GCOT Security and Resilience Principles for 6G

1 GCOT Foreword

The next generation of mobile networks – 6G – is already taking shape. Industry standardisation is still in its initial stages, with the main services and requirements still being drafted and the specifications likely to evolve significantly over the lifespan of the generation. However, some broad predictions can be made based on the IMT-2030 Framework and initial 3GPP 6G studies:

- Artificial Intelligence will be supported natively both to improve network performance and enable new user services;
- Mobile networks will have the capability to support sensing (from both base stations and user devices), through the integration of external sensors and exploitation of communications signals themselves;
- Terrestrial and non-terrestrial technologies will be more tightly integrated, to expand seamless connectivity into currently underserved areas and increase network resilience;
- Spectral and energy efficiency over 5G Advanced systems will be significant priorities;
- More network functions will be virtualised, reducing reliance on specific hardware platforms and increasing the flexibility of network resource deployment; and
- Disaggregated architectures and standardised interfaces will enable better visibility for security, and better multi-vendor integration.

One of the central questions about 6G is commercial appetite and how to balance total cost of network ownership with the desire to roll out new service offerings. It would be reasonable to expect the success of the new generation to rely substantially, as with previous generations, on high uptake in mass market consumer devices like smartphones, and improved service offerings centred around those. Critically, uptake of 6G will depend on its commercial viability for network operators, determined by performance across a range of key metrics like spectral and energy efficiency which are still being thoroughly studied.

However, the development of 6G networks must also be understood as a matter of broader public and strategic interest, rather than a purely commercial or technological undertaking. 6G networks will be key pieces of society's digital infrastructure, underpinning essential services and vertical industries from manufacturing, transportation, and energy to healthcare and public safety. The standardisation process has to some extent already recognised this, with societal issues identified in the Overarching Design Aspects of the ITU's IMT-2030 Framework.

The security and resilience of 6G networks are critical aspects of that wider picture. 6G networks – both public and private – will come to play a vital role in the everyday life of people around the world, with much of our lives reliant on their efficient and secure operation. That matters to industry as much as to governments and regulators; we will only be able to maximise the commercial potential of 6G networks if consumers and businesses can trust them to provide secure and resilient services and to safeguard the privacy of user data. These networks will be part of our Critical National Infrastructure, and as such it is essential that they are secure and resilient by design – setting a high baseline that supports operators in maintaining sufficiently secure and resilient networks despite economic pressures.

We anticipate that new capabilities and developments will deliver a wider-reaching, more complex, and more data-rich communications system; however, in many cases, they will also bring a wider attack surface with greater opportunities and access points for malign actors. Alongside these challenges posed by new architectures and technologies, there will also be security challenges inherited from 4G and 5G systems, particularly where there is reliance on legacy systems and protocols with proven vulnerabilities or where continued interworking with 4G and 5G (and other) systems exposes traffic to differential levels of protection. It is vital that we do not allow the security of 6G systems to be determined by the security of legacy systems, including where backwards compatibility is required. The 6G system must be sufficiently separated from legacy systems with identified current or likely future security vulnerabilities, in order to minimise the risk of compromise. Further, the threat picture will continue to evolve. For instance, over their deployment lifetime, 6G networks may be exposed to increasingly sophisticated quantum computing, which will transform some of the security and encryption paradigms our communications infrastructure currently relies on. All these issues need to be grappled with as early as possible in the design and delivery of these systems.

Network resilience is a priority in its own right. Countries deploying 6G networks will continue facing resilience challenges of various kinds, whether from difficult geography and natural disasters, or market dynamics and concentration that create single points of failure or widespread supply chain dependencies. These can be managed to some degree through measures including targeted procurement strategies and good information sharing between suppliers and operators about supply chain dependencies. However, in the case of network supply issues, the risk of single points of failure in network supply will still need to be mitigated. GCOT partners have already taken steps to address this through various regulatory and research initiatives such as Canada's Telecommunications Reliability Agenda, Japan's Innovative ICT Fund Project for Beyond 5G/6G, the UK's Telecommunications Security Act and Open Networks Programme, and the U.S.'s Public Wireless Supply Chain Innovation Fund.

