QUANTUM AND THE CYBERSECURITY IMPERATIVE

MARCH 27, 2023

DR VIKRAM SHARMA, FOUNDER AND CEO, QUINTESSENCELABS

© 2023 QuintessenceLabs. All Rights Reserved. Commercial in Confidence.

THE SECOND QUANTUM REVOLUTION WILL TRANSFORM OUR WORLD

GENERATING, PROCESSING AND COMMUNICATING INFORAMTION IN A FUNDAMENTALLY DIFFERENT WAY

SENSING/METROLOGY

Using quantum effects – manipulating particles – to detect minute changes in information related to speed, gravity, and electric or magnetic fields.

Quantum sensing technologies are considered less technically challenging than quantum computing, and thus provide more near-term opportunities.

- Precision navigation
- Sensors to detect stealth aircraft, submarines, underground facilities, nuclear materials

COMPUTING

Using quantum effects to process information in a fundamentally different way, enabling computation at unprecedented speed.

Quantum computing has potential to transform the development of AI systems and machine-learning algorithms.

- Optimisation: logistics, supply chain, energy distribution, network optimization

COMMUNICATION

Using quantum effects to create new forms of communication systems and new methods for assuring confidentiality of information.

Quantum communication has the potential to provide ultra-secure communication and secure distributed quantum computing capabilities.

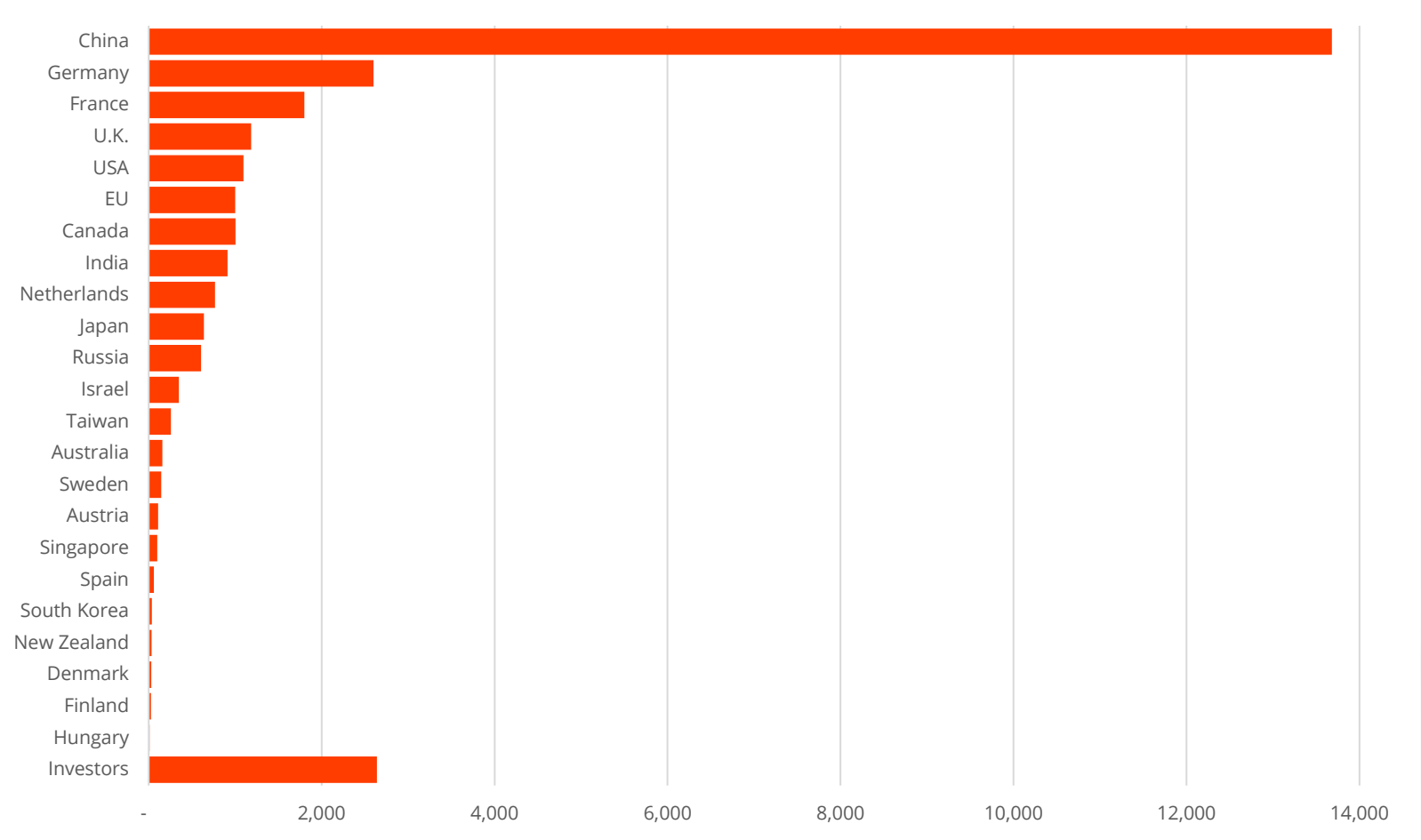
- Technologies commercially available: true random number generation, crypto-agile key management
- NIST has announced first set of quantum resistant algorithms
- Quantum-safe posture critical to securing sensitive information assets

