DiTech Topic 3

**TQO THE IMPACT OF QUANTUM COMPUTING TECHNOLOGIES ON CYBERSECURITY – BREIFING**

*Welcome to PHSMUN DiTech!*

*Resolutions for the topics (especially those that interest you!) are appreciated and should be submitted by any delegate hoping to be in the running for a prize - a digital and paper copy is preferable.*

*Position papers (max: 100 words) can be submitted if you like but aren’t mandatory by any means.*

*Both resolutions and any position papers can be submitted to either* *cosmological.constant1052@gmail.com* *or* *gw13radkowskialex@glow.sch.uk* *.*

*Resolutions will be chosen on the day based on a combination of signatures gained after lobbying and which we feel will lead to the most engaging debate.*

*Notes for writing resolutions:*

* *It doesn’t need to be perfect/ as long as possible – the best resolutions offer a strong starting point with interesting things to build upon during the debate.*
* *Focus on writing strong operative clauses – preamble makes you sound good, but is mostly decorative at the end of the day.*
* *We can’t stop you using AI, but we do discourage it – writing a resolution can be one of the most fun and creative parts of debating, as well as a good way to gain a thorough understanding of your topic even if your resolution isn’t chosen. Also, when you don’t know what your own resolution is talking about, it's very obvious 😉*
* *Look at the Rules and Info page on the website for more information and support on writing and reading resolutions, as well as other things.*
* *Don’t be afraid to email us any time you have questions about the topics or process – it's what we’re here for!*

*We hope to see you here soon :)*

 *- Chairs (Cara and Alex)*



What is a Quantum Computer?

 A quantum computer is similar to a classical computer, however it uses quantum mechanical phenomena (the strange physics of very small things) to improve efficiency and capability in carrying out complex calculations and tasks.

The concept of applying quantum mechanics to computing emerged in the 1980s, and increasing research is being done investigating ways making the technology functional in the real world. A classical computer uses a basic unit called binary bit to convey information – a switch which can represent either a value of 1 or 0, enabling various calculations to be carried out and data to be stored. A quantum computer uses qubits, which are essentially bits which operate in a state such that quantum mechanical effects are significant. This allows them to do many strange and useful things, such as exist in a superposition of multiple states (both the 1 state and the 0 state), with varying probabilities of collapsing into a state of 1 or 0 upon being observed.

These odd properties allow for quantum computers to solve problems and process certain information significantly faster and exponentially more efficiently than classical computers. The rapid development of quantum computing in recent years could allow them to revolutionise the world, finding breakthroughs in various fields and compute problems which are impossible for classical computers (within a reasonable timeframe.)

How Does This Affect/Threaten Cybersecurity?

Current digital cryptography (how information is hidden/encrypted) relies on mathematical models which garble data using a large number in such a way that it becomes unreadable to others unless they have the mathematical key to decode it. This key requires knowing the prime factorisation of the number. The process of finding prime factorisations of sufficiently large numbers with classical computers takes many many years, making it unfeasible to crack these codes in almost all current circumstances (look at links if interested).

A quantum computer poses a threat here as the nature of quantum effects mean that quantum computers can carry out far more calculations simultaneously, and therefore decrypt these codes much more quickly. (For some highly nerdy specifics of a way this can be done, see Shor’s Algorithm.) This means that if a functional quantum computer of a large enough capacity can be built, it could effectively undermine the security of almost all encrypted data worldwide.

What is Happening Right Now?

While the field of quantum computing has grown rapidly in the past few years, the current viable models are not nearly powerful enough to break or pose a threat to current encryption, so it’s predicted to be years still before quantum computers can be reliably applied to solving major problems.

However, experts believe it is essential to start thinking about quantum computing dangers early, to prevent disaster if we reach the point where all encryption is compromised. Quantum-resistant cryptography is already being developed by independent organisations and government agencies, all with varying standards.

The UN has started to recognise the threat quantum computing can pose and even declared 2025 as the Year of Quantum Science and Technology (along with a few other things), so it is time now for a resolution to be passed to efficiently decide how to address this coming threat, and to what extent the UN should be involved.

Things to consider:

* What is your nation’s attitude to and investment in quantum computing?
* What inequalities could this create between more and less developed countries? What is your country’s stance on this likely to be?
* Are there ways we could use this technology to strengthen cybersecurity, rather than threaten it?
* How do we safeguard our current systems against quantum upheaval, given that we do not yet have access to such technologies (or anything equivalently powerful)?
* What should we do in the event of a cybersecurity emergency?
* Do we need regulations in place around the development of quantum technologies? What ethical questions does this raise in terms of scientific and national freedoms?

Useful links:

* <https://www.btq.com/blog/quantum-computing-a-timeline>
* <https://www.unesco.org/en/years/quantum-science-technology>
* <https://uknqt.ukri.org/wp-content/uploads/2021/10/Quantum-Safe-Secure-Communications.pdf>
* <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-qubit#:~:text=Qubit%20explained,%2C%20smart%20materials%2C%20and%20beyond.>
* <https://youtu.be/JhHMJCUmq28?si=asbS0_2JFgbQrv0g>
* <https://youtu.be/RQWpF2Gb-gU?si=Esz4vQDhC3llymBI>
* <https://youtu.be/-UrdExQW0cs?si=BSeG4683GhRMU8fM>