GCOT partners agree that the ongoing standardisation and eventual deployment of 6G networks must pay due regard to these evolving security and resilience challenges. The technological innovation anticipated from 6G, twinned with its central role in national infrastructure (as with current mobile networks), will require fundamental protections and mitigations to be considered from the outset. That will require action on the part of governments, telecommunications providers, and those supplying the systems they rely on, including cloud and data infrastructure. It will also mean close working with domestic and regional regulatory bodies, and through public-private partnerships, where appropriate, to ensure common understanding of threats and robust compliance.

2 Outcomes and Purpose

This statement aims to outline some of the critical security and resilience considerations that GCOT partners recommend be prioritised in the ongoing development of the 6G system. At a high level, the 6G system should provide the following positive security and resilience outcomes:

1. **Containment:** The 6G system limits the ability of malicious actors or software to propagate through the network.

2. **Confidentiality:** The 6G system is built by design to protect the privacy of user data and able to process and provide data confidentially, e.g. it is secure against eavesdropping or attackers, even for data shared over channels which are not physically secure or known.
3. **Integrity:** The 6G system is able to maintain the integrity of data providing guarantees that any changes to data, as it travels through the network, are perceptible. Equally, the integrity of network infrastructure itself should be assured.
4. **Resilience:** The 6G system is measurably resilient and able to maintain service availability for users even in challenging circumstance – in particular for requirements like emergency or first-responder voice and data services, which must be future proofed in the transition to 6G. This includes secure and resilient supply chains.
5. **Regulatory Compliance:** The operators of 6G systems are able to fulfil the requirements of relevant national regulations and legislation.

The following principles set out some of the key technological means for 6G to achieve these outcomes. The introductory text in Sections 3 and 4 provide some overarching framing for Security and Resilience respectively, followed by specific principles in the subsequent subsections. Each principle is set out in grey at the top of each section, with explanatory text beneath.

These principles will help to guide ongoing GCOT collaboration on these issues, but they are also intended as a guide for all relevant stakeholders on the areas of significant concern in our jurisdictions. The development of 6G will be a collaborative effort involving the whole communications sector. GCOT partners would therefore encourage efforts from industry, academia and others to ensure that these principles are considered from the outset in standardisation and deployment of 6G.

3 Principles – Security

> The 6G system should be developed with security as a foundational principle – considered at all stages, from development to deployment and ultimately operation. The 6G system must be consciously designed to be more secure than previous generations, and manage legacy vulnerabilities where it relies on existing systems. Security controls should be informed by a proper examination of current and future threats, and decisions about the architecture and overall system requirements of the 6G system should properly consider the security model that they need to enable at an early stage and how they might need to evolve.

The promises of 6G – connectivity, growth, and innovation – can only be fully realised if networks are secure, so that user confidence is not undermined. Public networks are facing unprecedented levels of malicious cyber activity, of an increasingly sophisticated nature, so it is essential that they have sufficient security controls in place to ensure that the sensitive information carried across them is protected at the appropriate level. These networks form and support our Critical National Infrastructure and must be secured accordingly. Good security is

then not just an additional technical requirement, but a foundational pillar that will determine the success and adoption of the next generation.

A new generation of mobile technology brings an opportunity to examine critically the assumptions and working practices that have driven network design and implementation in previous generations. The doctrine of 6G being "secure by design" is now widespread but as the initial 6G system is developed, it is imperative that we move from rhetoric to practice – building upon the progress we have seen in 5G. If security is not understood and integrated properly into architectures and solutions from the outset, including secure interworking with third-party and legacy systems, the cost of retrofitting or patching systems later will be prohibitive both to communication providers and to consumer safety and trust. 6G needs to be designed and implemented to avoid implicit trust of previous generations or peer networks with a clear logical separation for security. For example, hosting Mobile Virtual Network Operators (MVNOs) or backward compatibility for legacy signalling should not reduce assurance of the security of the 6G system. Sections 3.1 and 3.2 discuss how we secure internal and external interfaces, respectively, to embed security in the underlying architecture of the 6G system – in line with the principles of Zero Trust.[1]

As with previous generational evolutions, we should expect continuous enhancements to the 5G system paradigm, including the resolution of cyber security design issues inherited from legacy systems or which real-world deployments have thrown into relief. At the same time, we expect that 6G will bring novel challenges and threats, such as richer sources of data to secure at greater volumes, and AI and sensing capabilities that can both enhance and endanger security – as discussed in Section 3.3. This includes technologies (like AI) that may, in part, sit outside of the scope of the main 6G standardisation bodies like 3GPP, but whose security will be essential to a successful and secure 6G deployment.