© 2023 QuintessenceLabs. All Rights Reserved. Commercial in Confidence.

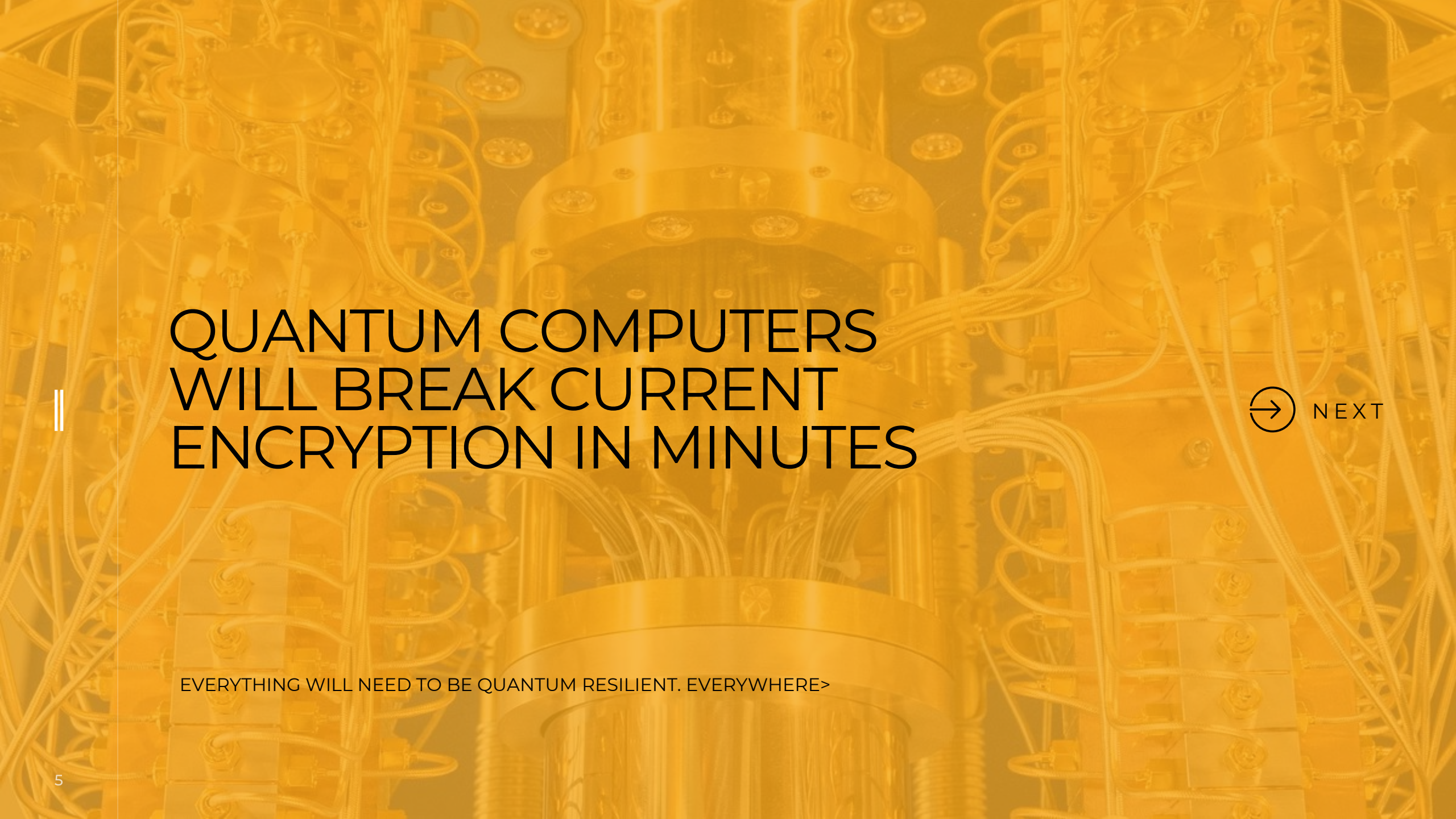
NEARLY €30B INVESTED

IN QUANTUM ACROSS THE WORLD

(early 2022 guesstimates from public sources)



© 2023 QuintessenceLabs. All Rights Reserved. Commercial in Confidence.



QUANTUM COMPUTERS WILL BREAK CURRENT ENCRYPTION IN MINUTES

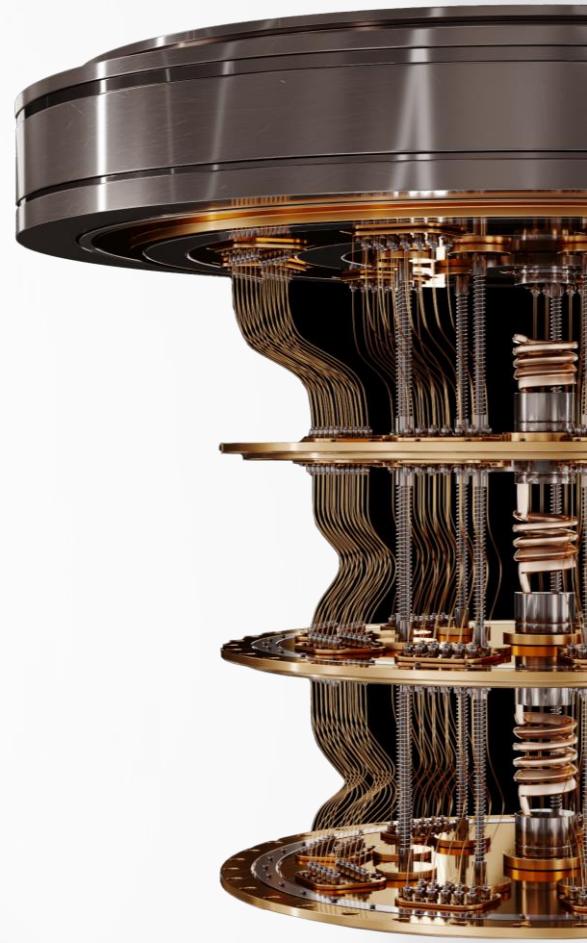
NEXT

EVERYTHING WILL NEED TO BE QUANTUM RESILIENT. EVERYWHERE>

CAPABLE QUANTUM COMPUTERS

WILL IMPACT TODAY'S CRYPTOGRAPHIC SYSTEMS

CRYPTOGRAPHIC FUNCTION	PRIMARY TOOLS	QC ATTACK	IMPACT
• Key Exchange • Digital Signatures	Asymmetric (RSA, DH, ECC)	Shor	Broken
• Data Encryption	Symmetric (DES, AES)	Grover	Weakened
• Authentication	MAC, AEAD modes	Simon	Broken



