WHITEPAPER

The Journey to Quantum Safety:

How Telecoms Operators Can Avoid a Y2Q

Published by

MOBILE WORLD LIVE

In partnership with

ARQIT

Introduction by GSMA Intelligence: Open RAN as a Post Quantum Warning

Every year, GSMA Intelligence works with mobile operators around the world to understand their network transformation priorities and challenges. How is the deployment of new network innovations proceeding? Which network investments do they plan to accelerate? Where are they running into deployment obstacles?

And, every year, we hear that network and user security are top priorities.

It's not difficult to understand why security factors so centrally into their planning and strategies. End-users – both consumer and enterprise – expect their connectivity services to be secure, and with security breaches becoming headline news on a near-constant basis, these users are paying attention to security more than ever. Operators who cannot protect their customers from vulnerabilities risk churn-inducing reputational impacts along with potential fines and regulatory pushback. And, with attack vectors including network infrastructure, service infrastructure, as well as end-user devices, keeping users safe has become an existential concern touching almost every part of an operator's business along with every team.

But, if this represents the "as is," what does the future look like? Unfortunately, the development of quantum computing innovations capable of cracking today's encryption solutions, means that operators will need to be increasingly vigilant. Yet, as with cross-cutting concerns like supply chain blockages or geo-political tensions, the existential nature of post-quantum security means it's not always clear where to focus when looking to develop a defense posture or simply to put the evolving threats into context. Here, drilling down into one specific network technology can be a useful exercise…especially since the #1 mobile operator technology priority for 2024 is Open RAN.

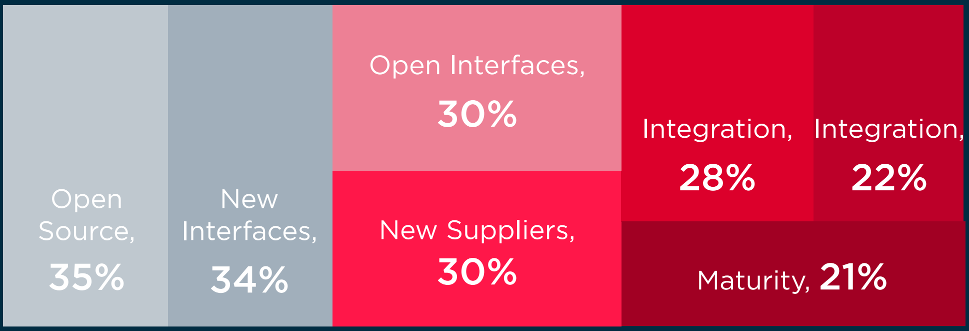
The Open RAN promise is fairly straightforward. Thanks to the use of standardized, open interfaces within the Radio Access network, operators can re-think the way they build their mobile networks, gaining an ability to mix and match suppliers or swap-in new ones over time. The benefits are just as straightforward: network investment protection via supply chain diversity, better bargaining power, and an ability to bolt-on new network innovations given the use of open interfaces. Deployment has been slow to ramp but operators around the works have made it clear that they see Open RAN as a strategic priority via press releases, vendor selections, and our surveys. These surveys, however, also point to a wide array of security concerns dogging Open RAN.

