterprise working to inspire and support girls, young women and non-binary young people to follow a career in science, technology, engineering, arts, and maths including cybersecurity.

- NeuroCyber is an organisation raising awareness, making connections, and working to foster inclusive environments. Neurodiversity is important for strengthening the resilience of cybersecurity activities, as NeuroCyber state, “it’s easier to think outside the box when you already live there” (35).

- CyberFirst is a programme of activities and bursaries from NCSC. It is designed to support young people explore opportunities and includes undergraduate bursary and apprenticeship schemes, a girls-only competition, and series of courses and recognition(s) for schools and colleges leading on cybersecurity education.

It is important to note however that these are general cyber security initiatives, and that similar challenges around skills and diversity are seen across the whole telecoms ecosystem as well.

(35) NeuroCyber.uk

6/ The Security Toolbox - Key Enablers

In this section, a number of key technical and non-technical enablers are explored, which could individually or collectively present mitigations to many of the security problems faced by telecoms networks, as identified earlier in this paper. It is important to note that these solutions already exist. What is required as the priority is not R&D into new solutions, but rather the understanding that they exist and need to be deployed, and a greater focus on innovation at later TRL stages to make it easier for these to be adopted.

6.1/ AAA (Authentication, Authorisation & Accounting) and Encryption

The purpose of AAA is generally to decide who or what can reach information or carry out a request and provide a layer of governance around actions carried out. In complex interconnected systems (like telecoms networks), these three functions provide the core underlying security framework that control access to systems and offer technical enforcement of security measures. Generally, few things are as clear cut as to "never" happen – for example, users with administrative rights (who can authenticate as such) will be able to carry out operations (such as rebooting systems) which other users should not be able to carry out. It is not feasible to simply say this can never be done – instead, AAA is used to prevent people who are not authorised from doing this, and authentication is used to check that they are indeed the individual they claim to be. The accounting layer provides for logging that records which user carried out which actions, which allows for detection of anomalies or security issues.

Of particular importance in this context is administrative access - we already know that 95% of security breaches happen because of human error (36), and one of the main weaknesses comes from problems with administrative access. This means it is especially important to manage access coming into any system vertically, as well as blocking any lateral movement (to stop hackers exploiting any toehold they might gain to move around the network. In many high-profile security incidents, weak authentication processes have been involved in attackers entering networks – for example, the Solarwinds supply chain compromise (37), Equifax around the time of their breach (38), and indeed T-Mobile USA's own network (39), where it appears that a GGSN (Gateway GPRS Support Node) was accessed from the internet to gain a foothold into their network (40).

(36) Global Risks Report 2023 | World Economic Forum | World Economic Forum (weforum.org) at page 45
(37) CNN SolarWinds Article by By Brian Fung and Geneva Sands
(38) Forbes Article: Equifax Lawsuit: 'Admin' As Password At Time Of 2017 Breach by Kate O'Flaherty
(39) BleepingComputer.com: Hacker claims to steal data of 100 million T-mobile customers by Lawrence Abrams
(40) Polymerhq.io Article: How did T-Mobile breach occur?

Given the tight interconnections and robust couplings of today's supply chains, lateral movement can today easily mean that a hacker can gain access to somebody else's network via yours, but of course with admin level access they can also get into your own management interfaces and move vertically through your network.

Approaches to access control are more a matter of good hygiene practices than they are advanced R&D. The priority must be the greater adoption of NCSC guidance (41), and the question how to get the importance of "best practice" in this domain. These are complex, however, especially in telecoms, where systems must inherently be interconnected in order to work – there is little value in having a telecoms network that cannot connect to other networks, even though these connections themselves give rise to security risks.

There are other approaches that can be used to securing systems, in addition to AAA – firstly, by isolating and securing management planes away from internet or user traffic, it is possible to fully isolate the ability to log in and manage systems from the access which regular users have. This means that privileged interfaces (such as SSH management interfaces) are not exposed to attackers, and attackers cannot reach them. In addition to management plane isolation, encryption and integrity checking on transmissions can be used to protect the confidentiality and integrity of these. While encryption is often heralded as a golden solution to cyber security problems, it is rarely this straightforward.

Encryption is a way to protect the confidentiality of information by scrambling it with an algorithm and key, such that it cannot be accessed without the key. In telecoms networks, encryption is used in various areas, such as between the handset and base stations, and to authenticate SIM cards to the core network. Encryption is not a silver bullet however – encrypted data is only as secure as the key itself is – if the key to encrypted data is held on the same system as the encrypted data, or the system holding the encrypted data can reach another server to request the key, or a decrypted version of the data, the encryption is ineffective. Encryption works when the key is unavailable and inaccessible to an attacker or unauthorised user.

(41) NCSC Vendor Security Assessment

Similarly, message authentication codes (MACs) and asymmetric digital signatures can be used to verify the integrity of messages, and as part of a robust authentication system. Despite this, they are not widely used as they ought to be – for example, smartcards and physical security tokens offer significant security protections against phishing and other attacks, and implement standards such as TLS client certificates, or SSH authentication using public keys or certificates. They are often eschewed in favour of passwords for ease of use. The technical solutions are available to build such robust systems, but the human factors and a preference for usability often results in these not being used. In the example of the T-Mobile USA exposed SSH interface, it appears that password authentication may have been available and exposed to the internet, based on the screenshot of alleged access to T-Mobile's systems (42).

It is critical when considering the application of AAA to understand which systems or functions it applies to, since AAA can be applied at physical infrastructure level, at platform/environment level, at operating system level, at application level, and indeed also at user level – each layer of the telecoms stack should consider principles and aspects of AAA. While compromising any one of these is likely to compromise the wider system, it is not sufficient to assume that AAA in another layer will provide integrity at another layer – for example, even though a telecoms network might have AAA built into 3GPP to cover user authentication, this would do nothing to protect the "lights out management" port on the physical server that hosts a network function, and vice versa. While the underlying platform must be secure to give confidence in a workload running on a system (and hence the importance in securing the underlying layers of the system), that alone is not enough to guarantee security of the higher layers unless they themselves implement the right AAA at network/application level – for example, a telco network may use otherwise secure infrastructure, but have the wrong AAA rules in place, allowing public users to access a private slice or APN – this is not a weakness of the infrastructure security itself, but rather a property of the layered approach to security in today's telecoms networks.

(42) BleepingComputer.com: Hacker claims to steal data of 100 million T-mobile customers by Lawrence Abrams

6.2/ Identity Management & Digital Signatures

Authentication is all about identity management – how you check that someone is who they claim they are, or who they can be. The problem with any enterprise, especially medium and larger ones is that in the business world nothing stays still. Divisions get reorganised, parts of companies sold off, outsourced to "trusted" third parties' operation within an enterprise's own network, or just forgotten. Given that this is the reality, we are once again faced with a significant risk that human error can occur, however good the underlying R&D.

A particular problem is with legacy authentication. Many of the protocols, approaches and techniques used in authentication may be weak or outdated.

Identity management is a key underpinning of many of the developments in cyber security architectures over the past decade. You cannot establish trust in a person or device without first establishing their identity.

The "ENISA Threat Landscape for 5G Networks" (43) lists threats related to establishing identity such as:

- Abuse of remote access to the network
- Abuse of authentication
- Lateral movement
- Identity theft and spoofing
- Man in the middle/ Session hijacking

Many of these threats have available mitigations for both human and device/service identity in widespread use in other domains such as Identity and Access Management (IAM) services and Zero Trust Network Architecture (ZTNA) in cloud and enterprise networks. In addition to established approaches, novel architectures such as the use of decentralised identity services in web 3.0 are being explored in logistics and supply chain use cases and the underlying technologies (such as distributed ledgers and privacy preserving techniques) may have utility in telecoms supply chains, subscriber authentication and device identity management.

Telecoms networks have a different set of constraints and a different threat profile to cloud and enterprise networks thanks to their highly distributed nature and physical security challenges, closer in some ways to the challenges of Internet of Things (IoT) networks. The use of hardware-based security mechanisms to generate and store secrets related to establishing identity is of relevance in both domains.

(43) ENISA threat landscape for 5G Networks

Innovation in identity management in the short and medium term could focus on the transfer of knowledge and capability from established good practice in other domains and resolving or circumventing some of the challenges that have prevented Telco's from adopting these architectures and technologies.

Fundamental to identity management and authentication however is that there should be a single source of truth around identity and authentication in a large system – this avoids overlapping sources of identity creating ambiguity, as well as dispersed identity authentication back-ends with outdated security factors in place. A single source of truth for identity also ensures that if access to a user or system is revoked, this is propagated throughout the whole system, and that access is not retained on other systems operating from a separate source of truth on identity.

For the longer term, the threat of quantum computing to disrupt identity management, and the current algorithms which underpin it, needs to be monitored. Novel approaches to embedding crypto agility into current hardware architectures to allow migration to post-quantum algorithms might help to mitigate this risk.

6.3/ Monitoring & Visibility

The complexity and heterogeneity of telecoms networks poses challenges for effective visibility and monitoring for security events. A large amount of effort must be spent by telcos to configure and manage security monitoring systems and the devices being monitored on an ongoing basis. Many monitoring platforms are focused on performance and capacity management, the same progress on security monitoring is perhaps lagging other sectors.

Challenges such as rolling out configuration to support monitoring consistently, tuning alerts to ensure acceptable levels of false positives and negatives, and the implementation of automated response might all benefit from innovations which ease the burden on telcos to enable them to improve the efficiency and effectiveness of their security monitoring and response operations.

Machine Learning can be applied to monitoring data in security tools to detect out of the ordinary behaviour and to flag potential events for further investigation and even automated response. But developing these models requires large amounts of representative data for training and testing including known good and potentially known bad traffic. Innovation in the generation and open sharing of datasets for training models on 5G security could provide opportunities to improve detection capabilities across the industry.

There is also an opportunity for modern systems to enable greater visibility across a network using open interfaces and APIs (such a syslog/rsyslog and similar), to support security monitoring. The monitoring and visibility parts of telecoms networks are security-critical however, and care needs to be taken to carefully control who and what can read from these aggregation points with visibility of network traffic, as they present attractive “honey pots” for attackers, to gain visibility of a network and its infrastructure from one place.

6.4/ Software & Platform Update Methods

One of the most important measures which can be easily taken to keep a telecoms network secure is the proper maintenance and updating of the platforms, systems, supporting firmware and software used to run the network. This extends from firmware tightly embedded in systems (such as UEFI firmware, BMC controllers, and network interface card firmware), through to the host operating system or hypervisor, the container/orchestration platform layer, the base container operating system used in a container image, and ultimately the workload deployed in the system.

Each of these layers should be receiving regular software patches, as vulnerabilities are identified and resolved. To deliver better security outcomes, these updates should be decoupled as much as possible from each other. This requires long-term stability and functional testing, to ensure that as vendors produce security patches, they do not introduce incompatibilities or unexpected changes to important behaviours. This lack of confidence is a key reason why, at present, many telecoms operators prefer to patch infrequently and irregularly – there is a significant workload requirement to test and validate a new software image before deploying it.

The move to container, VM and cloud-based software to provide network functions can make software updates more straightforward, as these provide layers of abstraction over the bare metal hardware used in a network.