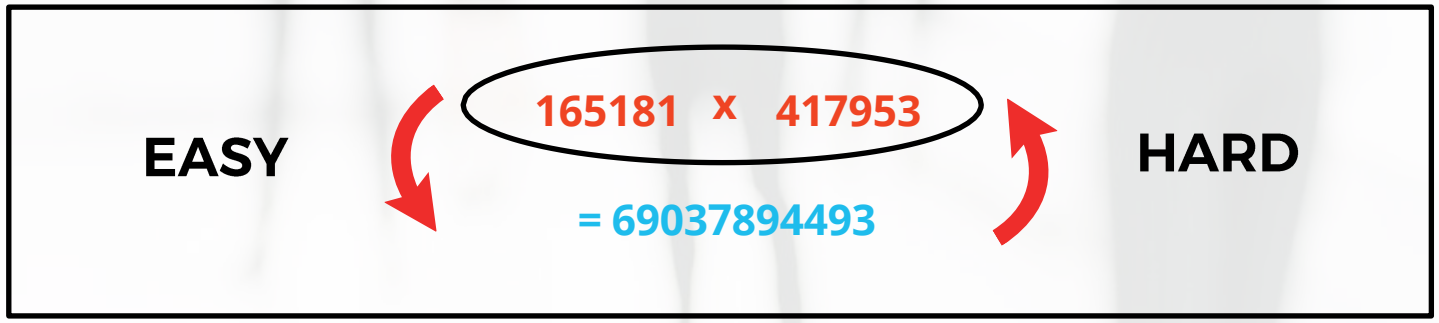
- **No communication link will be trusted to be secure**
- **Communication would not be trusted to be authentic**
- **Transactions could be repudiated**

© 2023 QuintessenceLabs. All Rights Reserved. Commercial in Confidence.

QUANTUM COMPUTERS

AND CYBERSECURITY

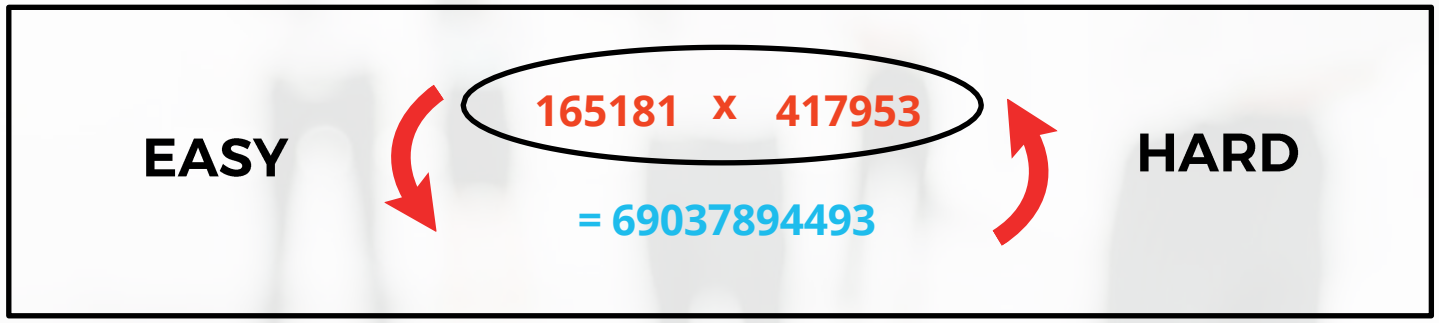
ASYMMETRIC ENCRYPTION



© 2023 QuintessenceLabs. All Rights Reserved. Commercial in Confidence.

