Stuart Poole-Robb CEO
info@kcsgroup.com
KCS Group Europe

No solace in this quantum: The development of the Jinan network in China

Stuart Poole-Robb, CEO of KCS Group Europe, a leading provider of security and intelligence services, shares his views on the development of quantum cryptography in China and explains that despite the theoretically 'unhackable' nature of the new communications network being developed, which is based on the principles of quantum cryptography, human fallibility will always be a threat to cyber security however advanced the march of technology.

In parallel with the rise of cyber technology, from the Colossus of the Second World War to China's Tianhe-2 computer of today (the most advanced ever), it is possible to trace the rise of cyber crime from its infancy to the developed, insidious methods we have today. No longer do we hear sad tales of the Nigerian astronaut stranded on the International Space Station, who just needs three million dollars to come home. Nor, really, do we see brute force attacks on the same scale as the past. Instead, we have an increase in the application of social engineering to both scope and exploit just one potential victim, as opposed to many thousands (but with a much greater degree of veracity to make the scam seem real), and backdoor efforts that induce the victims to exploit themselves - as with the 'email attachment' ransomware that formed the bedrock of the recent NHS attacks.

This is an evolution in tactics which is gradually being taken seriously by companies and governments, and represents the 'third stage' of cyber security. First there came encryption and packets, right at the outset of the internet, securing and breaking down the data so it could not be read if intercepted on the basis that nobody was going to use the internet if it was not private. Then came the hardening of the outer walls with the explosion of anti-virus programs, blacklisting sites and signatures, and so on - the first sign of a 'siege mentality' with the assumption that you could be attacked at any moment. And now, at last, we are in a phase of interior hardening, educating employees on the dangers of social engineering and looking closer at how human fallibility can play into criminals' hands - the understanding that even though your battlements may be secure, there is nothing to stop the enemy trying to tunnel underneath.

Yet for all the evolution in defence strategies, we can only ever at best hope to remain five minutes ahead of the bad actors. There is, after all, no one-size-fits-all, one hundred percent effective protection method, and we need to be lucky every single time - an attacker needs to be lucky only once. Evolution is therefore necessary, but will through no fault of its own ever be enough. Moreover, the human dimension adds a whole new problem. No matter how good security is, at the moment it is only ever as good as the perceptions of those responsible for it - and this is often severely lacking.

In this spirit then, China has recently announced the development of a new communications network based upon the principles of quantum cryptography which, theoretically, is 'unhackable' - at least in the manner of transmission. Quantum key distribution (conducted prior to the sending of the message itself) is conducted through particles of light. Attempted interception will always disrupt, alter or destroy the key in the particles and alert the sender and receiver both - resulting in the message being discarded. Therefore, an attempt

China has taken the lead in this development through the 'Jinan network,' so named for the city of its application, and is of the stance that anything run through the new quantum network will be unbreakable.

Image: Markus Spiske / Unsplash.com

to intercept will always be obvious. If the criminal is left with something worthless, they will soon realise that their time is better spent elsewhere.

The implications for this as a revolution, rather than evolution, in computer science are immense. If it becomes a literal impossibility to intercept a message - given that, in the quantum world, to observe is to change, thus keeping the original message unbreakable - the hackers will find themselves playing to different rules. New dogs, and new tricks.

China has taken the lead in this development through the 'Jinan network,' so named for the city of its application, and is of the stance that anything run through the new quantum network will be unbreakable. The initial test, which started only last month, will see 200 users in Government, military and financial sectors use the technology in commercial practice. Should it succeed, China intends to roll the system out nationwide. But despite the 'next level' nature of the Jinan system, this is but one plank in China's cyber defence strategy: it has been constructing a supposedly impenetrable computer network since 2014, launched a supposedly unhackable communications satellite in 2016, and has committed to being the pre-eminent AI and cyber power of the world by 2030.

Leading figures in the creation of Jinan have expressed their desire to create both a satellite network and a ground network that could theoretically expand quantum encryption worldwide, and comparative research studies are being carried out across the globe (although none quite as advanced as Jinan, though this is likely to only be a matter of time). Not only could this revolutionise transmission IT security, quantum computing in general could set the stage for a new era of problem solving.

A quantum computer is estimated as being 100 million times faster than a desktop PC - and could theoretically solve algorithms in hours that it would take a standard computer the entire life of the universe to crack. This means that the science is classic dual use technology: it can be used defensively in ensuring compromise free quantum key distribution, and offensively in cracking codes and encryption of terror networks in almost real time (the discussion over privacy is, perhaps, one for another time). All told, this could be the biggest cyber revolution since the invention of the internet itself, and security will by necessity play a major part in this.