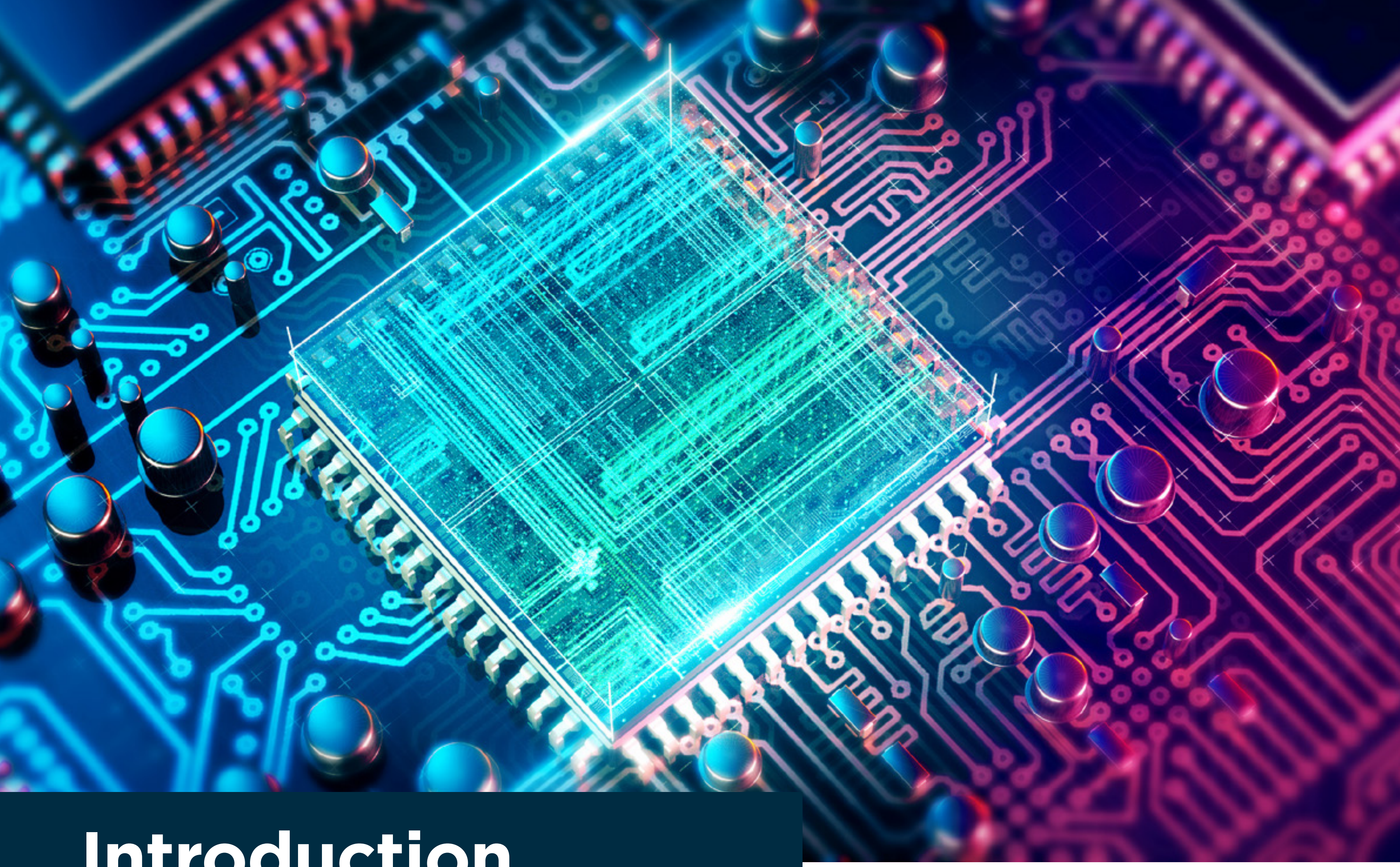
As we noted in an analysis from late 2022, the “newness” of Open RAN creates a number of potential worrying dynamics, introducing interfaces, suppliers and functions that operators aren’t necessarily familiar with. Combined with its open nature, the concern is that securing this top network priority will be anything but easy – and that’s in a pre-quantum world!

While Open RAN represents a major network focal point in 2024, there’s a larger message here; the need to integrate security thinking into how new technologies are planned and deployed alongside existing operations. Open RAN is a good example – because deployments are set to ramp and potential threat vectors are numerous – but it’s just one example. With quantum computing on the horizon, the need to begin planning for post-quantum network and service security in the here and now is very real.

Open RAN: Security Concerns

When deploying or valuating Open RAN solutions, what are your top security concerns?’





Introduction

Quantum computing will propel humanity into a new era of technology-powered progress. In so doing, it will offer an at-present unquantifiable opportunity to solve some of the biggest challenges facing the planet. But with tremendous opportunity also comes great risk. Quantum computing might sound like science fiction. But the smartest minds in the world are already turning theory into practice—one breakthrough at a time.