QUANTUM COMPUTERS
AND CYBERSECURITY

ASYMMETRIC ENCRYPTION



Factoring 1024-bit semi-prime

- Conventional computer: 3,000 years
- Quantum computer: minutes

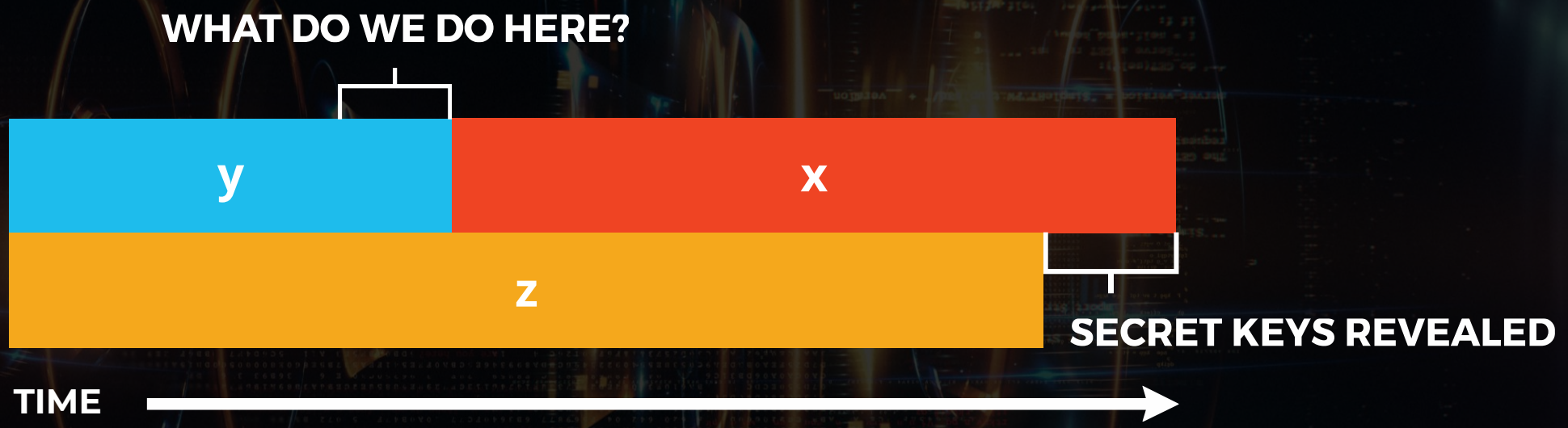
Quantum Computers with Shor's algorithm

- Exponential speed-up of factorization problem
- Other possible algorithms

PUBLIC KEY EXCHANGE WILL NO LONGER BE SAFE

© 2023 QuintessenceLabs. All Rights Reserved. Commercial in Confidence.