This reduces the likelihood that a BMC or UEFI firmware update is likely to have a significant impact on a given workload. This also reduces the challenges posed from rebooting systems, since having inherently orchestrated network functions with redundancy makes it more straightforward to reboot individual server nodes to apply low-level firmware patches on a more regular basis.

In handling and executing software updates, there are a few key factors which need to be considered, both at system design stage, and when in-use by an operator.

6.4.1/ Software provenance, supply chain, installation & downgrade detection

Firstly, it is important that software updates are installed from authoritative sources, retrieved securely from the upstream vendor. It is important that these vendors implement best practice around software supply chain security and transmit these updates securely. The SolarWinds scandal showed the risk of pervasive software supply chain compromise is real, and valid. In that case, Solarwinds' build chain was compromised to the extent that legitimate signatures were placed on malicious binaries, which were then installed and trusted by clients. Build processes can be secured through various means – examples include holding signing keys offline and carrying out signing on air-gapped systems, using keys which are held on dedicated hardware security devices.

In the case of Solarwinds, based on their statement that the source code was not itself modified (44), there are two likely routes of exploitation – compromise of the build environment itself (i.e. the compilers and similar tools), or modification of the binaries after the build process, before they were signed. In either case, reproducible software builds (which were reproduced outside of the regular network-connected build environment) would have detected this issue. There is also a growing area of interest around software supply chain security and provenance, such as through projects like Sigstore (45). For the latter case (of the binary being changed before signing), a robust governance process around signing software builds (and keeping signing keys offline on hardware-protected devices) would have prevented compromised binaries from being signed, as basic checks would have identified the binaries had been altered. This is one small component of the challenge of software verification and trustworthiness, and recent HMG announcements around resilience and security of software (46).

(44) What You Need to Know About the SolarWinds Supply-Chain Attack SANS Article by Jake Williams
(45) Sigstore.dev
(46) Government response on software resilience and security - Policy Paper

This is still however going to likely be a relatively manual process. For some firmware (such as NVME drive controllers, and similar), this may need to be installed via userspace software, such as fwupdmgr (47) on Linux, though it is worth noting that this is run by third parties, to centralise firmware updates, rather than the vendors themselves.

There is also a need to consider how to prevent downgrades of software, which could be carried out to enable installation of software with known and exploitable vulnerabilities. This is one of the NCSC Vendor Security Assessment framework principles – VSA V.E.4 states that built-in detection capabilities should alert whenever software is downgraded during an installation process, and that there is a log or alert message shown in a location it will be seen by an administrator. This is not generally present in most low-level platforms, and may not be present at package level in operating systems. There is therefore likely to be merit in use of atomic updates (i.e. whole filesystem packaged Linux distributions), to make it easier to detect and alert on a system downgrade, rather than attempting to monitor every package version over time on every host.

Finally, there is an additional challenge in that certain security patches are likely to be inherently unable to be reversed – for example, a UEFI dbx signature blacklist database should not be reverted after it has been installed, as this is used to store information about known vulnerable or exploited outdated bootloaders. This may present a challenge in managing a downgrade however, if the previously booted operating system bootloader was signed with a now revoked signature and is thus blacklisted in the new dbx update. There is therefore a need to carefully manage revocation and signatures on binaries, and to understand the wider ecosystem of secure boot when updating systems. All this technology exists today, but the challenges are in correctly implementing it in a production environment.

6.4.2/ Update rollback, recovery, & outage restoration

Having set out the importance of detecting and preventing unauthorised downgrades of software, it is similarly important to ensure that updates can be rolled back, and recovered from, in the event of an issue. Planning of rollbacks is generally a manual process (especially where data structures or schemas in databases are updated during an upgrade), but the importance of this was demonstrated well in the Kubernetes-related outage which Monzo bank experienced in October 2017 (48). There is an inherent conflict here between the need to prevent downgrades of components by an attacker or adversary, versus the need to enable rapid recovery and restoration in the event of an outage.

(47) https://fwupd.org/
(48) Resolved MONZO banking example

Such matters are again technically possible and resolvable today, using careful implementation of processes and existing technology, along with general due diligence and a deep understanding of the technologies used. They are, however, worth reflecting on, as the kinds of challenges that will be faced going forwards in the operations of telecoms networks, and as drivers for the "broad depth" of knowledge and skills that will be required – broad across the full stack of technology used to enable network infrastructure, with sufficient depth in each and every one of these areas, in order to provide the necessary level of intuitive technical understanding to be able to manage and deliver on these kinds of processes in a production environment.

6.5/ Adjacent factors surrounding attitudes to security

The three sub-sections on Incentives, Culture and Mindset, are inherently linked, in that they combine to form the human layer around how decisions are taken. Decision-making in security is a key factor, both at tactical level, as well as strategic level. From the lowest to highest level of an organisation, these human factors materially drive and dictate the posture of an organisation. For example, many organisations suffer data breaches, ransomware attacks, and intrusions because of staff clicking on phishing links – a human factors issue. Similarly, strategic decisions by an investment committee around vendor selections during procurement may result in the selection and deployment of equipment from a vendor with a poor track record in handling vulnerability disclosures, increasing risks to the network downstream.

6.5.1/ Incentives

The then-DCMS Telecoms Supply Chain Review Report (49) was initiated because of a series of concerns about "inadequate industry practices overall, driven by a lack of incentives to manage security risks". Specifically, there was a concern around the tension between operators' commercial priorities, and how these weighed against security concerns, particularly where improved security had a bearing on costs or investment decisions.

(49) Gov.uk Telecoms Supply Chain Review Notice

A tangible example of this included the selection of Huawei equipment for use in UK core and radio access networks – if operators do not consider security as enough of a factor in purchasing decisions, the supply/demand dynamic means that vendors are unlikely to prioritise it. The 2020 HCSEC Oversight Board report (50) reported that "critical, user-facing vulnerabilities" were discovered, "caused by particularly poor code quality in user-facing protocol handlers and the use of an old operating system." NCSC assessed that these were findings about "basic engineering competence and cyber security hygiene."

Fundamentally, to drive changes in security practices, incentives must align, such that everyone benefits from better security outcomes. This is, in theory, how policy would be formed in an ideal world. In the real world, however, it is very difficult to align such incentives, since market participants will find "loopholes" to give themselves access to the upside of such incentives, without making the requisite investment that was meant to be required to gain access to the upside. Tangibly – if there is a positive incentive to encourage products to be more secure, the likely market behaviour is that vendors will attempt to sell their product as "secure", while minimising the investment they make in securing their product.

This becomes a particular challenge in security, since independently quantifying whether a product is "secure" or not is far from straightforward. Indeed, the definition of "secure" is variable, and contextual – there needs to be an agreed threat model, definition of the attack surface, set of attacker capabilities, and other contextual bounds set around the kinds of attack which need to be resisted.

The Telecommunications (Security) Act 2021 (51) seeks to create a negative incentive for an operator being insecure or vulnerable, by setting out enforcement powers for Ofcom to assess whether operators have complied with their security duties, and setting out duties to take security measures, and to respond to security compromises. Since this legislation applies only to Public Electronic Communications Networks and Services (PECNs and PECSs), this creates an interesting incentives challenge. Operators need to ensure that their vendors are suitably incentivised to invest in security, but while ultimately holding accountability in law. This means that the rational and most likely outcome here is for operators to attempt to "flow down" obligations in the TSA to vendors contractually, through (for example) contractual indemnity clauses.

(50) Gov.uk Huawei cyber security evaluation centre oversight board: annual report 2020
(51) Legislation.gov Telecommunications (Security) Act 2021

While this appears commercially rational (an operator is exposed to a significant downside through financial penalties, as a result of deploying a vendor's insecure equipment), it is imperfect. It may be difficult and expensive for an operator to prove on the balance of probabilities (i.e. the burden of proof in a civil litigation) that it was a vendors' negligence which caused a security incident, given the complexity of a telecoms network, and extent to which operators are responsible for much of the configuration and maintenance of their systems. A vendor could reasonably argue that an operator had made changes that resulted in an attack succeeding, or being able to permeate further through their network, or that they had failed to apply basic best practice security guidance (such as to prevent lateral movement).

To begin to look at aligning incentives, it is necessary to ensure that there is greater ability to differentiate between secure and insecure products, and we need to ensure that we have informed buyers, able to make and validate this differentiation by themselves.

There is a real risk that, if we do not address this, we may see telecoms converge towards a "market for lemons" (52), where the information asymmetry between market participants means that buyers (i.e. operators) are unable to differentiate "good" from "bad", and may result in a reduction in the quality of available products from vendors, since ultimately poorly-informed buyers who are unable to differentiate good and bad products is likely to result in a market where poor quality products are available at the prices buyers are willing to pay, rather than better quality products.

If this continues for a prolonged period, this may also result in a self-perpetuating loss of higher quality, more secure options on the market, since the higher quality options are likely to cease to be available, as buyers (i.e. operators) prefer cheaper options, which are lower quality, less secure products.

As such, returning to the topic of incentives, and the Telecoms Supply Chain Review Report, the report concluded that:

- there was a lack of clarity on the cyber standards and practices which were expected of industry,
- there were insufficient incentives to internalise the costs and benefits of security (as security risks were borne by Government, not only industry),
- there was no commercial driver for security, because customers of telecoms services tend to focus on cost and quality, rather than placing a high value on security,
- it is complex to deliver, monitor and enforce contractual arrangements around security.

(52) Akerlof, G. A. (1978). The market for "lemons": Quality uncertainty & market mechanism. (pp. 235-251). Academic Press

The first point has arguably been addressed, to some extent, through the Telecommunications (Security) Act 2021. Much of that is "soft" guidance, such as through the NCSC Vendor Security Assessment framework (53). It is hard to provide prescriptive future-proof guidance on security in legislation, and it is likely to be difficult to be more prescriptive than this, since security is highly context dependent.

The rest of these points relate to the wider challenges around articulating, explaining and quantifying security, which point to the biggest challenges around incentives. If security outcomes cannot be quantified and explained clearly, to be understood by all market participants, there are likely to continue to be shortcomings in security. To align these incentives requires each market participant to understand what is required, as well as to have the knowledge needed to test the validity of statements made at each part of the chain. This is likely to require more technical input and leadership over traditionally non-technical processes such as procurement negotiations, as well as cultural changes in these traditional business processes, to ensure that sufficient technical input is present to manage risks, as well as introduce a level of professional scepticism to the process to ensure that claims or statements made about security are valid, and that sufficient longer-term plans are in place by vendors to stay ahead of the curve.

6.5.2/ Culture

While every organisation has its own discrete culture in operations, there are a number of points of commonality that can be observed in the telecoms sector across organisations. Proving causation would be a complex task outside of the scope of this high-level paper however.

Culturally, operators in the telecoms ecosystem are less technically minded than one might expect of a company running a complex international network. Given the quantities of money invested in equipment, infrastructure and rollouts, telecoms operators are increasingly operating as a conduit through which capital investment in network infrastructure can deliver stable "infrastructure investment" levels of return on investment (i.e. a typical 7% inflation-adjusted year-on-year ROI, to match wider market returns).