Current quantum computing is very much in its infancy. A quantum key message is slow and can only be sent for a distance of 250 miles, making long-range and international communication impossible (a fully quantum satellite would be required to practically expand this further). There is also the somewhat thorny issue of what to do when - and it is when, rather than if - quantum computing can crack every algorithm known to man and 'security' risks become obsolete. But certainly Jinan

continued

represents a tangible, sizeable step in tackling key issues of cyber security.

However, this praise must be met with a caveat. Quantum encryption is currently only in basic, minimal use and is a long way from being the accepted standard. But even if it does become widespread, arguably the problem is only half solved. There is still a very high chance that users will fall victim to the biggest cyber threat of all: complacency.

This attitude manifests itself in a number of ways. Even for something highlighted as 'unhackable,' the resourcefulness of the criminal fraternity is such that it is beyond no estimation that quantum key distribution could never be broken. Certainly it has been known for some time now that criminals could disrupt the detectors on the receiving side, not being able to read it themselves but ensuring that nobody else could either (this could create a whole new version of ransomware - pay up or we'll constantly disrupt your detectors).

Alternatively, if your laser duplicates an encoded photon, which is then stolen while the original is sent as normal, secrecy is lost. Or one of the photons fails to hit a detector, creating the impression that somebody has attempted to intercept the chain... it is clear that this is far from a perfect method of protection.

Likewise, to focus on the imperviousness of the distribution method would be to neglect other methods of intrusion: social engineering or phishing through the 'back door,' so to speak. No system can watch over every weakness all of the time, and quantum key distribution (and the benefits of quantum computing, in general) does absolutely nothing about the human elements. Nobody is going to invest millions in quantum technology if they can still be compromised by human error.

In today's less technologically advanced world, where quantum computing is still largely developmental, the impetus is on users to never accept that they can let their guard down or that cyber security is 'sufficient.' No program of cyber security will ever be sufficient or one hundred percent defensive, for the simple reason that it is an impossible task. Perimeter protection is an entirely different beast to staff education, for instance, and the approaches are likewise dissimilar.

But the attitude must be the same: whatever we have, we can always do more. However well we think we are protected, it only takes one failure to prove that we are not. This is the mindset which needs to become prevalent, but which is still lacking in companies of all sectors and sizes, from the family-led local business to a worldwide legal firm.

The latter are particular low-hanging fruit: dealing not only with client's money but also with their most sensitive secrets, the data a firm holds could be even more valuable than their finances. Said firms are also large, unwieldy beasts and it can be problematic to institute a global policy on matters such as social media, 'bring your own device' and two-factor authentication when individual offices, and countries, may want to set their own rules and to impose will seem draconian.

If (as is often stated) the biggest threat to cyber security is sat between the chair and the desk, and firms are not being proactive in taking this as seriously as they would take the possibility of a brute force hack, the stagnation will only help the criminals. If it is not understood that such measures are not viable methods of attack but also the most likely, this is practically an open goal.

Still, there is the conception that perimeter hardening is sufficient, or that a company does not have anything of value to be stolen (neither of which are ever true). Quantum cryptography, or any such similar advancement which professes to offer a next step up in unimpeachable security, would only increase this sense of the assumption of integrity. This is dangerous. Even when behind the highest castle wall, you should not let down your guard, but constantly be alert and accepting that you are still at risk no matter how protected you think you are.

While unhackable data remains the holy grail of information technology, it is to be welcomed that the Chinese, Americans, Europeans and anyone else following the quantum trail cannot be accused of standing still on what they can do. This is an excellent attitude to adopt and one that should (but regrettably is not yet) seen as standard - the world of cyber defence is like swimming in an ocean full of sharks and to stand still will invite disaster. Already there is talk of 'post-quantum computing' - the evolution of the form after quantum computers have already broken everything currently possible. While any effort to secure data transmissions is to be applauded, one cannot escape the core feeling that efforts are being poured into secure data at the expense of what, for want of a better phrase, we shall characterise as 'unhackable humans.'

You may be able, through the Jinan network, or its mirrors, to send encrypted data in as close to surety of secure encryption as is possible. You may even see a significant decrease in the 'man in the middle' scams which characterise intercepted data today. But what quantum key distribution cannot do is protect a file of sensitive customer details from an intrusion into one's system where no data transfer is required; it cannot stop an employee accidentally (or even purposefully) allowing a ransomware or other virus into the network. This is the warning against putting all the eggs into one basket: it is impractical, unhelpful and fails to take into account the constantly evolving nature of both the threat and the response which must be taken. This is why, ultimately, quantum technology should not be seen as a panacea and should be seen as a warning that no matter how advanced the march of technology, the most crucial element of all - the human factor - cannot be ignored.