It is essential that whatever innovations are adopted are securable and respect the privacy of user data from day one, including third-party services that 6G networks rely on. That will require a fresh look at threat models, and a strong testing ecosystem that can check standards compliance and true operational resilience. Our approach to cyber security and the tools we use must also continue to evolve to protect users from current and emerging threats into the future. This includes the advent of cryptographically relevant quantum computing – discussed in Section 3.4.

[1] NIST SP 800-207, Zero Trust Architecture (ZTA) (https://csrc.nist.gov/pubs/sp/800/207/final).

3.1 Security Monitoring, Authentication, and Authorisation

> The 6G system should transition away from perimeter security to more granular function-level security in line with the principles of Zero Trust, with continuous security monitoring of the network and effective logging to assess dynamically the likelihood of potential compromise of network components. This should be coupled with robust authentication and authorisation of individual network components, based on a rule of verification before use and limiting a given component's access to only data required to fulfil its function.

6G looks to continue the trend of 5G towards greater virtualisation of network functions, decoupling software from underlying hardware platforms and hosting network functions on different generic compute platforms. In many cases, this utilises the scale and flexibility of cloud computing (either public, private or hybrid) to host a large number of network functions, and potentially other applications, on the same compute platform. There is also likely to be greater support for equipment and software from a number of different vendors to be integrated into a single mobile network stack. Further, the greater integration of AI in network management and the introduction of greater sensing capabilities will expose more data of different types across the network, building and relying on new relationships with third-party providers and consumers of network services.

These trends bring a number of potential benefits, both in terms of innovation and resilience (as discussed in sections 3.3, 4.3, and 4.4). However, they also present a reshaped and often wider attack surface that traditional perimeter security approaches are ill-suited to handle. This will require adherence to a critical aspect of the Zero Trust Architecture concept: robust security protection and authentication within the network, as well as at the boundary. As has now been recognised for 5G, 6G must move away from the design assumption that anything "inside" the system is automatically trustworthy. Network functions must be regularly and robustly authenticated before being given access to other network functions or data sources, with access granted for a given task and authorisation policies appropriate for specific contexts and data criticality. This should account for the particular sensitivities of different data types, such as the privacy considerations around collection and distribution of new sensing data. Authentication should also extend to underlying platforms, with secure roots and chains of trust.

Overlaying this, operators should be able to monitor network components and entities (including e.g. user devices and AI agents) for unusual activity or execution of undeclared capabilities – detecting potential intrusions early and suitably updating authorisation policies to limit the ability of malicious actors to propagate across the network and exfiltrate sensitive data. That will require 6G systems to be able to examine and analyse (and potentially expose to operator monitoring systems) information from across both radio access and core networks, to allow monitoring and incident detection, all while safeguarding user privacy. This should also include sufficient observability to monitor for potential attacks across isolation boundaries, for example exploiting vulnerabilities in underlying platforms to attack hosted network functions, or lateral movement of malicious actors between network slices.

While robust security standards for network functions and applications will play a vital role here, deployment models and architectures will also need to provide adequately secured physical and digital infrastructure for 3GPP and other standardised network functions to reside on. This includes rigorous configuration management, ensuring all network components and functions adhere to a strong security baseline from deployment and are continuously monitored and maintained to prevent misconfigurations. Furthermore, standards and/or regulation will need to ensure that cloud deployments can be tailored to mitigate increasing sovereignty concerns related to telecommunications networks as Critical National Infrastructure (CNI).

3.2 Secure External Interfaces

> The 6G system should support the robust security of interfaces with external (including legacy) networks, subnetworks, and other systems in order to maintain the privacy and integrity of user data and the security of the home network, whilst still adhering to local regulatory requirements for roaming users. The 6G system's overall security should furthermore not presume the security of networks or systems whose security is outside of the control of the home network operator.