This kind of hard commercial focus pervades cultures in organisations. It can have advantages – encouraging innovation and competition, creation of new services and product offerings, as well as disadvantages – an intense focus on the "bottom line", and in cutting back on necessary spend, or stretching lifespans of assets beyond their supported period.

(53) NCSC Vendor Security Assessment

Many mobile telecoms operators also make a large amount of their revenue from financing of handsets to customers. A GSMA report reviewing lessons learned from the US market (54) sets out the context of this – and a significant focus of it is understandably on operator balance sheets and "financial performance", rather than on tangible measures of operating a network. In particular, the report focuses on the impact on operators of losing handset purchase revenues (as seen by Apple introducing direct-to-customer handset sales), and how this results in significantly reduced operator revenue and EBITDA. This reflects the culture of what is sought by operators, and sets out background context of heavily financialised, market-beholden international companies seeking to aggressively optimise their balance sheets to compete in public markets.

Similarly, cross-organisational culture in security is relevant – largely because of these pressures, there is a (well documented) shortage in technical skills in the telecoms sector in the UK, which is discussed in Section 5 on Skills of this report. There is evidence to suggest that this is most notable in operators, where over previous decades, operators have taken every opportunity to move technical headcount off their payroll, to third party vendors and suppliers' pay-rolls.

6.5.3/ Mindset

Because we are living in the middle of a technological revolution every bit as important as the industrial revolution that preceded it, we may not always fully grasp the speed of the changes we are living through, since they appear to be "the norm." This poses problems for the security domain as some people find it difficult to imagine just how serious the impact of certain decisions might be.

The "24/7 uptime at all costs" high availability mindset does not sit well with the "but the patching is essential and reboots are vital" mindset. From a security standpoint there is absolutely no doubt what the right answer is... but if you grew up in an older generation that expected things to just "work-out-of-the-box" then even grasping that you had bought a product that did not work properly and required a patch could lead you to conclude that it is just an optional upgrade. After all it is rarely explicit enough that any upgrade will state that you need it "because we just found a fundamental flaw in our software that will enable hackers to destroy your company!"

(54) GSMA Intelligence: Risks and impact of handset financing: lessons from the US Report

The way to address this issue is to plan properly and have adequate redundancy, for a failure to do so and to apply patches in a timely fashion leaves you vulnerable and carrying considerable technical debt. The longer this condition continues, the more likely it will be that when the backlog of upgrades is finally inevitably implemented that something will not work. You might be OK... but you might not.

In business this often a money problem. If the Finance Director does not "get" the importance, then the money required to do what is necessary from a security standpoint may simply not be there...

6.6/ Approaches to wider security challenges

This section looks at key approaches that can be taken to security in telecoms networks. Whilst there is likely no single definitive breakdown of security, broadly we can break it down as follows, and then consider the tools available to us in our "virtual toolbox" to address the problems faced.

1/ Proactive and pre-emptive design mitigations – things we do to reduce the likelihood of a security breach, and things we do to make systems more resilient or robust if there is a breach, to isolate or constrain an attacker. This can include activities such as:

a. Security architecture – to design a system from top-down with a specific security posture, to deliver particular security properties based on the systems being implemented, and an understanding of how those work, and interact together to form the overall system.
b. Threat modelling – to understand the potential attack vectors and exposure points of a system, and use this to motivate the security architecture, and assess its efficacy. Also helps to consider wider less-technical threats (rogue insiders, social engineering attacks, etc.)
c. Hardening – making systems more robust and isolating systems, in order to make it more difficult to attack them, make attacks less likely to be viable, and limit the scope and breadth of a successful attack, ideally to only one system.

2/ Detection and Response – things that are done to detect an incident (on an ongoing basis), as well as to respond to one.

a. Log aggregation and monitoring – to provide visibility of actions, events and alerts in a network and the systems which comprise it, and to enable correlation and alignment of events across multiple systems.
b. Incident response and disaster recovery preparations – to ensure that there is a plan in place for how to respond to different kinds of issues, in the event that the detection and response capabilities, such as log monitoring, show indicators of compromise (such as unexpected traffic flows), and to also ensure that there are plans in place for how to restore operations (and regain confidence in infrastructure) in the event of a major incident where systems are rendered unavailable, or they have been accessed by an attacker and need to be rebuilt to regain confidence in their security.
c. Breach recovery and remediation exercises – to ensure that the people who will carry out a response to a security incident are well-practiced, that the process has been tested to ensure it is functional, and that they have access to the necessary systems or information in order to carry out an effective recovery (i.e. that credentials for break-glass accounts can be retrieved, and are functional, and give the access needed to deliver the response)

3/ Proactive vulnerability discovery and hunting – carried out ad-hoc, to replicate the process taken by an attacker, looking at the system from the eyes of an attacker, to find potentially exploitable opportunities.

It is important that we do not fall into the trap of believing that it is impossible to prevent cyber-attacks and incidents, and thus that it is not worth trying to prevent them – this is a view often seen in some areas (including some government departments) which are reticent to investing in security measures for a wide variety of superficially justifiable reasons. The harsh fact is that we all depend now on telecoms networks, which are critical national infrastructure. They are inherently connected to external and overseas networks, including those belonging to hostile nations. That is not about to stop. While it can be difficult to defend against many types of security incidents (such as compromised credentials and rogue insiders), these still remain significant routes of access and ingress into organisations and systems.

From a UK perspective, one of the challenges we face is that with telecoms as a global ecosystem of international vendors, we are limited in what we can do to meaningfully change this from the supply side, with a relatively limited manufacturing and development base. While it would be folly to suggest the UK can be fully self-reliant in telecoms in the short term, it would be possible for the UK to move to a position of having the telecoms sector and ecosystem being a "smarter buyer". The challenge is making this scale up, and in creating the right incentives on organisations to encourage them to spend what this will cost against a grim post-COVID financial position for the UK. The Telecoms Security Act, rooted in the 2019 Telecoms Supply Chain Review Report (55), identified and documented many of the challenges around incentives and market participant behaviours, and ought to drive operators to focus on managing security and resilience risks in their networks.

6.7/ Learning from systemic threats

One of the challenges we face today is that, as set out above, we already have these tools in our metaphorical toolkit to address challenges. There are copious amounts written about cyber-security issues, and yet the issues seen in telecoms are relatively predictable and broadly in line with the rest of the technology sector.

It is also important to note that, of the MITRE top 25 most dangerous software weaknesses (56), all of the top 9 weaknesses identified have been present in the last 5 years' weaknesses lists (57). Indeed, of the top 25, 15 of them have been present in each of the last 5 years' weakness lists.

In other words, we face, and continue to face, the same threats, which we are failing to effectively mitigate.

Indeed, MITRE's analysis of the 2023 data trends (58) point out a fairly straightforward issue – there are certain trends which are consistently ranking upwards – CWE-862 missing authorisation, CWE-918 SSRF attacks, and CWE-639 authorisation bypass through user-controlled keys.

CWE-862 reflects negligence in software development practices – developers are simply not implementing software correctly, resulting in ways to access systems without authorisation being checked.

(55) UK Telecoms Supply Chain Review Report (2019)
(56) 2023 CWE Top 25 Most Dangerous Software Weaknesses
(57) 2023 Stubborn Weaknesses in the CWE Top 25
(58) Trends in Real-World CWEs: 2019 to 2023

CWE-918 affects software which has been designed without adequate consideration of user-provided versus trustworthy input, resulting in users being able to make requests "as" the server, since the server blindly passes a request through to another system, allowing a user to carry out an action they shouldn't be able to, since the server is authorised to make the request. This is again a simple architecture and design issue.

CWE-639 simply refers to authorisation logic not being correctly implemented, therefore allowing any user with access to view all data stored, and is closely linked to IDOR attacks. In essence, this is negligent development practices resulting in a user being able to access another user's data (or a system being able to access data pertaining to another system).

None of these three attacks are "rocket science" – they are well-understood, and easy to mitigate. To mitigate them requires software developers to think about, and understand, security. It is highly likely that the underlying reason for these issues comes from a lack of suitable allocation of responsibility and accountability in software development – in the same way that an action taken by "all" in a meeting will usually be carried out by "none", if every subsystem developer assumes another layer will handle authorisation, it is likely that authorisation logic will not be implemented. Alternatively, skills and knowledge gaps which result in software developers that do not understand security may be developing these products.

6.8/ Identifying & Resolving the Underlying Causes of Pervasive Issues

Arguably, the single biggest underlying cause of these kinds of issues are poor software development practices. This is reflected in the NCSC Vendor Security Assessment framework guidance (59) for network equipment (which is specifically focused on the telecoms sector), where V.A. focuses on product lifecycle management, V.B. focuses on product security management, and V.D. focuses on specific mitigations against software exploits.

Part of the challenge is in measuring software quality, especially where software is a "black box", both to internal stakeholders (who may not be experienced software developers with sufficient experience to detect issues), as well as to external buyers (who are unlikely to see the source code to a product or may well not understand these issues).

(59) NCSC Vendor Security Assessment

It is hard to detect security issues in software, as they are not likely to be detected through functional testing. Defining granular functional tests for a system requires a deep level of knowledge of the overall solution and architecture, and is therefore difficult for a customer to define, even with suitably technically informed personnel. Even where security testing tools are available, these are often very limited – in the case of static analysis tools, for example, tools generally focus on the presence and appearance of proximate symbols, and can result in false positive alerts for security weaknesses where none exist (60). In addition, static analysis also cannot generally detect logical failures or other design-level faults.

At heart though, as set out above, there are a few key issues:

1. Technical competency and capacity across a broad depth of the technology and systems used, and a system-level understanding (i.e. the difference between a software developer, and an engineer that understands how each component works).
2. Customer/user capability to hold suppliers to account and set requirements. To deliver more secure products, customers need to be more informed, so as to be able to hold their suppliers to account and discern a good-quality product from a poor one. This requires significantly more high-capability technical input to be involved in account management and procurement processes, in order to create the right incentives for suppliers to focus and invest in security – when a supplier knows their customer may spot glaring security issues, they are more likely to manage these risks more carefully to preserve their reputation.
3. Attitudes towards security in commercialised and financialised telecoms companies. Increasingly, telecom companies (which are generally publicly listed and traded entities) are focused on delivering long-term utility-type financial performance for the markets – their goal is generally to deliver a stable return on investment, ongoing valuation growth, and predictable and regular dividends. This can sit at odds with delivering more secure networks, since delaying or deferring investment can deliver better financial performance quarter-by-quarter. Such investment cannot be deferred forever without significant security risks however. Since these risks are difficult for outside investors to quantify, however, and because security risks are difficult to observe or measure tangibly, they are relatively easy to carry for long periods of time without resolution. In addition, many of the mitigations discussed here would increase the purchase costs of infrastructure used in telecoms networks, by requiring time be spent on development and improving existing software. This is therefore unlikely to fundamentally add new features or value to a customer, even if it did increase security, and this makes it a difficult investment prospect for vendors.

