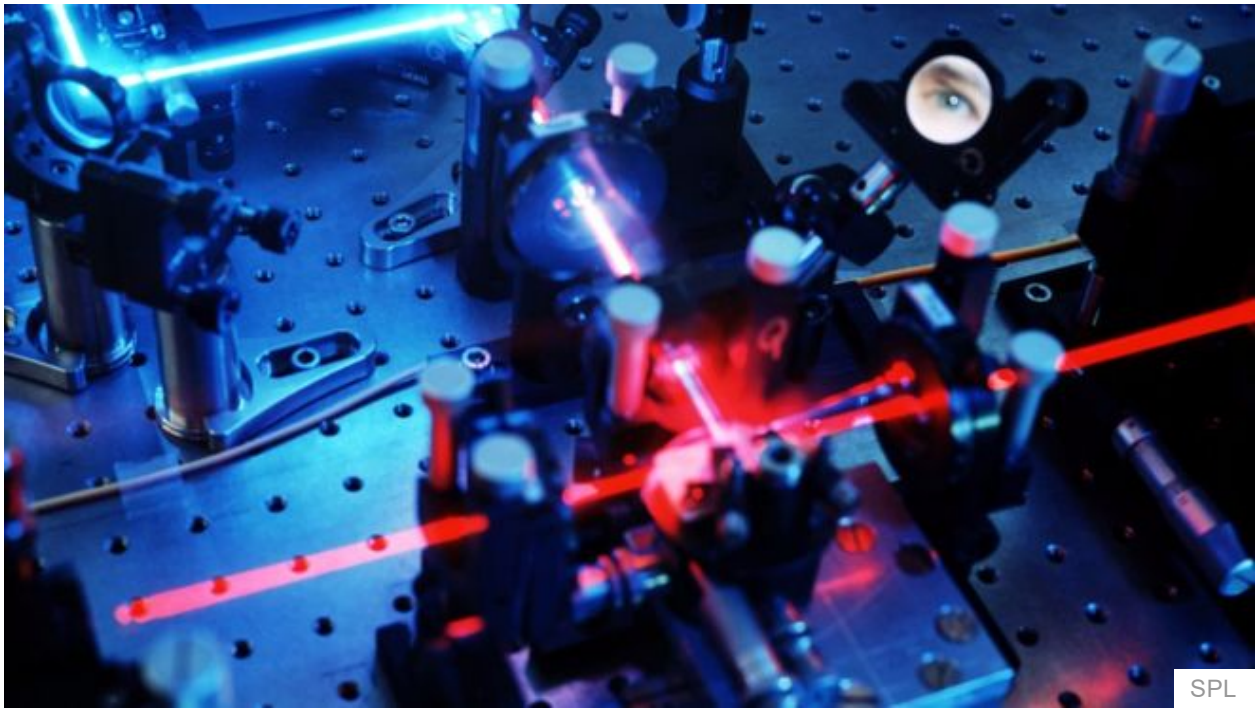
Technology

China set to launch an 'unhackable' internet communication

By Andreas Illmer
BBC News

25 July 2017 | Technology



SPL

As malicious hackers mount ever more sophisticated attacks, China is about to launch a new, "unhackable" communications network - at least in the sense that any attack on it would be quickly detected.

The technology it has turned to is quantum cryptography, a radical break from the traditional encryption methods around. The Chinese project in the city of Jinan has been touted as a milestone by state media.

The pioneering project is also part of a bigger story: China is taking the lead in a technology in which the West has long been hesitant to invest.

In the Jinan network, some 200 users from the military, government, finance and electricity sectors will be able to send messages safe in the knowledge that only they are reading them.

China's push in quantum communication means the country is taking huge strides developing applications that might make the increasingly vulnerable internet more secure. Applications that other countries soon might find themselves buying from China.

So, what is this technology into which the country is pouring massive resources?

'Unhackable' communication

If you send a message you want to keep secure from eavesdroppers, traditional encryption works by hiding the key needed to read the message in a very difficult mathematical problem.

But what is "difficult" in terms of maths? It means you have to think really fast to figure it out as you try endless combinations of long, numeric keys. In 2017, that means you need to use a very powerful computer.

