techUK Quantum Security Working Group

Workshop: Cybersecurity in a quantum world: Preparing for the new cyber age

techUK recently held a roundtable exploring cyber resilience for a quantum age. This discussion brought together the UK's cyber security ecosystem and the emerging quantum industry to explore how the UK can prepare for a quantum-secure future, and how to raise awareness around this once-in-a-generation transformation of cybersecurity.

The first meeting consisted of a workshop entitled *'Cybersecurity in a quantum world: Preparing for the new cyber age'*. Attendees focused on 5-key questions:

1. What current work is currently underway to prepare for the quantum secure transition?
2. Where does quantum fit into the UK's National Cyber Strategy, ensuring that the UK remains confident, capable and resilient to new cyber threats?
3. What solutions are available, and how will they integrate into current cyber infrastructure?
4. What can businesses do now to mitigate future Quantum Risk?
5. How can the UK lead in quantum security, building upon its thriving cyber ecosystem and developing best practice?

This session was the beginning of a wider conversation within techUK membership around the development of a Quantum Security Working Group. With member support techUK will advocate for a greater focus on cyber resilience in the UK as a route to strengthening public-private partnership around quantum security. If joining this group is of interest, please register your interest now.

Speaking during the workshop included:

- **Chris Parker**, Director, Government (Cybersecurity), Fortinet (CHAIR)
- **Steve Beeching**, SVP Government Relations, Arqit
- **Zygmunt A Lozinski**, Global Industries Senior Technical Staff Member and Quantum Ambassador, IBM
- **Annika Moslein**, Technical Project Manager, Quantum Dice

Key areas for discussion included:

Opportunity for the UK

Attendees and speakers discussed the ongoing innovation in this space, emphasising the exciting quantum compute applications that are emerging across sectors, including climate change, fossil fuels, new elements being discovery, alongside the new technology focused careers this will unlock. Such advancements will have a profound and positive impact in the UK and critical to achieving the UK's ambition to become a science and technology superpower.

There was also recognition across the discussion that, overall, the UK is in a strong place to realise these applications, being quick off the mark with the establishment of the National Quantum Technologies Programme (NQTP) in 2014.

This world-pioneering programme has already delivered £1bn investment across quantum technologies; and it will be instrumental in investing the £2.5bn to secure the UK as a world leading quantum-enabled economy by 2033 as set by the National Quantum Strategy.

Crucially, this programme has supported the early-stage development of different quantum technologies through the four technology hubs. This has ensured a diverse and thriving quantum ecosystem in the UK and has set the groundwork for different pathways to commercial success in the UK. Equally, the creation of the National Quantum Computing Centre (NQCC) to provide access, resources, and partnerships for the quantum industry will further push forward the quantum innovation ecosystem. At the time of its announcement, this was regarded as a novel and innovative project that would begin the long road to democratising access to Quantum Compute and harbour commercialisation when quantum compute moves from its current research stage and towards fault tolerance.

While recognising this strength, members cautioned about over-hype in this area, with quantum compute being further from market deployment than other quantum technologies due to significant science and technology challenges in qubit scaling. This is giving much needed time to address quantum resilience as application can be timely and costly for businesses and governments. Resilience of these technologies should become a huge focus in cyber, both for industry and Government.

Though appreciating the strength of the UK Quantum Programme, there was also concern expressed across the group that there seems to be no clear direction from Government – from either the NCSC or from within the recent National Quantum Strategy – that will push forward the UK as a leader in quantum cyber resilience. The Strategy emphasises guidance from the National Cyber Security Centre (NCSC) to help businesses put in place protective digital and physical security measures to ensure the protection of assets which are necessary to support growth, but there has not been any updated guidance from the NCSC since 2020. In this evolving field it is imperative that businesses start to develop quantum resiliency and further guidance from Government is needed. this lacks leadership, interest and engagement could ultimately hinder the UK's status as a pioneer in quantum.

Key Challenges

Alongside this, members agreed that some of the most pressing challenges were:

- Ongoing digital skills deficits
- Awareness and understanding of quantum and what this will mean for cyber resilience.
- Cost to implement.
- Cost of R&D (particularly in comparison to other technologies)
- Engagement between UK Government and Industry

It was also agreed that one area a potential working group could play a useful role explaining the different challenges and stages of Quantum Resilience, mythbusting some of the common misconceptions around the technologies and application, particularly around key management and encryption.

International Competitiveness

Three elements were discussed in terms of international competitiveness:

1. The UK is second behind the US on having a number of quantum companies, so is seeing real success in this arena;
2. There are synergies between the National Cyber Strategy and Quantum Strategy – for example Pillars 3 and 5.

3. Quantum is an area of significant global competition between US and China – concern around potential future state nation sponsored attacks in this space.

UK Government Role

Attendees were very supportive of the UK Government's broader National Quantum Strategy – and the associated £2.5bn in funding over the next decade – particularly highlighting the success of Government coordination in other sectors such as cyber security. However, this strategy, at times, is unclear on application. Therefore, key challenge became how to implement recommendations on cyber resilience in time.

Members stressed that the primary role of Government is always National Security – and argued that the strategy should represent the starting point for clearer guidance and engagement between UK Government and industry on the resilience of quantum technologies. Identifying roles and responsibilities in this space should be a key priority.

Some members argued that the current NCSC guidance is quite vague in this space, and that we are starting to see this gap being filled by individual firms in the UK or internationally by the stronger direction being issued by US CISA on Quantum Safety. This was also true for standards development, and it was discussed that any potential working group should look to stay engaged with work happening domestically and internationally, as this forms part of technology readiness levels needed for commercialisation.

Need for building awareness/Mythbusting

Members highlighted that one of the initial actions on this working group should be to give clarity to the wider technology community on how quantum compute can break encryption **but** there are solutions available to address this.

This would form part of a wider discussion around how to develop the right skills in the UK, particularly within the existing cyber community, to push forward quantum resilience.

Attendees agreed that the WG would focus the groups future activity on three key areas and actions:

1. techUK to set up Quantum Security Working Group
2. techUK to develop short explainer/guidance on Quantum Security for wider audience, focusing on mythbusting and awareness raising.
3. techUK to map key stakeholders from UK Government Departments, NCSC and NPSA to engage and explore using WG as a route to strengthening public-private partnership around quantum security.
4. techUK to engage directly with NCSC to explore their plans on this topic and to invite them to brief members on a regular basis for two-way exchange.
5. Finally, the WG will look to map its activity and actions to the aims and objectives of both the National Cyber Strategy and National Quantum Strategy.

-