(60) OWASP Static Code Analysis (also known as Source Code Analysis)

Most of the challenges faced today in telecoms security are unlikely to be truly technical ones. As pointed out through examples from MITRE CWE, some of the most common and rising security issues are simple to mitigate, and based on oversights, omissions, negligence, and poor responsibility for enforcing security rules when software is developed. Similarly, the #1 MITRE CWE weakness for 2023 was CWE-787, out-of-bounds write. This is a straightforward buffer overflow attack.

This weakness can generally be eliminated by using memory-safe programming languages. This is a topic regularly reiterated by CISA among others – in a post from September 2023, they quoted Microsoft and Google reporting that around 70% of the vulnerabilities they find (including in their own software) are memory safety issues. Google Project Zero has reported that 67% of "in-the-wild" exploited zero-day vulnerabilities they reviewed were exploiting memory safety vulnerabilities (61).

CISA is regularly reiterating the importance (62) of this (63) – and memory safety is part of secure by design and default. The problem is that being "secure by design and default" requires more time and cost to build a product. The market is competitive, and vendors compete to be the first available product to market.

In a large portion of the world, Western soft-power and influence around security by design will hold limited weight, compared with access to cheap or subsidised product and service offerings. Much of the world will not choose to place weight on this. There is clearly an opportunity for influence here, but this highlights the conclusion of this section – that while there are technical challenges, they are mostly solved, or have available mitigations or controls. That does not mean there is no role for future innovation, but rather that the priority now is to improve security outcomes and reduce barriers to uptake and implementation of mitigations, rather than drive more R&D into potential solutions that then do not see adoption. This in itself is likely to give opportunities for other innovation – adopting these kinds of solutions will not mean innovation stops, and there are many opportunities to innovate in ways that may reduce the cost of adoption/migration, or make it cheaper and simpler for vendors and telecoms operators to adopt these approaches more quickly.

(61) CISA Blog by Bob Lord: The Urgent Need for Memory Safety in Software Products
(62) CISA Blog by Jack Cable: CISA's Cyber Experts Talk Shop on the Need for Safer Tech
(63) CISA Blog by Jen Easterly: As Building Blocks for the Digital World, Coding Must be Memory Safe and Secure

The real challenge is in finding the right incentives, regulations, and levers to ensure that products are secure, while recognising that securing a product or system takes time, and costs money, due to the need to make use of finite skills and resources. The challenge for those deploying networks is that a secure design and deployment costs more – this is partly reflected in the way that the telecoms sector very heavily relies on vendor-provided solutions, generally where security is a value-added bespoke consulting service.

Part of the challenge with this is that it creates a cost-based incentive to reduce spend on security, and conversely a sales-based incentive for vendors to encourage more spending on security, even beyond the point of diminishing returns. A more cooperative and mutual outcomes-focused approach could yield better results.

Similarly, operators need to have more technical knowledge about how their networks work, and are architected, and how systems and subsystems (particularly legacy ones, and ones from other vendors) operate, in technical detail. This costs money, and in such a competitive market as telecoms, will ultimately impact on business' bottom lines.

At stake, however, is the UK's CNI. The recent example of a major BT 999 outage and incident post-mortem (64) highlights the extent to which resilience of telecoms is critical, but also the extent to which it has become ever more complicated as time moves on. The inter-dependencies between systems have grown. The linkages between previously disconnected systems have increased. And, as seen in the BT issue, the ability to actually localise and locate a fault (or other issue affecting service) is not to be taken for granted ("It was unclear which network cluster was affected because no alarms were presented"; "However, as became apparent later on, the network cluster that had been selected to attempt service restoration is where the fault lay."), and the complexity of systems makes them more fragile and vulnerable to failure ("While the backup system itself was ready to handle calls, the complex transfer process had not been completed successfully.")

To resolve the underlying issues, at both product development and network operations level, we need to address the financial incentive challenges that face both groups, so that security becomes an integral part of doing business. This means finding ways for vendors to use security as a competitive differentiator, and for customers (i.e. telecoms operators) to see security as a tangible benefit and differentiator during procurement. This also means ensuring that more participants in the ecosystem have access to (and use) the capabilities of the UK's cyber-security ecosystem in order to grow their own capabilities, as well as augment them for the purpose of assessing vendors (i.e. client-side relationships with experts).

(64) BT Press: BT Group review: 999 emergency call services disruption on Sunday 25 June 2023

7/ Telecoms Security Evolution

As we have explained earlier in this paper, today's telecommunications networks are evolving towards decentralisation and open interoperability while embracing complementary technologies such as the shift towards cloud-like technologies (e.g. containerisation) and the rise in interest in Artificial Intelligence (AI) as part of networks. With any technology evolution, new security threats will emerge while existing threats from previous generations must be accounted for.

This will no doubt have a range of implications on the skills we need to run our networks, but we would caution against trying to upskill people directly in specific areas set out here – in a presentation at European Microwave Week 2020, Bert Hubert set out the challenges of outsourcing and retaining sufficient technical knowledge to be able to avoid the "point of no return" in outside dependence (65). We therefore believe that future evolutions should inform our skills requirements, but that the underlying requirement is more, deeper, technical knowledge in our systems and networks, and retaining sufficient scale and breadth to train up the next generation in these technologies:

"And over the past 20 years, I've seen the extremely sad decline of all these communications companies into branding and financing bureaus, [...] because none of these telecommunications companies are technical companies anymore.

I spend a lot of time thinking about that, why? Why is that going on? And why is it bad? And that brings me to the central question of this presentation.

In any organisation, in any company, in any group, any country and even any continent, what level of technical capability, do we need to retain? How technical do we need to stay to remain viable as a company or a country or a continent? And is there a point of no return?

If you outsource too much? Is there a point where you cannot go back and relearn how actually making things work?"

Across the industry consensus is forming around emerging security technologies and novel applications which may become part of our evolving communications landscape. The purpose of this section is to "set the scene" and explore some of these areas in preparation for our second paper which will focus on recommendations.

(65) Berthub.eu post: How Tech Loses Out over at Companies, Countries and Continents

The following subsections present a summary of key developments and industry focus/research areas which align to the UK's International Technology Strategy (66):

7.1/ DevSecOps & Continuous Security testing

DevSecOps is an extension of the DevOps practices which are being implemented as Operators embrace disaggregated, multi-vendor open networking and cloudification. The concept behind DevSecOps is to integrate security as a continuous and shared responsibility throughout the entire lifecycle and is an evolution to older security practices that can no longer keep up with agile releases and the rapid cadence of updates.

Its goal is to catch vulnerabilities early in the development process, prevent regression of security postures during updates and allow for continuous monitoring and evaluation of security efficacy.

Fundamental to DevSecOps is an automated approach to security testing where common test tools and security test libraries (attacks) are consumed continuously across the Lifecycle with heightened focus towards non-functional testing around realism and day-zero what-if scenarios.

Key to the success of DevSecOps will be feedback loops providing qualitative data to reinforce security designs and decision making or to offer guidance for remediation or mitigation.

It is also envisaged that DevSecOps combined with AI could provide optimised recommendations for vulnerability remediations and infer how such changes will affect the rest of the networking environment.

In DevSecOps, it is important to ensure that, even though security testing is automated, it is sufficiently scoped and defined to deliver meaningful security tests – at minimum, there should be a focus on delivering positive, negative and fuzz-based tests, with robust and well-defined expected outputs or state transitions. This is important to ensure that the functionality being tested at each stage is sufficient, and that the security testing being delivered is both meaningful and productive in identifying issues or regressions – this means it should also evolve over time to cover previously identified issues, as part of a feedback loop as set out above.

(66) Gov.uk Policy Paper: UK International Technology Strategy

7.2/ Zero Trust (Networks)

Due to the heterogenous nature of future communications networks and the prolific growth of diverse end devices, no asset can be trusted implicitly and there is a clear need to architect our future networks based on zero-trust principles.

To enhance security, assets need to be verified every time they request access, even if they were authenticated earlier. Continuous authentication, and access control can ensure only legitimate parties with approved credentials can access the relevant parts of the network enabling highly personalised security policies and data privacy.

For Zero Trust to be successful it needs a broad implementation across the different dimensions of our communications networks including traffic planes (user, control and management), networking domains (Core, RAN, Transport, Wireline, Non-Terrestrial, IT (OSS/BSS)) and user equipment like smartphones, CPE devices and Industrial IoT equipment.

It is important to note that while Zero Trust Network Architecture (ZTNA) can often be used to refer to the idea of exposing sensitive systems to the public internet, behind a single-sign-on platform and device validation system, this is not inherently required. The underlying concept of ZTNA is about minimising the assumptions placed in each system in a network, and adopting a posture of “assume breach”. One of the challenges in adoption of ZTNA to date has been around validating the integrity of assets at point of request (i.e. robust device attestation), and many of the solutions available in this space are tied to vendor-specific implementations (i.e. Microsoft InTune or similar), rather than using open and interoperable standards for ZTNA device attestation.

7.3/ Quantum Safe

Future advances in quantum computing pose both a threat and opportunity to cybersecurity capabilities within our public and private communications networks.

As attack-capable quantum computers evolve during the next decade they will negate the efficacy of current complex asymmetric encryption algorithms and digital signatures. The ability to replace today’s cryptographic protocols will be essential for maintaining long-term defences. This will introduce the need for “algorithm agility”, to be ready to introduce and adopt and recognise new cryptographic algorithms in future.

New quantum-resistant public-key cryptographic algorithms will need to be thoroughly evaluated for efficacy and efficiency as they run the risk of placing significant overheads on the network.

Regarding opportunities, Quantum Key Distribution (QKD) offers a novel way to distribute keys between endpoints with protection against interception. It is already being practically demonstrated for current technologies such as fibre optics and lasers and offers a potential application for tamper proofing 5G advanced networks and future 6G "3 dimensional" networks.

However, QKD requires classical (i.e. non-quantum) authenticated communications channel to be established in advance of its use, in order to validate that the keys sent (and received) over the QKD-protected link were indeed sent by the expected transmitter – QKD can protect against and detect eavesdropping, but does not, in itself, protect against a "man-in-the-middle" type attack, where the counter-party to the communication is replaced by another party executing the QKD protocol themselves. To prevent this, classical authentication of the channel is used (e.g. via a shared symmetric key, or classical asymmetric cryptography). This authentication process is therefore critical to the security of a QKD link, and with access to a secure shared secret key at both ends of the link, classical techniques (such as use of an authenticated cipher) can be used to deliver similar security properties.

A 2021 paper by Ericsson's security research team (67) has set out some concerns around the viability of the use of QKD in telecoms networks however, indicating that there is not yet a clear consensus that QKD will solve these issues – indeed, Ericsson's paper concludes that there is a consensus in the security community that QKD has "many fundamental issues that would need to be solved". The paper goes on to highlight challenges around the need for the external authentication of the communications channel, the general use of a regular underlying symmetric cipher for encrypting the data being transferred, the dependency on custom hardware (which is likely to be harder to patch or upgrade in software), and that QKD is inherently a point-to-point protocol, requiring trusted nodes to carry out QKD between themselves, which may sit at odds with ZTNA principles, where trust in external nodes is desired to be reduced as much as possible.