That brings telecommunications providers ever closer to a potentially monumental cybersecurity challenge. The quantum threat looming large over the horizon is that the technology will provide a means to decrypt any data currently protected by public key infrastructure (PKI) cryptography. That means most of the communications currently traversing telco networks. This is the future the industry needs to start planning for today. The financial services sector has already begun—following the lead of government.

It is a challenge not dissimilar to Y2K. Call it: "Y2Q" (Years to Quantum). Yet unlike the countdown to the millennium bug, there is no obvious target date for telcos to build their post-quantum cryptography (QPC) strategies around. We simply don't know how soon functioning quantum computers will start to unmask PKI-encrypted data en masse. In fact, threat actors are likely to be already stealing and storing sensitive PKI-protected data, with a view to decrypting it later (SNDL). That means work should start now on refitting existing security architectures and mitigating risk across legacy networks.

The good news is that a solution already exists to help manage this transition. Arqit offers proven PQC technology which will integrate seamlessly into existing infrastructure to mitigate the quantum threat, in a non-disruptive, cost-effective manner. This might feel like a business problem that can wait for another year, or even another decade. But if Y2K has taught us anything, it's that procrastination will only lead to spiralling costs and fewer options.

History need not repeat itself, if telcos commit to a carefully managed journey to quantum safety. That journey must start today.

Where's the risk for telecoms operators?

1) The quantum threat

PKI is the core technology behind the digital certificates that establish digital identities and secure data and communications in telecoms environments. It uses asymmetric encryption to do so in a variety of scenarios, including code signing, VPNs, secure roaming, over-the-air (OTA) updates, eSIM provisioning, and secure network communication between servers, routers, cell towers and other assets.

However, there are well documented weaknesses and management overheads associated with PKI, which can create additional risk and cost. Certificate-related issues have already led in the past to major network outages, for example.

Over and above these challenges, the algorithms on which asymmetric encryption, or public key cryptography is based, derive their security from mathematical problems. These would take thousands of years for current computers to solve, but potentially just hours for a quantum computer. If so-called "Cryptographically Relevant Quantum Computers" (CRQCs) can be produced, nation states and well-funded cybercrime groups would have the capability to unmask all data and traffic currently protected by PKI.

This represents an existential threat to an operator's business, as it could create multiple risks outlined by the GSMA:

- **Store Now, Decrypt Later (SNDL):** The theft of PKI-encrypted data today with the goal of using CRQC to decrypt it later.
- **Code signing:** Asymmetric encryption algorithms could be cracked to attack service authentication and create vulnerabilities in software updates.
- **Data compromise:** Algorithms used to digitally sign data including call records and contracts could be cracked.
- **Key management attacks:** The asymmetric encryption used to store symmetric keys could be attacked, imperilling the protected data.

The bottom line for telco business leaders is that CRQC could enable mass data breaches and network disruption, causing potentially significant reputational and financial damage including regulatory fines.

"Practical quantum computing, when available to cyber adversaries, will break the security of nearly all modern public-key cryptographic systems."

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

2)5G expands the attack surface

Critical telco customers from healthcare providers to smart city stakeholders increasingly rely on 5G. But the architecture also opens up more avenues for attack. Although overall more secure than 4G, data security in 5G remains a challenge. There are several areas for concern:

- From the smart factory to the power grid, 5G heralds an explosion in Internet of Things (IoT) connected devices and smart sensors. They are often connected to edge computing environments, meaning threat actors can reach them. But their memory is too small to run asymmetric key-based post-quantum algorithms (PQAs)
- 5G networks are increasingly being built with open architectures, which means more third-party vendors and interfaces. This increases the risk of malicious third parties authenticating and connecting to the network
- The virtualization of the network with 5G creates opportunities for network slicing and layering, but also opens up the risk of malicious actors accessing restricted layers if not properly authenticated
- Open RAN is emerging as the standard of choice for wireless communication globally. But there are question marks over its security and resilience. Research has revealed that it does not specify security configurations between various RAN elements, potentially enabling denial of service attacks. Additionally, in an Open RAN ecosystem, third-party vendors provide services on virtualised network services (VNFs) running on open platforms, which could also be abused by malicious users

3)Legacy networks

Although 5G was designed with best practice Zero Trust principles in mind, legacy networks (eg 3G/4G) were not. Their inflexibility creates security risk as traffic profiles change dynamically. Securing the handovers between 5G and legacy networks is therefore critical to ensure malicious actors can't attack 5G assets via less secure networks. Failing to do so would be akin to locking the front and back doors of a house but leaving a window open.