THE PROMISE AND THE CHALLENGE OF QUANTUM COMPUTING

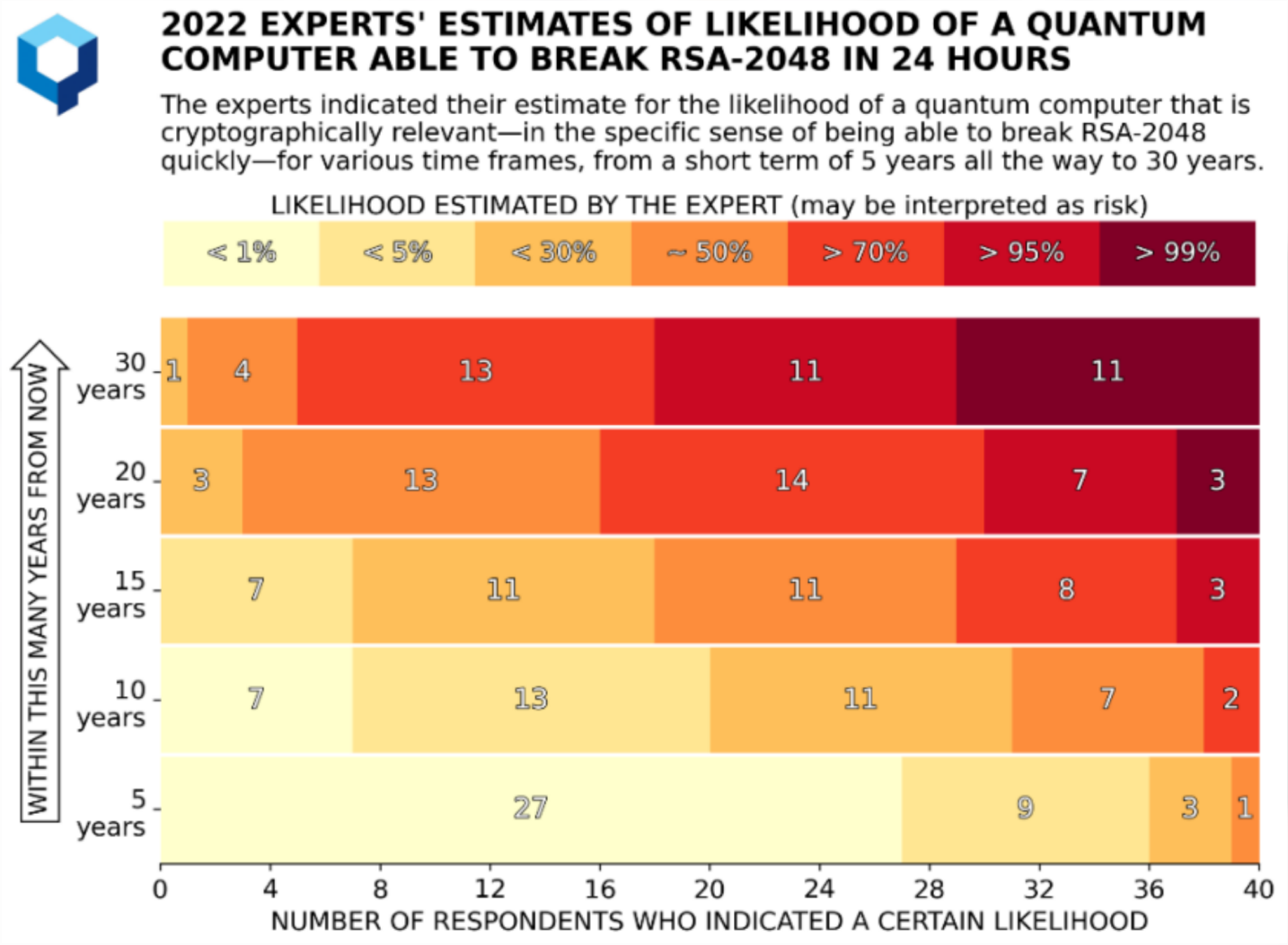


THEOREM (MOSCA): If x + y > z, then worry

y	How long encryption needs to be secure
x	How long to re-tool existing infrastructure
z	How long until crypto-relevant quantum computer built

©2022 QuintessenceLabs. All rights reserved. Commercial in Confidence.

WHEN WILL THE THREAT MATERIALISE?



New algorithms could considerably shorten this timeline due to advances in the last 30 years since Shor:

- **Use of AI & ML**
- **Use of hybrid technologies**

This timeline is based on the quantum requirements of Shor.

Quantum Threat Timeline Report 2022
Global Risk Institute
Dr Michele Mosca, Dr Marco Piani

© 2023 QuintessenceLabs. All Rights Reserved. Commercial in Confidence.

QLABS SITS AT THE INTERSECTION OF QUANTUM AND CYBERSECURITY.

Founded in 2008 as Australia's first quantum technology company with expertise and capability in data protection on premise, in the cloud, and hybrid IT systems

MARKETS

- Banking, Financial Services, & Insurance
- Government, Defence, & Defence Primes
- Critical Infrastructure
- Cloud
- IoT

INVESTORS

- Capital Airport Group
- Main Sequence
- Westpac
- Chevron Ventures (USA)
- In-Q-Tel (USA)
- InterValley Ventures (Japan)
- TELUS Ventures (Canada)

LOCATIONS

- Canberra (Global HQ)
- Sydney
- Melbourne
- San Jose CA (USA)
- Washington D.C. (USA)
- Denver CO (USA)
- Geneva (Switzerland)

©2022 QuintessenceLabs. All rights reserved. Commercial in Confidence.