(67) Quantum-Resistant Cryptography, Mattsson, Smeets & Thormarker, 2021

7.4/ Artificial Intelligence/Machine Learning

AI and Automation are now seen as foundational to the design and operation of our evolving communications networks enabling a large decentralised system where intelligent decisions are made at granular levels enabling:

- self-orchestration and optimisation,
- self-healing,
- and self-defending and securing networks.

With AI/ML already being used extensively in the field of IT/Enterprise cyber security defences, a precedent has been set for communications networks to follow.

Today early AI/ML security research and implementations in our networks focus on threat detection but it is envisaged this will evolve towards prevention and response.

In addition, the adjacent AI/ML research towards self-orchestrating networks where the constituent domains of RAN, Core and Transport can be dynamically re-configured and updated lends itself to autonomously responding to adversarial events, introducing a form of self-defence through adaption.

However, AI/ML technologies also present new vulnerabilities which need to be addressed including training data manipulation, reverse engineering of inference data sources and training data bias. New security capabilities will be required to not only ensure AI data efficacy but also to avoid compounding security risks through ever expanding and integrating models.

While preparing this document, the UKTIN AI Expert Working Group sought the input from the Security EWG – we have included in Appendix A – AI Security Summary Note a short report prepared by the Security EWG as input to the AI EWG.

7.5/ Distributed Ledger Technology ("DLT") and Blockchain

The evolution of our networks through containerisation and decentralisation leads naturally to a decentralising of security, operating as an autonomous part of a connected whole.

Distributed Ledger Technology (DLT), such as blockchain can provide new ways to handle trust relationships and the required auditing between interconnected and federated networks (terrestrial and non, public and private), edge computing and roaming functions. It also offers the potential for securing supply chains.

Without requiring a centralised management authority, blockchain can provide the relative independence to provide an authoritative record of secure transactions while enabling parties to transact directly in a secure manner.

7.6/ Private 5G / 5G / Wi-Fi Convergence

Private cellular solutions are growing in popularity and offering performance and feature sets that that can provide advanced and innovative solutions to connectivity problems. Cellular can then provide the levels of security and resilience needed in wireless solution and will increasingly be used in CNI applications to replace insecure or poor performing alternatives. Private cellular networks may also be used to provide infill coverage in areas where commercial mobile networks do not offer a service with sufficient capacity or coverage.

There is however a real risk of a 'race to the bottom' to provide features at the expense of security at a low-cost point in terms of Private 5G. Several open-source projects are feature-full, but often 'academic' in terms of code quality and system hardening.

If effective security standards and testing are not in place, these private solutions could represent significant vulnerabilities in CNI.

Historically, there have been various attempts made to converge Wi-Fi and cellular networks to form heterogenous and seamless connectivity experiences for users – for example, through cellular data offload over Wi-Fi, or EAP-SIM/EAP-AKA authentication for customers of mobile carriers to use Wi-Fi hotspots branded by their telecoms provider. Historically, many of these protocols have introduced vulnerabilities around security and/or privacy (68) – both EAP-SIM and EAP-AKA originally transmitted a user's IMSI in plaintext over the Wi-Fi network, in a manner which is visible to a passive attacker. Similarly, while WiFi calling (VoWiFi) uses IPsec with IKEv2 key exchange, the IKE_AUTH stage uses EAP-AKA, meaning that the exchange of IMSI is not protected by a certificate, enabling an active attacker able to carry out a MITM attack to access a user's IMSI.

While these issues have been addressed by 3GPP S3-170116 (Privacy Protection for EAP-AKA) and "IMSI Privacy Protection for Wi-Fi" (69), these indicate the wider challenges likely to be encountered when delivering convergence between access networks.

7.7/ Secure Geospatial Mapping, & Impact on Telecom Networks

The formation of the UK's Ordnance Survey had its roots in wartime – and security and mapping have gone hand-in-hand ever since. Even the prevention of a cholera pandemic in the nineteenth Century can be put down to mapping clusters of cases in London. With the advent of telecoms networks, they were immediately recognised as targets worthy of both high levels of physical and digital protection – indeed, a comment in the House of Commons in 1993 (70) was focused around the mere existence of the Post Office Tower.

People may assume that with the advent of Google maps and the Internet more generally that it is no longer possible to "hide" telecoms assets. In fact nothing could be further from the truth. The precise location of both above and more especially below ground assets is if anything even more sensitive now than ever before, given that a dependency on telecoms infrastructure of all other so-called "smart" infrastructure that already relies on varying degrees on a robust reliable telecoms and Internet infrastructure.

(68) WiFi-Based IMSI Catcher Published by Oxford University, written by Piers O'Hanlon & Ravishankar Borgaonkar (2016)
(69) Wireless Broadband Alliance: IMSI Privacy Protection for WiFi
(70) Hansard, 19th February 1993, Debate 5, Column 634, Kate Hoey (Vauxhall)

Since 2019, the Cabinet Office has been leading a project called the National Underground Asset Register (71) ("NUAR"). This has been mapping all underground utility assets successfully (with the general exception of telecoms assets) and now has a minimum viable product. Also, The Department of Digital, Culture Media and Sport (now DSIT) has, since 2021, been running the Digital Connectivity Infrastructure Accelerator ("DCIA") programme. This has been about mapping above-ground assets to try to accelerate UK small cell deployments. All NUAR work was transferred to DSIT in December 2023 and is being expanded in scope and scale. This will inevitably have security implications.

One lesson learned from the DCIA programme was the importance of Local and National Government understanding the downstream supply chain dependencies on suppliers and developers of software used for mapping of strategically significant assets – in two cases in the programme, it emerged that UK-based software suppliers had previously unknown connections with, and presence in, Russia and/or Belarus, which came to light as a result of reviews of suppliers in response to UK Government policy changes, following Russia's invasion of Ukraine.

(71) Gov.uk Guidance: National Underground Asset Register (NUAR)

8/ Critical Infrastructure

The UK has 13 top-level critical national infrastructure sectors – these encompass those necessary for the country to function (Government, Defence, etc.), and those upon which normal daily life depends (Emergency Services, Energy, Finance, Food, Communications, Water, Transport, etc.), as well as some which are not critical to essential services, but which require particular protection due to dangers to the public (Civil Nuclear, and Chemicals).

The NPSA (formerly known as CPNI) has set out a criticalities process, which sets out the challenges for the UK, based on CNI becoming "increasingly interconnected and interdependent". This process maps out essential functions, understand what systems provide those functions, and ultimately assesses the impact of one sector's functions on another.

While the Criticalities Process (as part of the CNI Knowledge Base) is a non-public Government tool, this EWG can make observations based on their broad sectoral experience around some of the challenges that telecoms are likely to face.

Dependencies

Consumer and business telecoms critically depend on:

- Other Telecoms (upstream bandwidth providers, upstream telecoms providers, overseas interconnects, wholesale telecoms providers, internet exchanges and data centres)
- Energy (mobile cell sites require mains power and have very limited backup power. FTTC street cabinets require power, as do Virgin Media HFC cabinets. Phone exchanges and OLTs/head-ends require power. Core networks, routing, switching and interconnects require power. Upstream network providers, peering exchanges and data centres require power and cooling).
- Water for data centre cooling, particularly in hyper-scale data centres (72). In 2019, for example, Google was estimated to use 2.3 billions litres of water in 3 US states alone (73). A single 15 Megawatt (medium sized) data centre (74) can use 1.36 million litres of water per day (75). In the event of disruption, this would impact on data centre operations – the Uptime Institute recommends that Tier III and IV data centres store 12 hours' worth of water use on site (76).

(72) DgtlInfra.com, Data Center Water Usage: A Comprehensive Guide
(73) Time.com article: The Secret Cost of Google's Data Centers: Billions of Gallons of Water to Cool Servers, Nikitha Sattiraju / Bloomberg
(74) DgtlInfra.com, Data Center Power: A Comprehensive Guide
(75) Computer Weekly, Why water usage is the datacentre industry's dirty little secret by Caroline Donnelly
(76) Uptime Institute, Water Scarcity Could Put Your Data Center at Risk PDF

Telecoms clearly has other dependencies, but these are not directly causational towards the ability to provide services (i.e. telecoms relies on the finance sector, but the network itself would continue to operate without that sector, as opposed to energy, where telecoms infrastructure would fail in the event of widespread outages).

The energy sector relies on:

- Civil nuclear, for some base-load generation capacity.
- Communications (which we will discuss below).

In particular, the electrical utilities are increasingly relying on telecoms infrastructure, in order to carry out "asset sweating" and make more use of existing assets like transmission cables. This is necessary to help the UK deliver on net-zero commitments, which require electrification of transportation and heat, among other use-cases (77).

Active network management (ANM) effectively allows energy networks to control their energy assets over communications networks, and manage their network in real-time, to allow load and generation to be switched on and off as required to deliver stability of the network. ANM makes it possible for more generation to be connected to the electrical grid than would otherwise be possible, which is a significant enabler for the connection of dispersed renewable generation such as wind turbines – by managing and monitoring constraints on an area of the network in real-time, energy network capacity can be maximised by allocating capacity in real-time (78).

Flexibility services will allow energy system operators to dispatch (i.e. request) services from providers nearer to real-time (i.e. day-ahead or in-day), to help to balance the grid and alleviate local constraints (i.e. areas where there is more demand than the grid can handle, or where there is more generation than the grid can transport, so generation can only be accommodated with more local demand).

All of this depends on telecoms. Increasingly, cloud services are used for ancillary (non-critical) systems in network operators. Additionally, public telecoms networks are already being explored for use in certain critical functions, such as tele-protection (for example, the UKPN CONSTELLATION project (79)). Telemetry gathering, and network visibility are often delivered through public cellular connections (or satellite connections for certain operators in their primary substation network).

(77) Will there be enough cables for the clean energy transition? (FT)
(78) ArgandSolutions.com, What is Active Network Management (ANM)?
(79) UK Power Networks, Future Ready - Constellation

The energy sector is more tightly regulated than the telecoms sector, in that network operators (who own and operate wires and infrastructure) are constrained in their ability to make profits – their expenditure is approved directly by the regulator through a series of price control periods (RIIO-ED2 for distribution networks (80), RIIO-T2 for transmission networks (81). This regime means that network operators must deliver value-for-money to the billpayer, and that their spend is heavily regulated, to ensure that returns on capital deployed or debt costs are carefully managed, and that Return Adjustment Mechanisms (82) are used to protect customers and investors against significant deviations in expected costs.

This means that the energy sector is not in a position to make significant investments in their own communications networks. Historically, there have been challenges in reaching common understandings between regulated sectors – as one example, the financial services sector has widely adopted the use of SMS as a two-factor security authentication mechanism, to the displeasure of some telecoms operators (as this increases social engineering attacks on customer services staff for SIM-swap attacks, as well as increasing the potential for SS7 SMS interception attacks, like those seen against O2 Germany (83)).

Energy network operators are subject to the NIS Regulation, which telecoms network operators were previously exempt from. This is likely to change with the introduction of NIS 2. In the UK, the Telecoms (Security) Act 2021 has now taken effect, and goes further in introducing specific technical regulations to mitigate systemic security risks. This non-alignment has created inter-dependency challenges. Energy networks seek resilient infrastructure, and often assume that telecoms networks have more power autonomy than is really the case. Conversely, telecoms network operators ask energy network operators for resilient power, but are not willing to pay the cost for a truly redundant feed (i.e. from a second energy network operator), since this would require a significant cable lay from another region to a cell site!