There are also post-quantum security implications to consider in an international roaming scenario, when different carrier networks use the Security Edge Protection Proxy (SEPP).

Why current PQAs are not yet viable

Fortunately, the US government's National Information Technology Laboratory (NIST) is leading international efforts to design PQAs. The less reassuring news is that, by its own admission, this approach is far from perfect. In fact, it warns that such algorithms may be broken in the future, as they derive their security from mathematical processes.

It can be misleading to label these algorithms as "quantum-safe" when they only provide unknown levels of quantum resistance, as powerful attacks can be discovered at any time. AES 256 is often considered to be quantum-safe, due to the theoretical analyses by Zalka that showed Grover's quantum algorithm would not drastically reduce its security. This is in sharp contrast to other cryptographic algorithms like RSA and ECC that would be severely compromised by Shor's quantum algorithm. In just the past 18 months, three of the NIST finalists were surprisingly compromised (without a quantum computer). It is imperative for deployment in operational telecommunications settings to have a defense-in-depth approach so that the entirety of our cryptographic framework is not lost.

Even if PQAs can be designed to withstand the compute power of CRQC, they are likely to be extremely costly, time-consuming and disruptive for telcos to implement. That's partly because the algorithms take longer to process and require more memory and bandwidth to use. According to NIST:

"Updates to protocols, schemes, and infrastructures often must be implemented when introducing new cryptographic algorithms. Consequently, algorithm replacement can be extremely disruptive and often takes decades to complete."

Starting the journey to quantum safety today

There will be essential use cases for these PQAs. However, there is an alternative to PQAs whilst they mature their security proof: symmetric encryption. AES256 is military-grade encryption methodology uses a single key to encrypt and decrypt data, and is faster and more efficient than asymmetric encryption. Most importantly, it has been confirmed by the US and UK governments and GSMA as post-quantum secure.

"In contrast with PKC, the security of symmetric cryptography is not significantly impacted by quantum computers, and with suitable key sizes, existing symmetric algorithms - such as AES - can continue to be used." - National Cyber Security Centre

In fact, such is the US government's confidence in symmetric encryption that a White House National Security Memorandum in May 2022 ordered federal agencies to "implement symmetric-key protections...to provide additional protection for quantum-vulnerable key exchanges" by 31 December 2023.

Standards are everything in telecoms

It is only through the great work of generations of telecoms engineers setting standards and regulations that 5G is able to be interoperable and viable globally. Similarly, standards in security are critical.

Aside from being quantum secure, symmetric encryption has multiple benefits for telecoms providers:

- The technology is available now, and can be introduced with minimal disruption: no rip and replace needed
- It works with existing infrastructure and IPSec/TLS protocols, which are used widely in telecoms environments
- There's minimal risk of it being broken in the future
- It's highly cost effective
- It can be used to secure network slicing and interfaces with third-party vendors
- It can be used to secure handovers between legacy and 5G networks
- It can be used to secure IoT traffic
- It works across public and private 5G networks
- It can be used to secure roaming between SEPPs of different service providers

In acknowledging that that new PQAs brought forward by the global community are not currently fit for purpose, the US Government has helpfully laid down some new standards and requirements.

1. White House memorandum M-23-02 (whitehouse.gov). This provides direction for agencies to comply with National Security Memorandum 10 (NSM-10). It has become a directorate that federal agencies move to zero trust architectures.
2. NIAP's protection profile publication for VPN Gateways now mandates the inclusion of RFC 8784 for approved components under the NSA CSfC authority. IETF RFC 8784, Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2), describes how symmetric keys may be injected into networking appliances like VPNs. As NSA CSfC and NIAP create a demand signal for securing classified data with symmetric keys, this will likely propagate into the commercial realm.
3. NIST and BSI have made recommendations on what they call "hybrid cryptography", together with the use of RFC 9370. This can be brought to life with dynamic symmetric key cryptography in a standards compliant manner which is easily integrated into existing appliances.

