

priz<sup>3</sup>m Experienced Team

UK Core 999 system

National Security Systems

Critical National Infrastructure

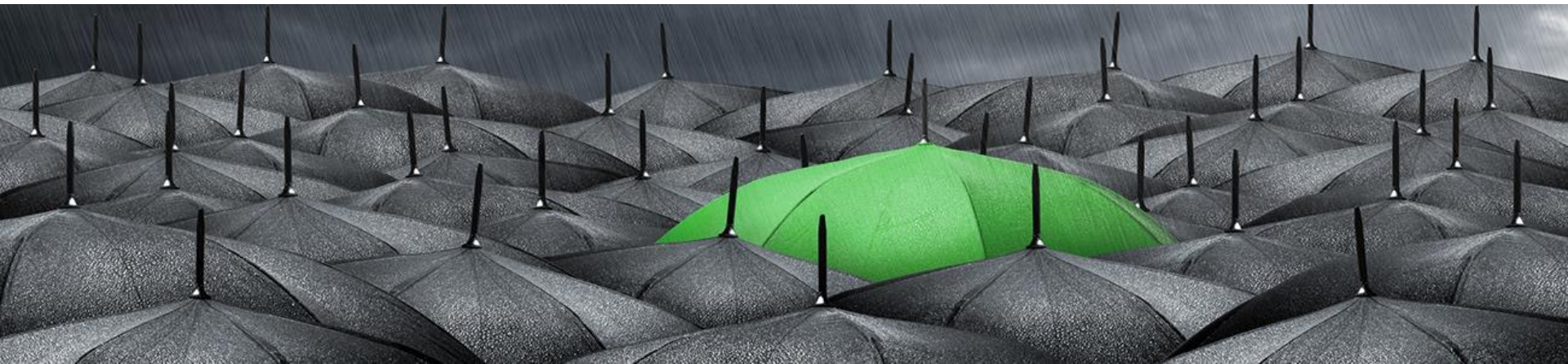
Trusted by:

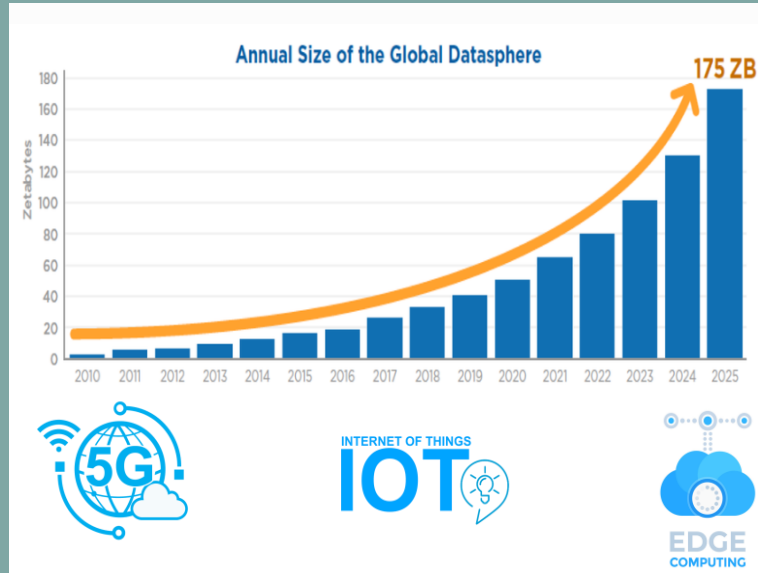


Ministry  
of Defence




ORACLE





60 Billion  
Exposed Files

Data Risk


[CIO](#)
[Hardware](#)
[Microsoft](#)
[Storage](#)
[Innovation](#)
[Apple](#)
[Security](#)
[Newsletters](#)
[Blog](#)
[More](#)
[Edition UK](#)

[MUST READ](#)
[Log4j flaw puts hundreds of millions of devices at risk, says US cybersecurity agency](#)

## Hackers could steal encrypted data now and crack it with quantum computers later, warn analysts

Analysts at Booz Allen Hamilton warn that Chinese espionage efforts could soon focus on encrypted data.