Extending connectivity to currently underserved areas is a vital objective of 6G – as evidenced by the designation of Ubiquitous Connectivity as a key IMT-2030 Usage Scenario by the ITU.[2] To achieve this, subscribers are likely to engage with 6G as part of a broader "network of networks", with user data travelling across PLMNs, subnetworks, across satellite and terrestrial systems, and between 3GPP and non-3GPP access types (principally WLAN/Wi-Fi). This will also include legacy systems that present security challenges, and networks whose security is outside of the user's home operator's control.

In tandem, as mobile operators look to diversify revenue streams and other industries look to drive increased productivity via connectivity enhancements, 6G is likely to see a renewed focus on supporting so-called vertical applications such as e-health, smart manufacturing, and autonomous vehicles. With this will come an increasing diversity of connected devices, including typical smartphones, smart wearables, distributed IoT, and more – many having to support very low-cost production and very low energy consumption. These different devices will come with a range of security requirements specific to the data that they carry and the environment that they operate in, a range of hardware and software limitations, and vastly differing device refresh cycles (considering both hardware and software updates/refreshes) that need to be accounted for when designing their security. Further, enabling functionalities and services such as "AI as a Service" and programmable Application Programming Interfaces (APIs) will require new external interfaces for data exposure out of the network, expanding the potential attack surface (as also discussed in section 3.3).

Interaction with such a variety of systems cannot be treated as a bolt-on to the overall security paradigm for 6G; it must be integral to it. Communications providers must be able to maintain the integrity and privacy of user data as it traverses this complex, highly heterogeneous network

[2] Recommendation ITU-R M.2160-0 (11/2023) - Framework and overall objectives of the future development of IMT for 2030 and beyond (https://www.itu.int/rec/R-REC-M.2160-0-202311-I/en).

of networks. Interfaces between different networks, subnetworks, and with external applications need to be properly secured to limit the potential impact that security weaknesses of systems outside of the home operator's control can have on the broader network – including comprehensive API monitoring and governance. This should build on the Zero Trust approach to securing internal interfaces outlined in Section 3.1. However, relevant mechanisms should also comply with regulatory requirements for roaming users.

Beyond the interfaces themselves, the exposure of data from 6G systems should maximise user privacy and adhere to the data minimisation principle – ensuring the third-party networks and services can only access data required to fulfil their authorised functions. This includes measures such as rigorous data classification, appropriate encryption (including at rest and in use, where appropriate), and clear data lifecycle management policies.

3.3 AI for Security and Secure AI

> The 6G system should take advantage of AI-driven mechanisms to more quickly and effectively monitor and respond to potential cybersecurity threats and incidents. At the same time, AI systems in telecommunications should be developed, deployed, and operated in a secure and safe manner.

GCOT has already drawn attention to the need for AI systems to be integrated into 6G systems securely and leveraged for ongoing security monitoring and response, in our principles on AI adoption in the telecommunications industry.[3]

AI presents a significant opportunity to enhance 6G system cybersecurity. AI within the network ("AI for Network") can help to provide the essential monitoring and response capabilities needed for 6G networks to respond to malign behaviour, detecting potential breaches earlier and supporting efficient remedial action – improving upon current "anomaly detection" systems. Adjacent developments, such as digital twins, may also support enhancements to the capabilities of AI security tools in future.

At the same time, we must ensure that AI systems and processes (including those hosted externally) are designed and deployed with strong security embedded throughout the AI lifecycle, including verifying the quality and provenance of training data, and that responses to security incidents in the network are supervised and appropriate. Without appropriate security requirements, the use of AI in networks could result in greater vulnerabilities to attacks and new threat vectors, such as poisoning of training datasets and backdoor attacks. This could draw on relevant industry or research-led efforts in different jurisdictions.