How Arqit can help

Arqit's approach to quantum safety is not to reinvent the wheel. It is to use the strongest PQC building blocks available today to deliver a cost-effective and future-proof architecture for telcos. That means utilising proven symmetric encryption technology in a Symmetric Key Agreement platform, whilst adopting a crypto agile approach to working with other PQC methods where fit for purpose.

Arqit's Symmetric Key Agreement platform (SKA) designed to secure the data traversing telco networks — both now and in a post-quantum world. It works with a wide variety of network-connected endpoints using SDKs written in several different languages. This enables secure data-in-transit between two data-centre firewalls (physical or virtual), or between a user device (e.g. a laptop) and a cloud service. It's also lightweight enough to deploy across IoT devices communicating with a base station.

The quantum-safe encryption keys can be used on top of existing infrastructure like PKI and work with popular existing protocols like TLS and IPsec to enhance their security. Key rotation is handled by Arqit, removing a significant security and management burden for customers. The security proofs for the design aspects of the key-establishment protocols used to enable symmetric key agreement over classical IP network infrastructures were independently assured in 2022 by the Surrey Centre for Cyber Security, at the University of Surrey in the United Kingdom.

Arqit was recently able to make a public announcement which confirms that the Symmetric Key Agreement Platform invented and patented by Arqit complies with the NSA Commercial Solutions for Classified Symmetric Key Management standard:

Arqit SKA adopts a zero-trust approach for enhanced security, so that devices must always authenticate before using any of its services. It uses strong authentication that is invulnerable to attack by quantum computers, and doesn't rely on public/private certificates which are difficult to manage and deploy at scale. Customers gain full control over their network, deciding which devices have access and which don't.

Telecoms operators could use Arqit SKA across:

- Cloud-native networks
- Metro access networks
- Enterprise and telecommunications data centre networks
- Software-defined wide area networks
- Last-mile fibre broadband networks
- 5G and open radio access networks

The technology continues to be tested and validated to the highest standards:

DCMS FRANC (Future RAN Competition):

- As far back as January 2022, Arqit was selected by the UK government's Department for Digital, Culture, Media and Sports (DCMS) to develop a secure wideband solution for 5G Open RAN platforms.

DCMS Trials and Testbeds Programme:

- In May 2022, Arqit and Blue Mesh Solutions successfully completed and demonstrated a quantum secure MQTT (MQ Telemetry Transport) service for Industrial IoT. The project highlighted the ease with which SKA can be integrated into existing protocols and systems to make them quantum safe.

DSIT and ARIANE:

- Project ARIANE (Accelerating RAN Intelligence Across Network Ecosystems) won UK government funding from the Department of Science Innovation & Technology (DSIT) Open Networks Ecosystem (ONE) competition. Arqit is teaming up with nine partners including TIP, Accenture, BT, VMware, Amdocs, HCL, Reply and Viavi. Their ARIANE initiative hopes to accelerate real-world Open RAN deployments.

Ampliphae and HPE Athonet Collaboration:

- Arqit teamed up with cybersecurity vendor Ampliphae and HPE Athonet to successfully complete a project designed to deliver quantum-safe security for Private 5G networks. Arqit's SKA platform was integrated with Ampliphae's network security analytics on an HPE Athonet RAN to mitigate QRQC-related risk in a hugely important use case. Private 5G networks are already rolling out across sectors as diverse as manufacturing, healthcare, defence and smart cities.

GSMA Intelligence: The 2024 Business Dynamics to Watch

In our introduction, we positioned post-quantum security as an “existential” concern for operators that crosses nearly all aspects of their network / service estates and needs to be planned for in the near-term. Two statements from the white paper that followed help to capture this very well.