This creates a complex set of inter-dependency – the energy sector wants secure and resilient telecoms, but the telecoms sector requires secure and resilient energy supply.

These kinds of inter-dependencies are only likely to increase with the rise of connected vehicles, autonomous vehicles, and a general propensity by vendors to add connectivity to previously-offline systems, in pursuit of service-based recurring revenues, rather than one-time revenues. Despite this, there is a gap around who will pay to make telecoms infrastructure more resilient and secure!

(80) ofgem, RIIO-ED2 Final Determinations
(81) ofgem, Network price controls 2021-2028 (RIIO-2)
(82) ofgem, RIIO-ED2 Final Determinations
(83) TheRegister.com, After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts, Iain Thomson

9/ Research, Development & Adoption Landscape

The purpose of this section is to study some of the key public facing bodies currently involved in the telecoms network R&D ecosystem, and projects taking place that are relevant to telecoms security. Secondarily, it will explore some of the challenges and issues around the lack of adoption and uptake of the outputs and outcomes of research in the telecoms security domain, as discussed elsewhere in this paper. There are several:

National Physical Laboratory ("NPL")

The NPL is operating UK Telecoms Lab (UKTL) on behalf of DSIT. The Lab provides security testing, research, interoperability testing & skills development. It is designed to address perceived threats around security requirements hampering innovation & diversification. It also aims to improve security testing skills in the UK.

Engineering and Physical Sciences Research Council ("EPSRC")

In October 2022, EPSRC launched funding (84) for early-stage federated hubs for future communications systems, and each should cover cross-cutting themes including "security, resilience and trust". These hubs are encouraged and are working closely with UKTIN.

EPSRC also invest in research through the Information and Communication Technologies (ICT) theme (85). One of the priority areas is "Safe and secure ICT" which, although not targeted at telecoms security specifically, should accept proposals for research into this topic. Given the significant and increasing overlap between telecoms and IT, future telecoms networks such as 5G are increasingly based on commodity off-the-shelf IT hardware and software platforms.

UK Space Agency ("UKSA")

The UK Space Agency has run a series of calls on specific or general topics relevant to emerging and innovative technologies, which include telecoms:

- An Open Call for Technology (86)
- UK National Delegate support for the OPS-SAT Versatile Optical Laboratory for Telecoms and Lunar Communications - ARTES (87)
- National Space Innovation Programme – Kick Starter – Open Call (Call 1)
- Announcement of Opportunity: Space Cluster Infrastructure Funding Call

(84) UKRI, Springboard for telecoms research and innovation
(85) UKRI, Information and communication technologies theme
(86) Gov.uk Notice, Enabling Technologies Programme - Call Four
(87) Gov.uk Notice, Call for applications: UK National Delegate support for the OPS-SAT Versatile Optical Laboratory for Telecoms (VOLT) and Lunar Communications - ARTES

- ARTES programme - ARTES Programme Advanced Technology Proposal Form Guidance Notice

As a general comment, there seems to be a considerable activity building up on space technologies (horizontal, not just security, but the latter is relatively under researched).
Other potentially relevant research investment programmes include:

- Digital Security by Design (DSbD)
- Ensuring the Security of Digital Technologies at the Periphery (SDTaP)
- ICT networks and distributed systems

Others

There are other academic research organisations like CyberSec groups with focus on telecom, as Academic Centre of Excellence in Cyber Sec Research e.g. (88) or notable industry activities from companies like QinetiQ or Thales as examples.

9.1/ Barriers to Adoption

There is active research in security topics across the key properties of a secure, resilient system: availability, confidentiality, integrity, authentication, and accountability. It may be done for its own sake, such as novel approaches to encryption relying on results at the edge of cryptographic mathematics. It may be practical and applied to address a known problem.

Even if mature, and at the highest level of TRL, the adoption pathway for the R&D outcomes may be difficult to travel. For example, the solution may not scale when implemented. There may be resistance to changing a standard. The impact on best practices may not be acceptable.

9.2/ Long- & Short-Term Research

There is a clear need to balance long and short-term research. Research can generally be considered “pure/fundamental”, or “applied.” Pure/fundamental research is carried out without a specific goal or problem in mind, to further understanding or foundational knowledge. Applied research is that which is carried out to attempt to solve a specific problem.

(88) NCSC, Academic Centres of Excellence in Cyber Security Research

It is important to find a suitable balance between them, even though there may be challenges in doing so - security, for example, is a heavily and inherently applied area, where research is focused on making a particular thing secure.

Fundamental research in security may focus on software development theory and techniques, or cryptographic algorithms and in formal security proofs. One challenge is that this work is often highly abstract and theoretical, and difficult to demonstrate in practical form, since security proofs are generally a derivative of mathematical proofs, focusing on demonstrating that breaking a given algorithm can be reduced to having to break a known or proven-hard problem.

In contrast, a more applied, engineering-oriented approach to security research is likely to steer away from such research, and instead look at the overall architecture and design of a system, and how there could be weaknesses that are exploitable.

An analogy of this is that fundamental research may develop better or more secure, or perhaps even perfect locks, but applied research might study the wider construction approach and point out that the door frame is weak and rotted, or that the window has been left open, and thus the lock's security is functionally irrelevant.

Despite this, both areas of work are important to focus on, but we need to better understand the outputs and outcomes of research, and look at how impact and demonstrable value can be realised from research. This report has identified problems with the lack of adoption and uptake of R&D. We believe this lack of impact is holding back the telecoms sector, but also the UK. We suggest that it is worth reviewing the desired outcomes of research, to ensure that research funding is focused and targeted towards impactful areas that align with the UK's strategy.

There will always be a place for blue-sky, moon-shot type research at low TRLs, and we should embrace this higher risk research, and also look at how to be more tolerant and accepting of failures in such research – like the DARPA approach.

Two key properties of the DARPA approach which may benefit are the broad focus on what has been described as "pushing the frontiers of basic science to solve a well-defined, use-inspired need" (89), and a rapid-feedback outcomes focused, rather than time-bound, approach to research – unsuccessful approaches are quickly shut down, successful ones are prioritised and receive ongoing funding, and personnel can move between teams to support the successful attempts.

(89) Harvard Business Review, "Special Forces" Innovation: How DARPA Attacks Problems by Regina E. Dugan and Kaigham J. Gabriel

By enabling foundational basic research, but focusing it on a "use-inspired need," this avoids the linear model of innovation, and enables early-stage low TRL research to be carried out, but in furtherance of specific goals and outcomes, where learning is an outcome and goal, rather than delivery of a 3 year programme to a plan set at the outset (like much current research). We believe that, particularly in security, the linear model has failed to deliver (as evidenced by examples given in this paper) and would recommend instead that we look at how to deliver answers to "well-defined use-inspired needs", as opposed to completely blue-sky time bounded research.

This way, foundational research can rapidly transition towards applied research, and into solution development, as the underlying understanding is being sought with reference to a specific real-world problem. This both helps the UK stay ahead (since we need lower TRL research to remain competitive in future decades), and helps to begin a process of driving adoption, since the direction of research would be focused on results, and the research is focused on meeting a use-inspired need.

It is also important that we tolerate, embrace, and welcome failure in research, especially where it advances knowledge, and perhaps avoids wasting greater amounts of time in future pursuing infeasible routes. The DARPA model illustrates how the ability to rapidly reallocate people from unsuccessful challenge solutions to other successful ones can create stability for individuals, while remaining focused on delivering outcomes.

We believe that "problem-oriented" research is a good approach – an approach which NCSC has started to take, with its public problem book (90). While some may argue that such an approach constrains fundamental research, we believe that in fact use-inspired fundamental research will deliver better results and benefits, and ultimately lead to more advanced R&D being carried out in the UK.

There is already evidence (91) from the US to suggest (92) that the current approach to fundamental research leads to a division in labour between universities performing basic research, start-ups finding commercial applications for said research, and large established companies developing and scaling up those applications. In particular, it found that "publications in scientific journals" has "little effect on the various components of corporate R&D", leading to the conclusion that "corporate innovation is largely unresponsive to 'pure' knowledge spill overs."

(90)The NCSC research problem book
(91) NBER Working Paper Series, The Effect of Public Science on Corporate R&D
(92) The Economist, Article: Universities are failing to boost economic growth

These findings sit alongside our earlier observations in this paper about the UK's approach to telecoms and telecoms security R&D, and underline our point about the need to look at new ways to deliver more use-case oriented and applied research at all TRL levels, and look at how to improve adoption and uptake of existing solutions and research outputs in commercial products to realise the benefits of the research our universities and businesses do carry out.

10/ Regulations

10.1/ Relevant Security Legislation

There has been a surge of legislative activity in the consultation, development and enacting of Acts with regards to cybersecurity in recent years. There are both security focused Acts, and revisions of previous Acts that are updated to consider security provisions.

While most stakeholders (research community, organisations and companies, etc.) welcome the need to reduce risks of cyberattacks against digital infrastructures, the complexity of both the digital/telecoms devices themselves and the supply chains, there are also expressed concerns on what the technical, economic and societal impact would be. A representative case concerns Free & Open Source Software (FOSS), which dominates the market share of digital devices (including telecoms specific). The challenges where digital devices with FOSS can be realised through the requirements and provisions in the following cases of the recent Acts:

10.2/ UK Legislation

10.2.1/ Telecommunications (Security) Act 2021

This Act amended the Communications Act 2003 by introducing new duties on providers of public electronic communications networks and services to identify and reduce the risk of security compromises and prepare for the possibility of their occurrence. The Telecoms (Security) Act sits alongside a range of other legislation that together forms a strengthened cyber security framework for telecoms networks. It covers a wide range of areas, and incorporates, by reference, specific technical guidance and recommendations around best practice for security, which reflects the significance of the telecoms sector, and the growing cross-sectoral dependency on telecoms networks to sustain daily life as we know it.

10.2.2/ The Electronic Communications (Security Measures) Regulations 2022

The ECSMR was introduced through powers established in the Telecommunications (Security) Act, and is a Statutory Instrument (secondary legislation) introduced by the Secretary of State, as authorised by Section 105D of the Communications Act (2003), in order to bring into effect legislation that establishes specific measures which telecoms providers must take in order to meet their duties under the Communications Act (2003), to "identify and reduce the risk of security compromises occurring and prepare for security compromises".

The ECSMR sets out the telecoms security framework, and powers to issue codes of practice containing technical guidance – the Telecommunications Security Code of Practice (93) therefore sits alongside this legislation as technical guidance.

10.2.3/ Network and Information Systems Regulations 2018

The UK's implementation of the NIS regulations also covers the security of digital infrastructure, which sits adjacent to telecommunications, and underpins many of the modern services which people interact with through telecoms networks, such as many critical components of internet connectivity and access – public DNS services, internet exchange points, and top-level domain services are among those services which the NIS regulations cover, alongside online search engines and cloud computing services. Each of these is critical to the secure operations of the internet as citizens know it today, and failures of these are likely to have similar scales of consequences to traditional telecoms infrastructure.