The integration of agentic AI into 6G systems is expected to be a significant feature of future networks. How these agents act across networks, interact with one another and with existing network functions, are managed, and kept updated with network information remain points of

[3] Global Coalition on Telecommunications: principles on AI adoption in the telecommunications industry (https://www.gov.uk/government/publications/global-coalition-on-telecommunications-principles-on-ai-adoption-in-the-telecommunications-industry/global-coalition-on-telecommunications-principles-on-ai-adoption-in-the-telecommunications-industry).

contention. Agentic systems may well offer significant advantages to network operators in delivering enhanced network performance and personalised services to customers, as well as potentially being useful tools in the detection and resolution of any recorded anomalous behaviour in the network. At the same time, it is critical that agentic systems are designed after a robust threat modelling and analysis, and are only integrated into systems alongside robust control, authentication, and assurance mechanisms.

We must consider whether and what restraints are appropriate on the actions AI systems or agents are able to undertake autonomously, as well as mechanisms for secure recovery if AI services fail. Security mechanisms outlined in sections 3.1 and 3.2 apply here as well. This will require effective coordination between standards bodies like 3GPP and the IETF to ensure that agent authentication and authorisation are based on industry standard practices, and communication between them is properly secured and sufficiently robust to merit inclusion in our Critical National Infrastructure. Beyond the technology itself, deployment of AI agents must also properly account for potential risks arising from human error in training, deploying, supervising, and updating AI agents, whilst still enabling sufficient access to network data to fulfil their function. There are also challenges in determining clear lines of accountability for tasks handled by AI agents.

In general, care must also be taken in enabling "Network for AI" capabilities, such as using latent network resources to complete third party compute tasks or model training. The integrity of data moving in and out of the 6G system for use by or for third-party AI services must be maintained and verified at all times – in line with the requirements laid out in section 3.2.

3.4 Quantum-Safe

> We expect 6G to support quantum-safe cryptography from day one, based on widely accepted quantum-safe cryptographic algorithms/ technologies such as those standardised by the US National Institute of Standards and Technology (NIST). This should be implemented through appropriate standards processes, with strong international cooperation.

Cryptography forms the vital backbone of mobile network security, ensuring the confidentiality and integrity of sensitive data as well as underpinning robust authentication mechanisms to prevent unauthorised access. For each generation of mobile communications, the cryptographic algorithms in use are re-visited and updated to reflect increases in computing power or newly-discovered techniques for more efficient attacks. However, in many cases, it has previously been sufficient to simply update the parameters (such as minimum key lengths) of legacy algorithms without fundamentally changing the underlying structure. Much of the Public-Key Cryptography (PKC) in use today still relies on the intractability of mathematical problems such as integer factorisation and calculating discrete logarithms, which have been at the core of PKC algorithms since their creation in the 1970s.

The advent of Quantum Computing represents a step-change in the field of cryptography, using properties of quantum mechanics to compute in ways that are fundamentally different from classical computers. It has been shown theoretically that a large, general-purpose quantum

computer, known as a Cryptographically Relevant Quantum Computer (CRQC), could efficiently solve many of the mathematical problems that underly modern PKC and undermine the security of current cryptographic algorithms. While current quantum computers are not sufficiently advanced to threaten current PKC algorithms, the introduction of 6G systems should carefully take into account the expected timeframe for the migration to "quantum-safe" cryptographical algorithms/technologies.[4] In addition, "harvest-now-decrypt-later" threats, where malicious actors store encrypted data so they can decrypt it once sufficiently powerful quantum computers are available, pose a risk to sensitive data transmitted today that is encrypted using algorithms theoretically vulnerable to quantum attacks. Therefore, where broader enabling standards (e.g. relevant internet protocols from the IETF) are developed and made available sufficiently quickly, we expect 6G to support quantum-safe cryptography from day one, though transition deadlines may vary by jurisdiction. Where or if there is an unavoidable delay, the 6G system should have proper mitigations in place to manage the consequent risks.

As part of this transition, it is vital that newly proposed quantum-safe cryptography is subject to proper scrutiny by the research community, given its importance to the 6G system. For example, NIST's process for developing their first post-quantum cryptographic algorithms pushed proposed algorithms through multiple rounds of scrutiny over an 8-year period before its first standards were published.[5] We must ensure that any proposed solutions are robustly tested to allow confidence in their viability and network performance, particularly for areas like critical communications.