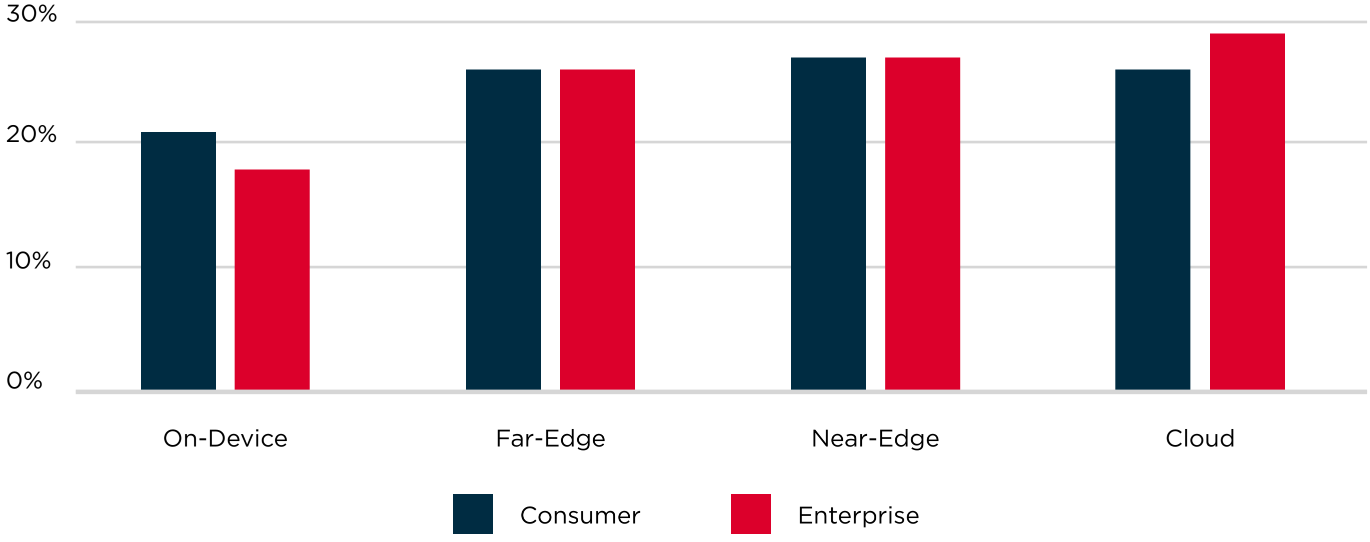
“The quantum threat looming large over the horizon is that the technology will provide a means to decrypt any data currently protected by public key infrastructure (PKI) cryptography. **That means most of the communications currently traversing telco networks.”**

“There is no obvious target date for telcos to build their post-quantum cryptography (QPC) strategies around. **We simply don’t know how soon functioning quantum computers will start to unmask PKI-encrypted data en masse.”**

As we move further into 2024, there are various reasons to expect that the need for post-quantum strategies will only grow. Most obviously, there is the simple reality that quantum computing R&D and innovations will continue apace; as they do so, the window will close on any preparation time available to operators. Beyond that basic reality, however, a number of 2024 market trends and aspirations all conspire to raise the profile of keeping mobile networks and secure.

- **B2B Expansion and Vertical Demands.** From the earliest days of the 5G Era, it was acknowledged that sales into the enterprise vertical would be the main 5G revenue upside for operators. Monetizing 5G via vertical sales remains a work in progress for most operators but requires a solid security message given the business-critical nature of connectivity for many businesses combined with data privacy requirements.
- **IoT Innovation.** Enterprise 5G is about more than just equipping workers with new smartphones. It’s about connecting “things” with the speeds, latencies, quality, and price points required to meet vertical-specific demands and business cases. 5G IoT evolutions including RedCap and passive IoT will begin getting attention this year. As they drive IoT growth, the attack surface for 5G networks and services will only expand.
- **Open Networks**. Noted earlier, Open RAN is high on operator technology agendas in 2024, but also comes with potential security risks. What we didn’t mention is that one of the most frequently cited obstacles to Open RAN deployment is “uncertain internal ownership.” Where roles and responsibilities around technology ownership are unclear -seemingly the case in many Open RAN rollouts – security may well slip through the cracks.
- **Multi-Cloud Edge and Core.** Operators have been moving workloads to, and delivering services from, the cloud for some time. New use cases such as Generative AI may accelerate adoption, but will also highlight that multi-cloud, multi-location thinking is key in order to meet application demands. As traffic traverses diverse clouds (and, potentially, diverse suppliers) new threat vectors will need to be recognized and secured.
- **5G-Advanced and 6G.** While the timeline for 6G commercialization is far from clear, 5G-Advanced specifications will be complete this year with deployments planned not long after. Positioned as an evolution of today’s 5G, 5G-Advanced is poised to amplify much of what operators already have planned for 2024 (with associated security implications): more B2B, IoT, and cloud while serving as a trigger to investigate new (open) network architectures.