10.2.4/ The Product Security and Telecommunications Infrastructure Act 2022

The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 comes into force end of April 2024. It distinguishes between internet connectable products (mainly IoT devices) and network connectable products, the latter encompassing all products that do not support IP connectivity.

(93) DCMS, Telecommunications Security Code of Practice

Requirements and provisions:

- Security by default (ban default passwords)
- Vulnerability disclosure policy
- Transparency on minimum length of time of support through security updates
- The product will need to be accompanied with a statement of compliance (for security requirements)

10.2.5/ National Security and Investment Act 2021

The National Security and Investment Act 2021 (NISA) was enacted in the UK in early 2022 with an objective to "making of orders in connection with national security risks arising from the acquisition of control over certain types of entities and assets; and for connected purposes" (94). This has a significant implication for corporate financing of several critical sectors including technology and telecommunications. The communications sector is one of the 17 mandatory sectors captured by the NSI regime. As a regulated sector, the definition of telecoms for the purpose of the NSI regime mirrors that of the Communications Act (for telecoms, including associated facilities), and the definition of digital infrastructure mirrors that of the Network & Information Systems Regulations 2018.

NSIA 2021 essentially gives substantial powers to the UK Government to intervene in acquisition of influence and control (through acquiring of shares for a certain minimum threshold of holding) in an entity of interest. For this purpose the entities of interest include (other than an individual) any company or corporate, partnership or a trust who are holding a qualifying asset such as land, tangible moveable property or IP (of some industrial, commercial or economic value) in any of 17 specified sectors which include (of relevance to the telecoms sector) artificial intelligence, communications, computing hardware, critical suppliers to government, cryptographic authentication, data infrastructure, define, military and dual-use, satellite and space technologies, and suppliers to the emergency services. Entities working in advanced robotics, civil nuclear, defence, energy and transport are also in scope; many of these areas are also where entities in the telecom sector operate.

NSIA 2021 would serve to dramatically alter the corporate financing and governance landscape for the telecoms sector, as is already evidenced by the interventions executed under the legislation. It gives powers to the Secretary of State for Business, Energy & Industrial Strategy (the portfolio which has now split across three departments since 2023) to block, impose conditions or clear acquisition. From the interventions so far, there are lessons for the telecom sector in terms of the sector adopting effective cybersecurity measures and, ensuring continuity to support infrastructure and services critical to UK national security and economy.

(94) National Security and Investment Act 2021

As part of an acquisition, Sepura Ltd (a provider of mission critical communication services, TETRA, and hand and vehicle devices to private sector and Government customers) was "required to implement enhanced controls to protect sensitive information and technology from unauthorised access, and to provide rights of access to premises and information so that relevant agencies are able to audit compliance with the security measures (which was deemed) necessary and proportionate to mitigate the risk to national security" (95). Notable here is that the acquisition enabled Sepura to be transferred from overseas (Chinese) ownership to UK ownership; the scrutiny and measures were insisted regardless.

As part of an acquisition, Inmarsat Group Holdings Limited (a major provider of satellite communications provider to maritime and other sectors) also faced conditions whereby the Secretary of the State ensured that "controls are in place to protect information from unauthorised access, and strategic capabilities continue to be provided by Inmarsat and Viasat to the UK government" which were deemed to be "necessary and proportionate to mitigate the risk to national security" (96). However, not every investment called in for assessment attracts active measures, as is demonstrated in the case of the French telecom group Altice's investment in BT where no remedies were suggested (97).

10.3/ EU Legislation

Given that the UK makes up only around 2% of the global telecommunications market, vendors of equipment are also likely to need to align their own product development with the general European direction of travel. Given that a significant proportion of ETSI's funding is from the European Commission, and the Commission can issue mandates to ETSI for standards formation, it is highly likely that, going forwards, general principles and practices of EU legislation will be proposed for standards. Similarly, to export and sell products into the European market, UK-based vendors will need to comply with these.

10.3.1/ Radio Equipment Directive (RED)

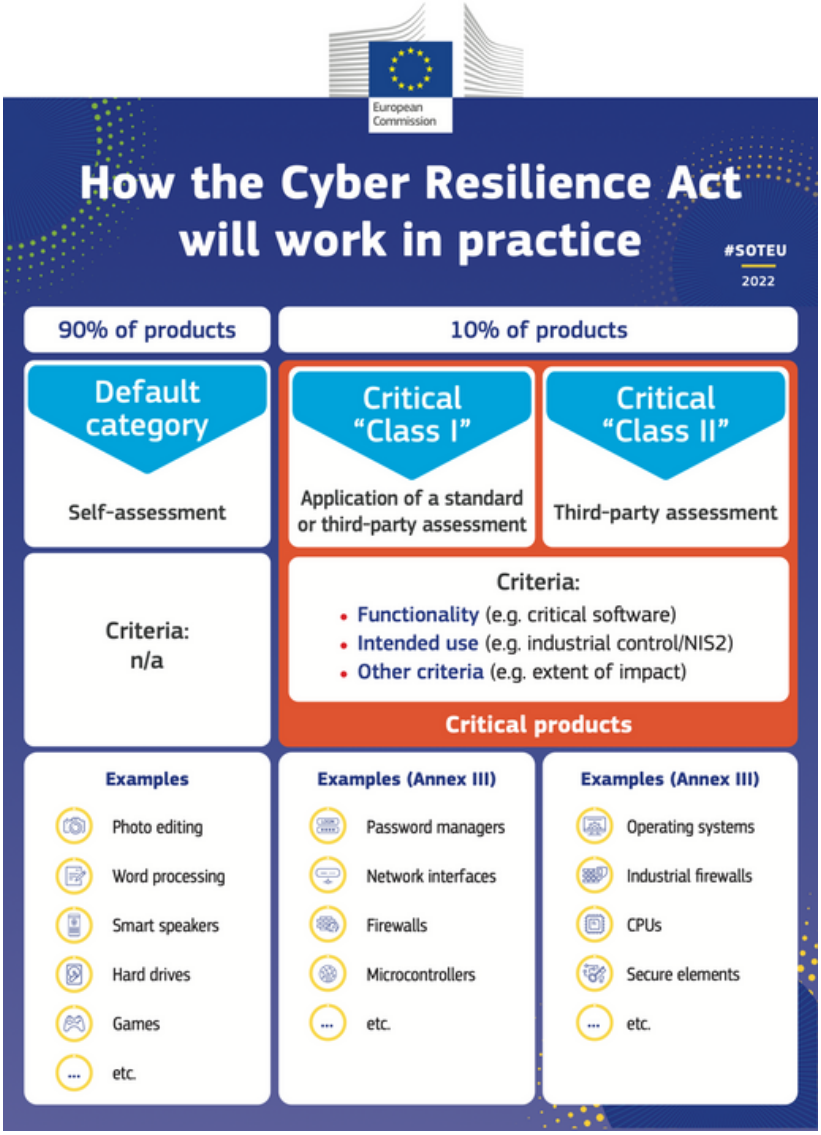
The Commission have activated Articles 3.3(d,e,f). These provisions require that radio equipment does not harm networks, protects user privacy and support features to prevent fraud. Manufacturers of radio equipment need to take steps to ensure that they would actively reduce the risks, by updating their software and addressing any discovered vulnerabilities.

(95) Department for Business, Energy and Industrial Strategy National Security and Investment Act 2021
(96) Cabinate Office Decision, Acquisition of Connect Topco Limited by Viasat, Inc.
(97) Gov.uk News Story, Government to take no further action under National Security and Investment Act on BT share acquisition

10.3.2/ Cyber Resilience Act (CRA)

According to the CRA, manufacturers will remain responsible for products with digital element throughout the product's lifecycle and ensure that vulnerabilities are dealt with (no known ones, new ones addressed within 72 hours upon disclosure).

Telecoms equipment are expected to be classified into Critical Class I or Class II categories, depending on their functionalities, intended use and deployment:



Source: https://ec.europa.eu/newsroom/dae/redirection/document/89528

10.3.3/ Cyber Solidarity Act

Increased preparedness for detecting and responding to significant large-scale cybersecurity threats and attacks. Information sharing between Security Operating Centres (SOCs), Computer Security Incident Response Teams (CSIRTs) is the focus of the Act. As such, telecoms providers, being part of critical infrastructures, are expected to be involved accordingly.

10.4/ Standards:

- There is an effort to harmonise laws against standards relating to making radio equipment available to the market. A summary of changes can be found here: https://ec.europa.eu/docsroom/documents/51934
- Referenced by the Acts:
  - ISO/IEC 29147:2018 Information technology - Security techniques - Vulnerability disclosure standard
  - ETSI EN 303 645 European Standard on Cyber Security for Consumer Internet of Things: Baseline Requirements
  - ETSI TR 103 838 Cyber Security; Guide to Coordinated Vulnerability Disclosure

10.5/ Main processes identified:

- Conformance (self, or third party for high-risk products). Self-declared conformance assessments relate low-risk equipment, with limited or low impact application domains. For infrastructure equipment classified as high risk, these will need to be certified.
- Vulnerability management, handling, coordinated vulnerability disclosure. In any case, all digital equipment in the market will need to be supported by appropriate vulnerability management processes, to support risk management and mitigation processes.

11/ Appendix A – AI Security Summary Note

The below text comprises a short summary of security considerations identified by the UKTIN Security Expert Working Group, prepared and shared at the request of the UKTIN AI Expert Working Group. It is included here to augment the information contained in the main body around AI in telecoms networks.

11.1/ Unpredictable Behaviours

Non-linearity leading to unpredictable behaviours that make AI hard to supervise

- AI/ML systems inherently (to add value) need to be doing more than implementing basic linear logic. Otherwise you would simply use linear logic and avoid the issues – for example, "if load on server is high, scale app by spinning up another container pod" – that is basic linear logic, and you can easily monitor this logic and set failsafes, like not allowing all pods to be spun down, and set a maximum scale-up rate.
- A naïve solution to this problem would be to set up "supervisory" logic or functions, sitting around the AI and monitoring its behaviour. The problem is that since AI will be used in settings where basic applications of simple linear control logic will not suffice, it is inherently difficult to develop appropriate and effective safeguards/supervisory functions.
- The harder it is to independently check/predict the correct outcome or decision, the harder it is to supervise and check control inputs taken by AI. This is especially true where even the ability to observe actions being taken is difficult (for example in RAN optimisation).

11.2/ Increase in Complexity

Increase in complexity making it difficult for telcos to effectively own/operate their own networks themselves (as required by TSA)

- In contextualising the obligations of telecoms operators, and implications of use of AI on security, the December 2022 Telecoms Security Code of Practice (98) (TSCoP) should be used as a technical foundation, and the Electronic Communications (Security Measures) Regulations 2022 (99) (ECSMR).