The transition to new algorithms/technologies, including support for greater cryptographic agility, should then move through the appropriate standardisation processes. This will improve the consistency and security of implementations as well as enable proper interoperability between systems. This will involve a wide range of standards bodies, such as the IETF, 3GPP, and the O-RAN Alliance, which will review current recommendations for ciphers and associated cryptographic primitives, protocols, and key management practices.

Once appropriate quantum-safe cryptographic algorithms/technologies are developed and widely accepted, traditional asymmetric cryptography must be systematically identified and phased out. The implementation of new algorithms should be tracked comprehensively through a Cryptographic Bill of Materials (CBOM) or cryptographic inventory for all relevant network functions or elements. This should be supported by shared best-practice, and international cooperation will be vital.

[4] UK NCSC Timelines for migration to post-quantum cryptography (https://www.ncsc.gov.uk/guidance/pqc-migration-timelines).
[5] US NIST Post-Quantum Cryptography project (https://csrc.nist.gov/projects/post-quantum-cryptography).

4 Principles - Resilience

6G must be engineered with resilience by design to ensure the continuity of essential public safety, critical infrastructure, and consumer services during periods of disruption. This requires moving beyond simple protection to include intelligent adaptation and rapid recovery. To be effective, these capabilities must be verified through internationally standardised quantitative metrics, establishing a reliable performance baseline that can be promoted across jurisdictions.

As the global economy becomes increasingly dependent on the uninterrupted operation of our mobile networks, the potential impacts of any service disruption grow far more severe. Beyond safeguarding against cyber-attacks, the future 6G system must be fundamentally engineered for resilience. This is a multi-faceted capability that encompasses not only the protection of network infrastructure against harm but also the ability to intelligently adapt to changing conditions (often leveraging AI) and, crucially, to recover with minimal delay following any natural or man-made (including AI-related) disruption. This includes disruption to vital supporting services, such as power outages. A truly resilient network is one that can anticipate, withstand, and quickly recover from faults, ensuring service continuity for public safety, critical infrastructure, essential government services (such as emergency calling), industry, and consumers.

To achieve this, resilience must be treated as a foundational principle – a “resilience-by-design” approach integrated throughout the entire system lifecycle, from initial standards to operational testing. The GCOT partners view this as moving resilience from an abstract concept to an achievable engineering goal supported by international standards, and by developing ways to measure it quantitatively. Establishing standardised metrics, such as 'time to full recovery' or 'service availability under specific threat scenarios', will allow stakeholders to assess and independently verify the robustness of systems, ensuring accountability across jurisdictions and helping to inform national policies and regulatory requirements. This ability to quantify resilience is the critical first step toward ensuring a minimum acceptable level of service can be maintained, even under duress. This should include consideration of how different failure modes relate to each other, designing and deploying systems to avoid cascade failures that significantly hamper recovery. These resilience capabilities will be built and managed nationally according to each country’s requirements, relying where useful on national-level guidelines, such as the UK Ofcom’s Network and Service Resilience Guidance for Communications Providers and the U.S. Federal Communications Commission’s Mandatory Disaster Response Initiative.[6]

A key operational outcome of this resilient design is the capability for safe failover: an intelligent process to maintain critical service continuity during a crisis, discussed in Section 4.1. This includes both dynamically prioritising traffic within the network and, when necessary, seamlessly switching to alternative access networks, such as satellite, or alternative carriers where necessary. The GCOT partners emphasise that this vital capability; however, it must be

[6] UK Ofcom Network and Service Resilience Guidance for Communications Providers (https://www.ofcom.org.uk/internet-based-services/network-security/resilience-guidance); U.S. Federal Communications Commission (https://www.fcc.gov/wireless-network-resiliency-during-disasters).

built upon a foundation of absolute technical stability, including uncompromisingly resilient timing and synchronisation – discussed in Section 4.2. Where applicable, resilient AI should be used to optimise the reliability of 6G systems and expedite their safe failover when needed, as is discussed in Section 4.3.

Furthermore, the entire system must be sustained by a robust and secure industrial base. Fostering a diverse, secure, and resilient supply chain is therefore critical to the strategy of mitigating long-term vulnerabilities. This includes building upon the strong foundation of 5G Open RAN to ensure that 6G is open and interoperable, to support multi-vendor RAN – discussed in Section 4.4. However, resilience in the broader 6G supply chain should also be considered, including new supply chains arising from the integration of new technologies into the 6G system, such as non-terrestrial networks.