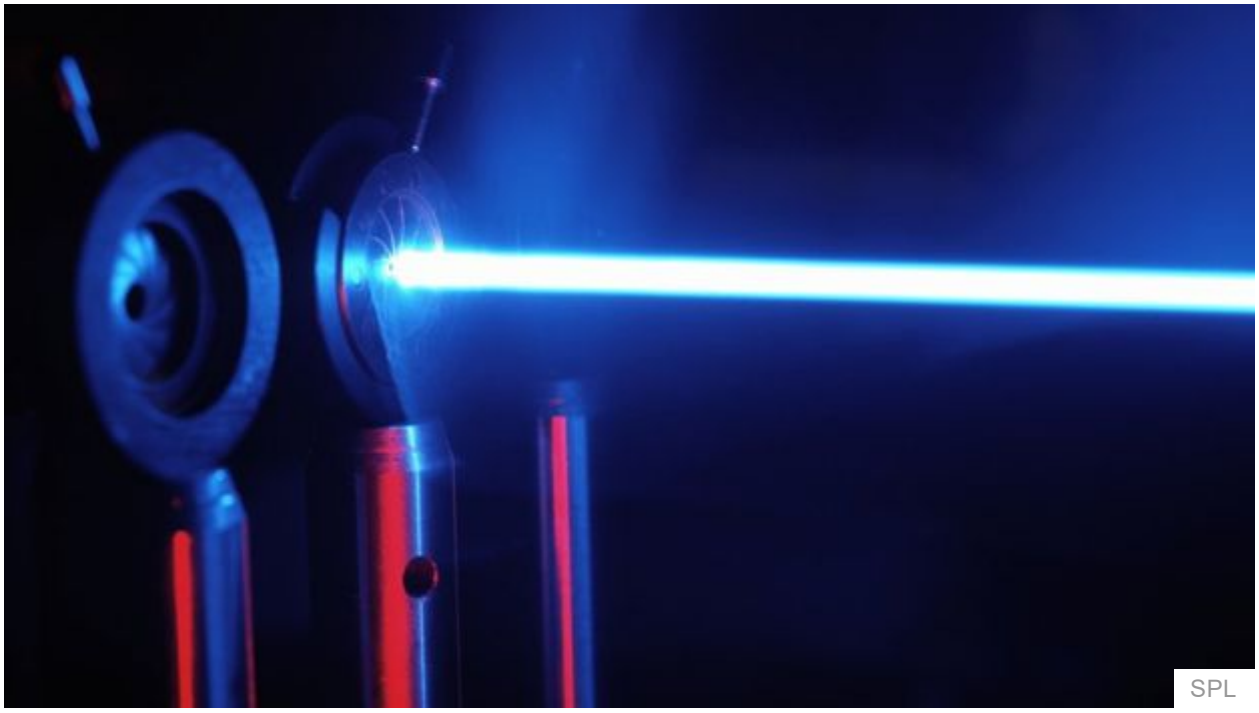
- **Cyber-offenders put through rehab camp**
- **Cash machine hacked in five minutes**
- **Staging security at the National Theatre**
- **The mindset you need to avoid cyber-crime**

Steady improvements in computer power mean that the number-based keys have to be lengthened periodically. Encryption has a shelf life and is rapidly becoming more vulnerable.

There are also fears that the development of quantum computers, which effectively represent a massive step change in number crunching ability, will render much of modern encryption software vulnerable.

Quantum communication works differently:

- If you want to send your secure message, you first separately send a key embedded in particles of light
- Only then doyou send your encrypted message and the receiver will be able to read it with the help of the key sent beforehand



SPL

The crucial advantage of this so-called quantum key distribution is that if anyone tries to intercept the light particles, they necessarily alter or destroy them.

What this means is that any attempt at hacking will immediately be noticed by the original sender and the intended receiver - hence its description as "unhackable".

Leaving the West behind

If quantum communication can help to secure online communications, why is China so far ahead?

"For a long time people simply didn't think it was needed," says Prof Myungshik Kim of Imperial College, London, adding that it was not clear whether there was a commercial market for this technology.

"The mathematical difficulty of the current coding system was so high that it was not thought necessary to implement the new technology," he says.

The research itself is not new and China does not have an edge over the competition. Where it does have an advantage is when it comes to applications.

"Europe has simply missed the boat," says Prof Anton Zeilinger, a quantum physicist at Vienna University in Austria and a pioneer in the field.

He says he tried to convince the EU as early as 2004 to fund more quantum-based projects but it had little effect.

"Europe has been dragging its feet and this has hindered us from being able to compete," he says.

There are quantum key-based networks operating in the US and Europe but most are being carried out as research projects, rather than with commercial partners.

Creating a market

One problem is that it is expensive to build applications like the Jinan network. And if there is not yet a commercial market, it is hard to get investors or governments as backers.

"We have to admit that when China invests into something, they have the financial power and manpower that is beyond probably anything else in the world except the US military," says Valerio Scarani, a physicist with Centre for Quantum Technologies at the National University of Singapore.

The Jinan network is not the only quantum communication application China has developed.

CHINA DAILY/REUTERS

Last year, it **launched a satellite** equipped to test quantum communication over large distances that cannot be bridged by cables. There has also been a link established between the country's two main hubs, Beijing and Shanghai, so both ends can communicate and know when others are listening in.

So while it might not be clear yet whether quantum communication will indeed be the one technology to replace traditional encryption, it is widely considered as one of the leading candidates.

And China, in turn, is the leading country when it comes to building and experimenting with real applications of it.

"It's a situation where the technology can create its market," says Prof Zeilinger.

Once the technology is sold by Chinese companies, international banks might well be the first lining up as customers.

This week BBC News is taking a close look at all aspects of cyber-security. The coverage is timed to coincide with the two biggest shows in the security calendar - Black Hat and Def Con.