[in](#)
[f](#)
[t](#)
[p](#)

Written by Liam Tung, Contributor on November 30, 2021 | Tech Security

Beijing-backed hackers might soon start trying to steal encrypted data -- such as biometric info, the identities of covert spies, and weapons designs -- with a view to decrypting it with a future quantum computer, according to analysts at US tech consultancy Booz Allen Hamilton (BAH).

**ZDNET RECOMMENDS**

- Best VPN services
- Best security keys
- Best antivirus software
- The fastest VPNs

"In the 2020s, Chinese economic espionage will likely increasingly steal data that could be used to feed quantum simulations," the analysts write in the report *Chinese Threats in the Quantum Era*.

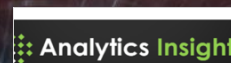
At risk are data protected by the current algorithms underpinning public-key cryptography, which some fear may be rendered useless for protecting data once quantum computers become powerful enough.

**Also: Spy chief's warning: Our foes are now 'pouring money' into quantum computing and AI**

The big question is when such a quantum computer might arrive. However, Booz Allen Hamilton's analysts suggest it doesn't matter that an encryption-breaking quantum computer could be years off because the type of data being targeted would still be valuable. Hence, there's still an incentive for hackers to steal high-value encrypted data.

Recent studies suggest it would take a processor with about 20 million qubits to break the algorithms behind public-key cryptography, which is much larger than the quantum processors that exist today. But a quantum computer that threatens today's algorithms for generating encryption keys could be built by 2030.

# CHINESE THREATS IN THE QUANTUM ERA


[INSIGHTS](#)
[LATEST NEWS](#)
[MAGAZINE](#)
[INDUSTRY](#)

[ABOUT US](#)
[PUBLISH](#)
[CONNECT](#)
[MORE](#)
[SUBSCRIBE](#)

## DANGERS OF QUANTUM HACKING: A THREAT TO ENCRYPTION

LATEST NEWS **QUANTUM COMPUTING**  
by Aratrika Dutta / September 1, 2021

### Quantum hacking is the biggest threat to encryption.

Quantum computers have limitless potentials. There is no doubt that one day quantum computers will find a cure for cancer or help in eliminating world hunger. But along with this, they could also help hackers get access to our most private data by breaking encryption. While quantum computing is beneficial, quantum hacking is dangerous.

#### What is quantum hacking?

To be precise quantum hacking is the use of quantum computers to carry out malicious actions. Quantum hacking is performed by modern cryptographic strategies which often use private and public keys to encrypt and decrypt data through a mathematical equation. These mathematical equations can be easily broken by advanced quantum computers. It would surely take a while, but the process is still possible using the nonlinear protocol of quantum computing.

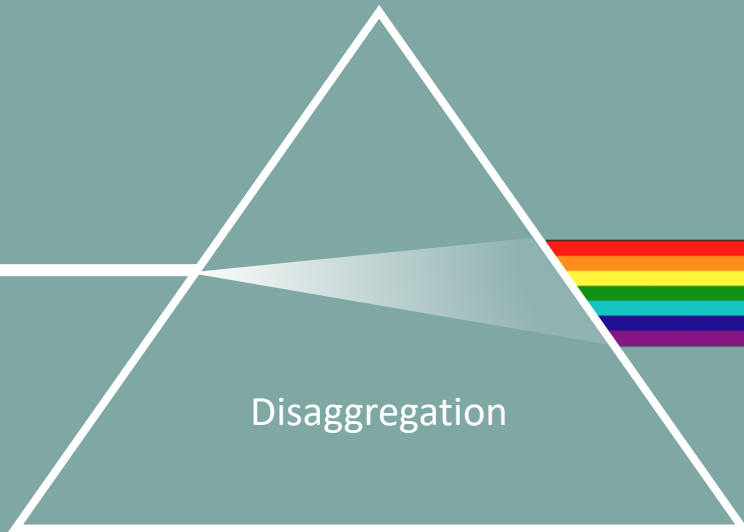
When quantum hacking becomes possible, a system that repairs the existing internet security practices needs to be developed. If not, it would be easy for hackers to break through data and cause costly issues.