Where is data processed in telco networks?



Conclusion

Taking the first steps today

Telecoms operators can't be sure exactly when fully functioning CRQC will start to appear. But as providers of critical national infrastructure, nor can they afford to ignore the prospect that this will one day happen — undermining the security on which their networks have for years depended. Instead, they must assume SNDL is happening right now, and plan for the future.

Given that PQAs involve significant cost, complexity and disruption—and the threat of being broken at some undetermined point in the future—the focus for industry should be on symmetric encryption. Workable solutions like Arqit SKA exist today to help telcos begin a measured, confident journey to quantum safety. The benefits are potentially enormous.

Five steps to quantum safety

To get there, consider the following:

1. Ask your vendors what they're doing to achieve quantum safety (interfaces, protocols, encryption use and type of data)
2. Monitor what they're doing to understand where you can harden the interfaces
3. Invest in a quantum-safe solutions leveraging crypto agility including symmetric encryption
4. Set policy to mitigate the quantum threat
5. Conduct continuous reporting and ongoing compliance monitoring

ARQIT

Arqit Quantum Inc. (Nasdaq: ARQQ, ARQQW) (Arqit) supplies a unique encryption Platform as a Service which makes the communications links of any networked device, cloud machine or data at rest secure against both current and future forms of attack on encryption – even from a quantum computer.

Compliant with NSA standards, Arqit's Symmetric Key Agreement Platform delivers a lightweight software agent that allows devices to create encryption keys locally in partnership with any number of other devices. The keys are computationally secure and operate over zero trust networks. It can create limitless volumes of keys with any group size and refresh rate and can regulate the secure entrance and exit of a device in a group. The agent is lightweight and will thus run on the smallest of end point devices.

The Product sits within a growing portfolio of granted patents. It also works in a standards compliant manner which does not oblige customers to make a disruptive rip and replace of their technology.

Recognised for groundbreaking innovation at the Institution of Engineering and Technology awards in 2023, Arqit has also won the Innovation in Cyber Award at the National Cyber Awards and Cyber Security Software Company of the Year Award at the Cyber Security Awards. Arqit is ISO 27001 Standard certified.

Find out more at www.arqit.uk

MOBILE WORLD LIVE

Mobile World Live is the premier destination for news, insight and intelligence for the global mobile industry. Armed with a dedicated team of experienced reporters from around the world, we are the industry's most trusted media outlet for breaking news, special features, investigative reporting, and expert analysis of today's biggest stories.

We are firmly committed to delivering accurate, quality journalism to our readers through news articles, video broadcasts, live and digital events, and more. Our engaged audience of mobile, tech and telecom professionals, including C-suite executives, business decision makers and influencers depend on the unrivalled content and analysis Mobile World Live provides to make informed business decisions every day.

Since 2016, Mobile World Live has also had a team of in-house media and marketing experts who work directly with our brand partners to produce bespoke content and deliver it to our audience in strategic yet innovative ways. Our portfolio of custom work - including whitepapers, webinars, live studio interviews, case studies, industry surveys and more – leverage the same level of industry knowledge and perspective that propels our newsroom.

Mobile World Live is published by, but editorially independent from, the GSMA, producing Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and home to GSMA event keynote presentations.

Find out more at www.mobileworldlive.com

Disclaimer: The views and opinions expressed in this report are those of the authors and do not necessarily reflect the official policy or position of the GSMA or its subsidiaries.