(98) DCMS, Telecommunications Security Code of Practice
(99) Legislation.gov.uk, The Electronic Communications (Security Measures) Regulations 2022

- In particular, Section 13 of the ECSMR set out competency requirements which are likely to be relevant here. They set out that the responsible persons require "appropriate knowledge and skills to perform their responsibilities effectively", and that where third parties are used, they are "competent to show appropriate understanding and appraisal of the activities of third party suppliers and of any recommendations made by third party suppliers". Section 7(5) also sets out an obligation on operators to have at all times a written plan to "maintain the normal operation of the public electronic communications network in the event that... a third party supplier is interrupted." Similarly, Section 7(4) sets out that there must be "written plans to manage the termination of, and transition from, contracts with third party suppliers."
- Each of these requirements is likely to introduce complexity and security barriers to the adoption and use of AI in telecoms networks, given the increases in costs faced by operators to meet these requirements. These requirements themselves are entirely reasonable, but they will require non-trivial expert capacity in operators, to understand these technologies.

11.3/ Over-Optimism Bias in Those Using AI

Over-optimism bias in those using AI, including automation bias, towards accepting recommended solutions due to inertia:

- "It's shiny new tech, it must be the latest and greatest" – when ChatGPT became available to end users, there have been many end-users who believed that it was accessing the internet (which it was not capable of doing, and was not doing – its training had a hard cut-off at September 2021 at the time). Despite this, users asking ChatGPT questions could get it to issue responses suggesting it had accessed the internet. These were not true, but users were willing to believe it, despite it being untrue. Users are often over-optimistic about the capabilities of technology, and believe what they are told, when it seems authoritative, rather than questioning and critically evaluating it for themselves. This is likely to especially be the case for users who are less intricately familiar with the workings of the AI technology in question.
- Example – two New York attorneys were formally sanctioned by a judge for submitting a legal brief containing fictitious case citations generated by ChatGPT, finding they acted in bad faith, and made "acts of conscious avoidance and false and misleading statements to the court" (100) – they simply did not believe that ChatGPT could make up false cases. Of interest was the methodology one of the attorneys used, by asking ChatGPT itself if a case was real, and what its source was – ChatGPT responded after "double checking" (which it did nothing of the sort) that the case was real and could be found on legal reference databases like LexisNexis and Westlaw (which it could not be, as the case was not a real one) (101).

(100) Reuters Article, New York lawyers sanctioned for using fake ChatGPT cases in legal brief by Sara Merken
(101) BBC News Article, ChatGPT: US lawyer admits using AI for case research by Kathryn Armstrong

11.4/ Provenance of Pre-Trained Models

Provenance of pre-trained models, and training processes for self-trained models:

- There are interesting potential use-cases for AI in classifying and categorising traffic and using it to hunt for wheat among the metaphorical chaff.
- One scenario commonly given as an example for the use of AI is in monitoring traffic flows for security-related findings or indications. An AI classifier could be trained on both malicious and benign traffic, and then attempt to detect new, previously unseen, traffic flows or patterns.
- For use-cases like this, with a defensive security implication, there are important considerations around the provenance of models used for these purposes – they present a clear opportunity for an adversary to (for example) use their own training data-sets which are derived from legitimate data, but which also contain data approximating some of their own "prepared" weaponised attack techniques, in order to train the classifier not to alert on such traffic.
- This introduces two key considerations – who trains the AI models (i.e. on whose compute infrastructure and under whose supervision this takes place), and the provenance, inspectability and supply chain security of the training data used.
- Given that multiple telecoms operators are likely to deploy the same vendor products, there may be an economy of scale in using "black box" models provider by vendors – potentially existing equipment vendors, or new security solution vendors. These would become points of risk aggregation across multiple telecoms operators, and potentially a critical point of failure. Such a vendor would likely sit outside of the direct purview of security review over operator personnel, yet such an arrangement would entirely outsource responsibility for training the model to this outside provider, whose personnel could elect to include (or not include) certain training data, or influence the labelling process.
- Where labelling (or categorisation/ground truthing) of training data takes place, the provenance and supply chain of this should be considered – many internet technology companies have resorted to using low-paid contract labour for these tasks (102). Systemic labelling errors on data could lead to classifiers ignoring particular inputs, or wrongly categorising them, which would affect the integrity of the underlying system.

11.5/ Commercials of Pre-Trained Models

Commercials of model training leading to use of pre-trained models

- Given the recent increase in the profile of AI technologies, and rapid growth in demand for chipsets and hardware to carry out AI training and inference, there are security considerations around how training is carried out.

(102) TIME Article, OpenAI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic by Billy Perrigo

- Given the costs of hardware required for efficient model training (like leading-edge AI series GPUs), there is a shift towards use of multi-tenant cloud-based computing. This both reduces capex outlays (by avoiding the need to buy a rapidly depreciating GPU, which will likely only be top-of-the-range for a year at most), and enables efficiencies through flexibly allocating hardware access across organisations in a multi-tenant environment since GPUs can be time-sliced between end users, delivering efficiencies where an end user is not training models 24/7.
- Where servers or GPUs outside of the control of the telecoms company are used, there should be consideration given to the potential for residual code to "inject" into training processes. This is a concept seen previously in cloud computing through cross-tenant isolation. There is however an emergent threat in AI, given that it is very hard (or impossible) to inspect an AI model (i.e. the output of a training process) and tell whether it is legitimate, correct, or tampered with. Given model generation from training data is generally non-deterministic, it would also not be sufficient to spot-check reproducibility of training on independent infrastructure and seek the same model output.

11.6/ Use of Non-Deterministic Logic

Use of non-deterministic logic in NCSC-designated security critical or network oversight functions of a network

- Many of the heralded benefits of the use of AI will be in areas of networks that are considered security critical, or network oversight functions.
- For instance, the Code of Practice sets out a range of network oversight functions in Paragraph 1.8, such as element managers, virtualisation orchestrators, and OSS systems.
- Providing any automated system with management and control plane access will be a challenge – for human users with management access, this needs to be carried out from privileged access workstation (PAW) type devices, per Section 4(4)(a) of ECSMR. Providing access to an AI system (assuming internally hosted) could be achieved if it was itself isolated from outside systems and the internet.
- Were there a desire to introduce updatable logic into AI models, these would end up more widely connected in the network, and the process of updating the AI model would break the "air gap" between outside influence and the logic being used to control a network. The introduction of a malicious model as a means to gain lateral movement should be considered here – this will require careful consideration of how to restrict and independently monitor the actions carried out by AI network management functions (without relying on AI for this task, in order to avoid malicious actions going undetected!)

- Use of AI is likely to be to drive down personnel costs in tasks that are perceived to be automatable. There are open questions around (for example) whether this will help or hinder people in roles like Security Operations Centres – while AI might help them to focus on suspicious traffic flows, it is not clear, yet that AI will help them to react better, or if it may reduce their capability, by causing people to defer to the automation as it's "normally right." This could cause staff to be less proactive and miss novel attacks that the AI does not spot, but the human would previously have detected.
- If more capability to control systems is granted to AI-based control systems, there is likely to be less accountability and governance review around use of such access – what may previously have required multiple independent authorisations and review processes may be able to be carried out by a single AI model running on a server under the control of a single system administrator in the operator or, even more dangerously, under the control of an outside party or vendor.

11.7/ Vendor Remote Access

The requirement for vendor remote access for new technologies

- Increasingly, telecoms vendors seek remote access to the systems they install in operator environments, to provide technical support, and provide managed services such as upgrades and maintenance.
- AI systems provide a new risk channel, in that the loading of a model is likely to present a difficult-to-manage risk – pre-trained models are opaque "blobs" of data, and it is not feasible to compare or inspect these and understand the changes made.
- Where AI systems have access to control or management functions, these will also likely require remote access and support by vendors or third parties – remote access to a system exercising powers on the network that would perhaps not have been afforded to outside providers or third parties at all. This introduces a new range of second-order risks around introduction of implants to a network via remote support staff (who are likely to be off-shore and potentially based in countries where there is limited ability to assure a lack of connection to state-affiliated attackers).

11.8/ Confidence in Telecoms Sector

AI in customer service causing even further loss of confidence in telecoms sector

- E.g. can't report a security issue to the CSP because they are using AI-based customer service that doesn't understand the contact, or doesn't provide a proper channel to an intelligent technically capable individual in the org.
- Same as the risks of having incompetent/badly trained support staff (which is an issue many CSPs have today), but potentially with higher legal liabilities when someone eventually takes a telco to court and prevails with a large award and an angry judge.

ACRONYMS

Acronyms	Description
3GPP	The 3rd Generation Partnership Project
AI	Artificial Intelligence
BSS	Business Support Systems
C-SCRM	Cyber Supply Chain Risk Management
CNI	Critical National Infrastructure
COTS	Commercial Off-The-Shelf
CPE	Consumer Premises Equipment
CRA	Cyber Resilience Act (EU)
CRM	Customer relationship management
CSP	Communication Service Providers
DLT	Distributed Ledger Technology
DSIT	Department of Science, Innovation and Technology in UK
ETSI	European Telecommunications Standards Institute
EWG	Expert Working Group
FOSS	Free & Open Source Software
ICO	Information Commissioner's Office
IETF	Internet Engineering Task Force
MNO	Mobile Network Operators
NFV	Network Functions Virtualisation
OSS	Operations Support System
R&D	Research & Development
R&D&I	Research, Development, and Innovation
RAN	Radio Access Network
RED	Radio Equipment Directive (EU)
RFC	Requests for Comment
RIC	Radio Access Network (RAN) Intelligent Controller
SAI	Securing Artificial Intelligence
SDO	Standards Development Organisations
SWOT	Strengths, Weaknesses, Opportunities, And Threats
TRL	Technology Readiness Level
TSA	Telecoms Security Act in UK

Refer to NIST for a detailed list of System and Network Security Acronyms and Abbreviations (103)

(103) NIST, System and Network Security Acronyms and Abbreviations

13/ Contributors

Members of the Expert Working Group are listed below. Members are voluntary, selected via an open selection process, and participate in an independent capacity, not on behalf of their organisations.

Name	Role / Position
Dave Happy	Security EWG Chairperson, Non-Executive Director Jet Engineering and MD Telint Ltd
Greig Paul	Security EWG Vice Chair, UKTDTF, Strathclyde University
Hamid Falaki	Specialist Adviser - UK Telecoms Network, University of Bristol
Anas Tawileh	Senior Advisor, AWS
Danny Skipper	Team Lead, UKTL / NPL
Jon Renshaw	Deputy Director Commercial Research, NCC Group
Paddy Paddison Nick Hampson	CTIO, Wildanet Head of Innovation, Wildanet
Rob Leenderts	Director, INCA, and CEO Hubbub
Stephen Douglas	Head of Market Strategy, Spirent
Steve Pattison	ARM (rtd)
Vasilis Katos	Professor of Cyber Security, Bournemouth University
Colin Wood	Head of Econ Development, Dorset Council
Siraj Ahmed Shaikh	Professor in Systems Security, Swansea University
Daisy Curtis	Associate Lecturer and PhD Researcher, University of Exeter (Security working Group Observer)

Version Control

Revision	Description	Author(s)	Date
1.0	First draft	EWG	01/12/2023
2.0	Updated UKTIN's comments	EWG	
3.0	Revised based on first round of feedback	EWG	26/01/2024
4.0	Revised include comments from DSIT & UKTIN-AB	EWG	20/02/2024
5.0	Revised for external publication	EWG & UKTIN	08/03/2024
6.0	Clean Copy for Digital Print	UKTIN	10/03/2024