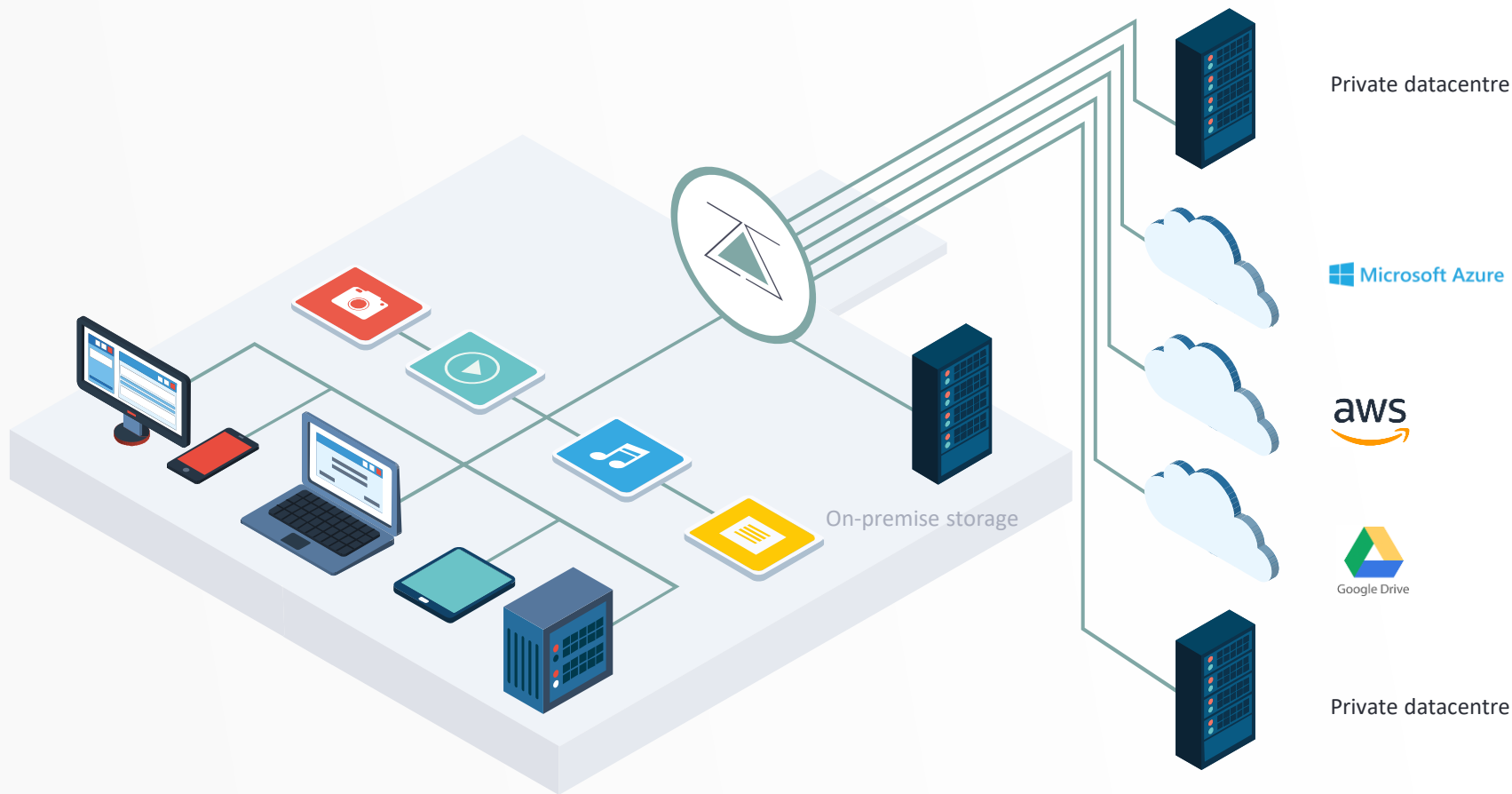
# Quantum Risk

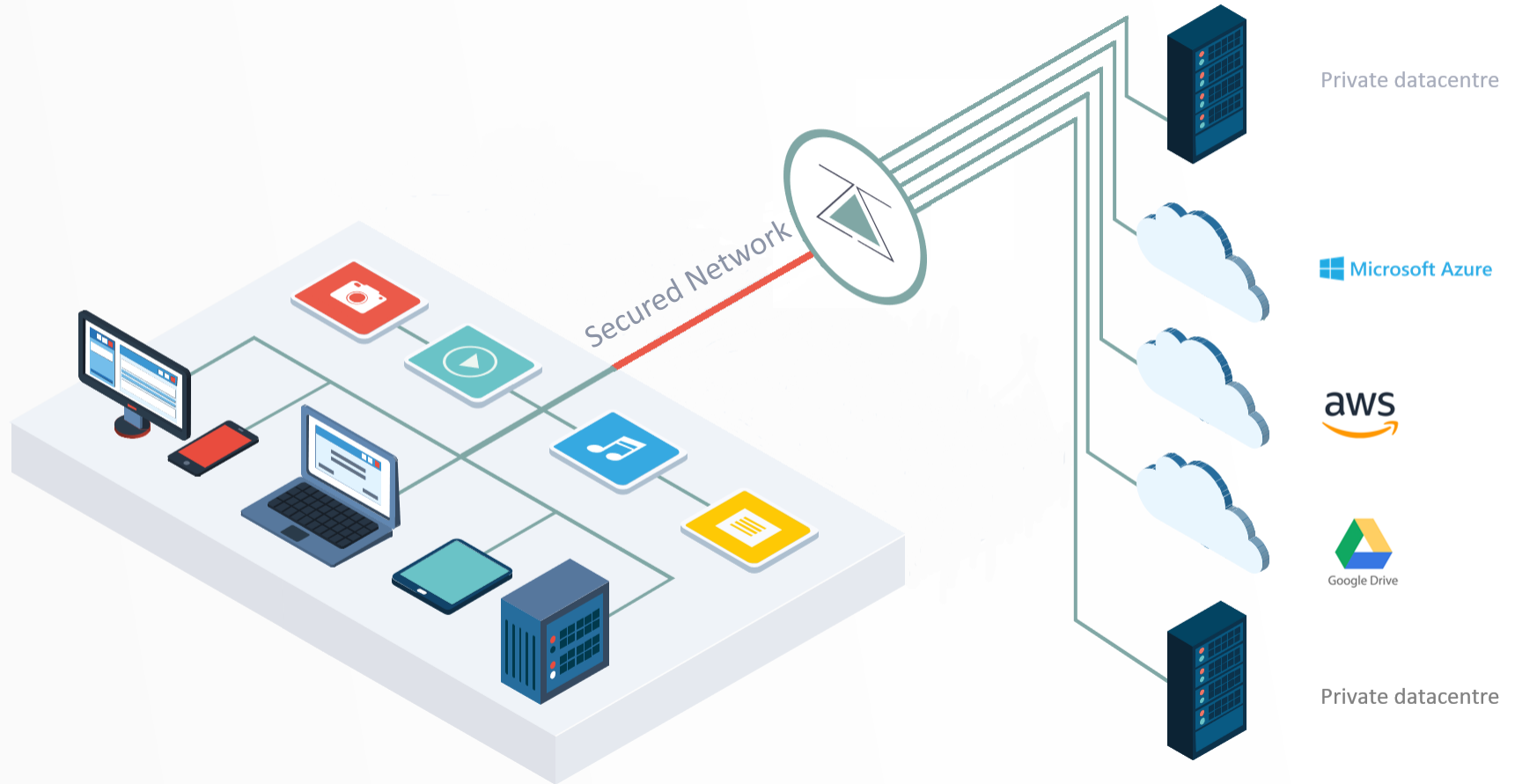
Digital Information

Random distribution

Disaggregation





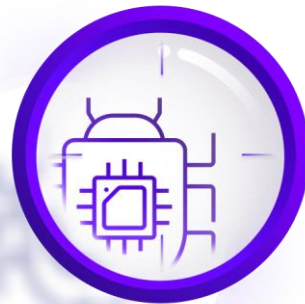




Ministry  
of Defence



Alpha Test  
Programme



Bug Bounty  
Programme



TEAM  
DEFENCE  
INFORMATION



BETADEN





Help us to build on our success

Defining  
Route to Market

Building  
Partnerships

Investment  
Readiness

AWS/Prizsm  
Alignment

AWS Engineering  
Input

AWS CD/CI  
Non-Functionals