By addressing these foundational, structural, and operational layers in concert, this approach aims to deliver a 6G network engineered to preserve the continuity of essential societal, economic, and government services under adverse conditions.

4.1 Safe failover

> The 6G system should support the autonomous detection of disturbance and the capability to reroute traffic through alternative access networks, including other modes and carriers, to maintain meaningful user connectivity (to the extent capacity allows), dynamically prioritising traffic based on criticality.

Risks of disruption to network equipment include not just the base stations themselves but also damage to supporting infrastructure such as fibre backhaul and power supply, instances of human error in network operations, or problems with software updates. In cases such as natural disasters, it may be infeasible to quickly re-operationalise terrestrial mobile infrastructure, increasing the length of disruption to normal user service as well as potentially hampering emergency response efforts. The integration of alternative access networks and those operated by other carriers, particularly those less reliant on terrestrial infrastructure, will therefore likely be key to bolstering the resilience of our future mobile networks.

Alongside this, the network also must have the capability to quickly and safely failover to these alternative access networks when required, to minimise user-experienced downtime. This should include mechanisms to dynamically prioritise traffic based on assigned criticality levels, maintaining critical communications when capacity is significantly reduced, and end-to-end management of any single points of failure. For emergency calls, these alternative access networks must also meet inbound roaming requirements. Further, there should also be mechanisms to balance load across alternative networks, to avoid overload, and robust security controls to protect against user devices automatically connecting to false base stations in these circumstances.

4.2 Resilient Position, Navigation, and Timing

> The 6G system should implement complementary and augmentative non-GNSS Position, Navigation, and Timing (PNT) systems to reduce the risk of disruption to the network in the case of disruption to GNSS signal reception.

Current mobile networks rely heavily on traditional Global Navigation Satellite Systems (GNSS) such as GPS for precise timing and synchronisation. However, these systems are vulnerable to jamming and spoofing. The risks of such disruption will be further exacerbated by potentially more stringent timing and positioning accuracy (as well as e.g. jitter) requirements for 6G, for example for applications like collaborative robots in industrial processes or timing and synchronisation requirements for network security protocols. It is vital that timing synchronisation requirements for 6G systems are properly defined and understood.

Relying solely on current GNSS capabilities for future mobile networks, without the added redundancy of alternative precise timing systems to fall back on in the case of GNSS failure, therefore presents a significant resilience risk. Alternative Position, Navigation, and Timing (PNT) sources and mechanisms for PNT information distribution across the network – including those provided by alternative satellite sources, such as those in low-earth orbit (LEO), or terrestrial technologies – should be explored during the development of 6G specifications. UTC (Coordinated Universal Time) traceability should also be considered, for synchronisation of different timing distribution mechanisms in the call of GNSS failure.

4.3 AI for Resilience and Resilient AI

> The 6G system should explore how AI can be utilised to maintain system availability during disruption (e.g. natural disasters) and intelligently prioritise critical services. Such deployments of AI in 6G systems should also be designed to maintain effective operation over time, including through a clear and robust process for testing, verifying, and correcting AI models over the lifetime of the 6G system.

AI can be leveraged to enhance resilience against a variety of hazards, including natural disasters and system failures, ensuring continuous operation and rapid recovery in diverse scenarios. For example, AI can enable more dynamic and intelligent prioritisation of network resources for critical services, including coordinating resources between different available access networks – e.g. supporting safe failover, as discussed in section 4.1.

At the same time, these AI systems themselves must also be able to withstand and recover from disruptions, maintaining continuous operation and avoiding over-dependence. AI should be integrated into networks in a way that controls the disruption to network functionality if AI systems begin to fail and facilitates smooth recovery when faults in the AI system are remedied. Resilience also requires addressing inherent problems of concept and data drift in AI models, ensuring accuracy and effectiveness over time, with AI systems robust against errors in training data.

