Source: *The Straits Times,* pB4
Date: 22 November 2022

Deputy Prime Minister Heng Swee Keat (third from left) with (from left) Toshiba regional managing director Hiroshi Fukuchi; Toshiba Digital Solutions Corporation president and CEO Shunsuke Okada; Japanese Ambassador to Singapore Hiroshi Ishikawa; National Quantum Steering Committee co-chair Quek Gim Pew; and SpeQtral CEO and co-founder Lum Chune Yang, at the opening of the Quantum Networks Experience Centre at the SpeQtral office at one-north last Wednesday. The centre aims to promote the adoption of quantum-secure systems in the region, and is open to strategic partners, including national agencies and private enterprises. ST PHOTO: ALPHONSUS CHERN

Telcos, banks, data centres urged to explore use of quantum security at new centre

Tech industry in race to roll out updated cyber-security software to protect systems

Osmond Chia

Hackers armed with quantum computers may soon trump virtual private networks, decode passwords and break other traditional encryption software that forms the basis of today's Internet security.

And the adoption of new cyber-security software to fend off hackers who could soon wreak havoc with quantum technology is not catching quickly enough.

A newly launched experience centre, dubbed the Quantum Networks Experience Centre, at research and development hub one-north hopes to bridge the gap.

It was launched last week by National University of Singapore's quantum security systems spin-off SpeQtral in partnership with Japanese firm Toshiba. The centre aims to promote the adoption of quantum-secure systems in the region.

It is hoped that national agencies and private enterprises such as telcos, banks and data centres can explore commercial uses for the technology.

The effort is backed by the National Research Foundation, Temasek and national institutions such as Enterprise Singapore and the Economic Development Board.

Standard encryption, which is based on mathematical codes, has become all too familiar to hackers who can decrypt it to access sensitive secrets or cripple networks.

Quantum cryptography, on the other hand, harnesses the quantum properties of light particles to create a seemingly unbreakable cryptographic algorithm to secure satellite or fibre broadband communications.

In the wrong hands, quantum technology can unravel the Internet, as it can potentially crack current encryption algorithms exponentially faster than even the best of non-quantum machines.

National institutions have recognised the promise and potential threat of the nascent technology and doubled down on investments in the field. The authorities and cyber-security providers have also urged businesses to heed these early warnings.

SpeQtral chief executive Lum Chune Yang said: "In terms of general knowledge about quantum communications, it is nowhere near what it needs to be... Any institution that handles high-value data or a high volume of data should take note."

He added: "We are entrusting government agencies, banks and cloud providers with all our data, so those entities handling this data really need to take a close look at securing their platforms. There's not even a price tag to this data."

SOLVES ONE CRITICAL ERROR

Hackers can still exploit errors at the end-to-end points. But, unlike classical encryption, they cannot intercept a signal and decrypt it. So this is not a solve-all solution, but it solves one critical error at least.

MR LUM CHUNE YANG, SpeQtral chief executive, when asked if quantum security is the final word in cyber security. He noted that while there was "no way" to hack a quantum network while data was being transferred, human error could still allow data to be compromised.

On show at the launch is a quantum key distribution (QKD) system – seen by experts as a crucial step towards building an unhackable Internet.

QKD systems exchange secret keys to encrypted data between intended users. Such keys are used to unlock the algorithm securing the data, so that it can be read.

If unauthorised parties or a hacker intercepts the data stream by stealing the key, the intended users will be notified to delete the stolen key, rendering the data unreadable to the hacker.

The system has been successfully deployed between two data centres of network provider SPTel. The centres are 55km apart in Singapore and linked via existing fibre optics networks.

The quantum data transfer is among the first of such trials here and is a test bed for the widespread use of quantum communications across the island.

Toshiba spokesman Hiroaki Tezuka said the trial proves that QKD technology can be seamlessly integrated into telecommunications networks today without disruption, paving the way for mass adoption of quantum communications.

Mr Tezuka, an expert in Toshiba's QKD business unit, said Singapore's small size and robust network infrastructure give it an advantage in deploying quantum systems. "Singapore is a very important market as it can be a showcase to the world of how quantum can be adopted," he said.

Toshiba is in the midst of testing quantum data transfers through longer distances of fibre optics, he added.

SpeQtral will launch a satellite – the SpeQtral 1 – into space by 2024 to facilitate intercontinental quantum key distribution.

This allows encryption keys to be exchanged between Singapore and Europe – a way forward for quantum communications on a global scale.

Quantum computing companies have popped up globally as the race to build a working computer hots up.

IBM, considered a front runner in the field, has plans to release a quantum processor in 2023, and this may see more businesses execute real-world tasks on quantum computers.

Quantum computing's greater processing ability offers new ways to solve issues, such as simulating DNA molecules to help discover new drugs, as well as processing images and software codes to filter misinformation and hate speech.

When asked if quantum security is the final word in cyber security, Mr Lum said while there was "no way" to hack a quantum network while data is being transferred, human error can still allow data to be compromised.

"Hackers can still exploit errors at the end-to-end points. But, unlike classical encryption, they cannot intercept a signal and decrypt it," said Mr Lum. "So this is not a solve-all solution, but it solves one critical error at least."

osmondc@sph.com.sg