The Daily Telegraph

Tuesday 1 June 2021 *The Daily Telegraph*

Business

How to stop hackers making a quantum leap

British start-up Arqit plans to use satellites to build networks with keys that even computers thinking in qubits can't crack.

By *Matthew Field*

Arqit will beam signals down from a network of low earth orbit satellites, generating keys that can be used by smartphones. Below left, founder and chairman, David Williams

The world's top spies are working on the assumption that their most secure encryption techniques are already compromised.

A new kind of threat is emerging to the security of the internet. Technology used to encode messages since the 1970s is about to be broken, potentially opening up state secrets to nation-state hackers.

The fact that the type of powerful computers – fully operational quantum computers – needed to achieve such a hacking attack do not even exist yet is not a problem. They may be five or 10 years away, but any coded messages intercepted now, while unreadable today, could be decrypted by the first nation-state to crack the quantum computer conundrum.

This has sent governments and spies at GCHQ in Cheltenham racing to build a new kind of encryption, quantum safe encryption, to resist this existential challenge. And one British company believes it has the answer.

Founded in 2017, Arqit was until last month almost entirely unknown outside of a handful of security experts. But a fortnight ago, the London-headquartered start-up managed to attract a $1.4bn (£990m) valuation in a listing on Nasdaq through a merger with a "blank cheque" company.

Arqit's team includes a roster of former GCHQ coders and British and US military officials. They are planning to build a communications network using satellites, data centres and a kind of quantum cloud computer that could create a newly secure internet backbone.

"The whole system is very, very radical," says David Williams, Arqit's chairman. "It is unlike anything the world has seen before and it is patented here in the UK."

The 52-year-old former chief executive of Avanti says existing "public key encryption" was not built for the modern world. "It is crumbling. It is not protecting us against the Colonial pipeline cyber attack or the SolarWinds attack."

Nearly all communications on the web rely on algorithms that scramble messages by multiplying prime numbers together. To crack the code, a computer will need to work out both the original prime numbers. Figuring this out for a number hundreds of digits long would take millions of years.

But such maths is trivial for the quantum computers planned by the likes of Google and IBM and researchers in the US, Britain and China. Rather than working out problems using ones and zeros, they use quantum bits known as "qubits". These can be one, zero or both simultaneously, making them millions of times better at crunching numbers than an ordinary computer. Britain has invested £1bn in the quantum race.

There are real fears China is already ahead. It claims to have reached the level of "quantum supremacy", meaning its computers can now outperform traditional machines.

Being hacked by a quantum computer is not just a problem for spooks in GCHQ. Roger McKinlay, the director of the UK's Quantum Technologies Challenge, says: "This has serious implications for the safe and secure running of critical national infrastructure. But also for us as individuals, with our online lives, including bank accounts, potentially vulnerable in the future."

Quantum computers are not yet ready to unleash hacking campaigns. The quantum computers that do exist suffer from inaccuracies and engineering challenges. However, more powerful models are coming.

Ian Levy, the technical director at GCHQ's National Cyber Security Centre, warned in November: "A quantum computer will allow the attacker to read information that has been encrypted in the past, and forge information in the future."

Creating encrypted signals that can resist a quantum attack is possible, but in practice difficult to implement.

The simplest way is to create a long, random number. Even a quantum computer cannot guess a totally random number thousands of digits long. If two people know this random number, they can send each other messages. This is known as "symmetric" encryption. The problem is distributing these numbers, without risking interception, beyond hand delivering them.

Another way is to use the quantum properties of light or subatomic particles to create a code that cannot be intercepted. In basic terms, if a hacker tries to intercept such a signal, they instantly alter the message and make it unreadable. This is known as quantum key distribution.

BT and Toshiba have installed a 6km quantum fibre network in Bristol using this method at a centre for advanced materials research. But it has limits: the signals degrade quickly over distance and are not easy to scale up.

Arqit claims it has created a system that uses a little of both methods to create a so-called "quantum safe" network. "Everyone I spoke to told me it was impossible, but we found a way to do it," Williams says. Using a network of low-earth orbit satellites, Arqit will beam down a quantum signal to ground receivers at data centres, creating a "quantum cloud" to generate infinite random numbers that can be used by regular smartphones.

Williams explains: "On day one, when you get your phone, you will have a piece of software installed. This allows you to have a secure communications channel using a symmetric encryption key, which cannot be broken by the quantum computer, shared with the quantum cloud."

This "quantum cloud" network can then match up different devices to talk to one another, in theory creating a network secure against quantum computers.

The claims have piqued the interest of cyber security experts, although Arqit has much to prove. It has kept its proprietary systems under wraps.

"I'd wait to reserve judgment on the specifics of things such as their new protocol," says Alan Woodward, a cyber security expert at the University of Surrey.

He is an "enthusiast, but a sceptic" of using quantum key distribution. "I think it is a clever idea, but there are a number of implementation issues under the hood that are open to question," Woodward says.

Arqit's solution is novel, but still needs development. The company plans to launch a pair of its quantum communications satellites by 2023. Its first customers include BT, which will be its exclusive UK reseller. It is also working with Virgin Orbit and Japan's Sumitomo to sell its technology to the Japanese government.

It plans to hire 2,000 people in the UK following the $400m investment from listing on Nasdaq through a deal with asset manager Centricus. Arqit's listing will also produce a tidy return for the British Government, which holds a small equity stake through its start-up rescue vehicle, the Future Fund.

The Daily Telegraph can also reveal the company has won a US contract with defence contractor Northrop Grumman. If Arqit's technology proves its worth, it could create a vital encrypted network for the Five Eyes Nations and its allies.

Arqit is far from alone in this race to build a quantum secure network. Dozens of start-ups and researchers are taking part in a challenge, launched in 2016, by the US National Institute of Standards and Technology to create new algorithms that can survive quantum hacking.

But if Williams is right, his technology could one day carry both sensitive government communiqués and your humble WhatsApps. It is nothing short of ambitious. "We are now hyper scaling the business from Britain," he says. "I believe this can be Britain's biggest tech start-up."