This will require the deployment of AI models from trusted sources, regular security audits, and the testing, validation, and verification of adopted AI models before, during and after deployment. It also means sharing, where possible, information on security incidents and vulnerabilities in telecom AI systems affecting multiple networks or operators. Communication providers must also pay due regard to the resilience challenges of failures or over-corrections driven by AI systems in networks and ensure that network management continues to allow for human intervention.[7]

4.4 Openness and Interoperability

The 6G system should enable Open RAN architecture and principles to ensure the support for day-one multi-vendor 6G RAN through open and standardised interfaces. Additionally, 6G development and deployments should explore mitigations (including potentially further disaggregation and additional open interfaces) where additional potential supply chain concentration concerns are identified, such as in the core network or in virtualised network functions. This should all adhere to the principles of:

- **open disaggregation**, which allows for modular and flexible network components from different vendors;
- **standards-based compliance**, which ensures compatibility and interoperability among different vendors;
- **demonstrated interoperability**, which verifies the performance and functionality of the network; and
- **implementation neutrality**, which avoids vendor lock-in and promote innovation and diversity.

As discussed in Section 3, this generation of mobile telecoms has seen increasing disaggregation of network functions – both breaking larger functions into smaller individual modules and decoupling software from the underlying hardware. Open RAN has built upon this by defining open and standardised interfaces between RAN components, through the efforts of the Open RAN (O-RAN) Alliance (building on top of 3GPP specifications), to enable easier integration of RAN components from multiple different vendors.

Allowing different vendors to supply individual components of the network or specific network services, versus e.g. the traditional model of single-vendor RAN, lowers the barriers to market access and supports greater diversity of supply for Mobile Network Operators (MNOs) procuring network equipment and services. This is an important step in reducing the resilience risks posed by shocks to global supply chains, as it reduces the cost and difficulty of MNOs switching to alternative suppliers, if required. Further, a greater diversity of suppliers within a mobile network can reduce the impact of systemic issues in specific equipment, such as software errors, malicious cyber activity, or other disruptions to supply.

[7] This could draw again on relevant industry and research efforts in different jurisdictions.

Within the network itself, disaggregation also tends to increase the simplicity of individual components and reduce (though not eliminate) their criticality and component cross-dependence, which should increase resilience over time. Additionally, well-specified interfaces allow for better visibility and monitoring of network behaviour, and better detection and investigation of abnormal behaviour, as well as supporting the easier development of security testing tools. However, a more open and interoperable architecture can also expand the attack surface and introduce new potential intrusion points for malicious actors, and this must be properly addressed. We have already seen positive progress here, with a strong focus on security in the development of Open RAN security, grounded in robust threat modelling and aligned with the principles of NIST's Zero Trust Architecture[8] and CISA's Zero Trust Maturity Model.[9] This offers a solid foundation for defending against both internal and external threats – in line with sections 3.1 and 3.2.

Arriving mid-generation for 5G, there has always been a delay between the release of 3GPP specifications and the corresponding Open RAN specifications. However, there is a risk for 6G that if such a delay persists, and 6G Open RAN specifications are published significantly later than 3GPP's corresponding initial 6G specifications, then the first 6G equipment to enter the market won't sufficiently enable true multi-vendor interoperability. This could push vendors back towards single-vendor RAN – losing much of the progress towards multi-vendor RAN that has been achieved during the 5G era.

To enable multi-vendor interoperability from day one in 6G, close coordination between 3GPP and the Open RAN Alliance is vital, both at an institutional level and at a working level between delegates in both organisations. Robust interoperability testing and certification should also be a key part of this approach, as outlined in GCOT's Open RAN certification principles.[10] On top of this, 6G development and deployments should explore mitigations (including potentially greater disaggregation) in other areas of the network to address existing or emerging supply chain concentration concerns. This could include potential new dependencies on platforms and infrastructure hosting virtualised network functions, or greater disaggregation of the mobile network core.

[8] NIST SP 800-207, Zero Trust Architecture (ZTA) (https://csrc.nist.gov/pubs/sp/800/207/final).
[9] CISA Zero Trust Maturity Model (ZTMM) (https://www.cisa.gov/zero-trust-maturity-model).
[10] Global Coalition on Telecommunications: Open RAN certification principles (https://www.gov.uk/government/publications/global-coalition-on-telecommunications-open-ran-certification-principles/global-coalition-on-telecommunications-open-ran-certification-principles).