ADDRESSING CURRENT AND POST-QUANTUM SECURITY NEEDS

TRUE RANDOM NUMBER GENERATION

Strengthen security of high-value long-lived digital assets and critical systems

Highest security seed content generated through the effect of quantum physics and not math

Ability to continuously monitor entropy source health

ENTEPRISE KEY MANAGEMENT AT SCALE

Efficient quantum-enabled management of and approach to encryption, signatures, and certificates

Speed and flexibility to rapidly adjust in response to new security incidents, threats, and regulatory compliance

POST-QUANTUM ALGORITHMS INTEGRATION

Understand and evaluate NIST's post-quantum encryption standardisation

CISO migration strategy and journey to quantum-resistant cryptography

Further enhanced security when combined with QKD

QUANTUM SECURE COMMUNICATION LINK

Need for a provably secure cryptographic building block – quantum key distribution (QKD) – for remote parties to share cryptographic keys

Ability to detect and address attacks on communication link(s) in real-time

STRONG ENTROPY SOURCE

AGILE KEY MANAGEMENT

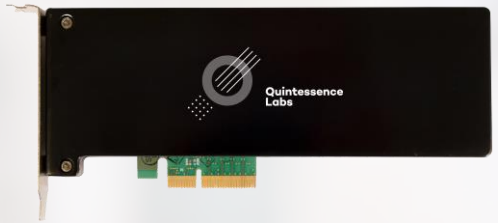
POST-QUANTUM CRYPTO DEFENCE

MINIMISE RISK OF "HARVEST-NOW DECRYPT-LATER" (HNDL) ATTACKS ON COMPANY AND CUSTOMER DATA

©2022 QuintessenceLabs. All rights reserved. Commercial in Confidence.

DEPLOYABLE HARDWARE & SOFTWARE SOLUTIONS

TRUE RANDOM NUMBER GENERATION



qStream™

- World's fastest commercial quantum random number generator (QRNG)
- Encryption keys generated using advanced quantum tunnelling technology
- Tested against standards
- Also available as-a-service

ENTEPRISE KEY MANAGEMENT AT SCALE

POST-QUANTUM ALGORITHMS INTEGRATION

Trusted Security Foundation®

- Cryptographic key and policy manager, incorporating qStream™ QRNG and a FIPS 140-2 L3 Hardware Security Module for root of trust
- Deployable in a cluster configuration for high availability and scalability

QUANTUM SECURE COMMUNICATION LINK

qOptica™

- Continuous-variable QKD protocol (CV-QKD)
- Sharing of secret keys through either fiber optic or free space, secured by the laws of quantum physics using highly tuned lasers
- Easy integration into legacy infrastructure

© 2023 QuintessenceLabs. All Rights Reserved. Commercial in Confidence.

QUANTUM-RESILIENT SECURITY – AN APPROACH…

- Discover & inventory your cryptographic systems
- Identify and map information held by your organisation
- Identify systems and applications exposed to quantum risk
- Understand consequences of compromise for each data category
- Evaluate quantum-safe solutions through trials and pilot programs
- Develop & Implement a quantum-safe transition roadmap
  - Deploy and operate hybrid infrastructure integrating quantum-safe crypto-agile products
    - Post Quantum Crypto Algorithms
    - High entropy symmetric key crypto
    - Quantum Key Distribution

The risk is we do little or nothing … until we are forced to!

© 2023 QuintessenceLabs. All Rights Reserved. Commercial in Confidence.

THANK YOU

www.quintessencelabs.com

© 2023 QuintessenceLabs. All Rights Reserved. Commercial in Confidence.