ENTELEC conference & expo

The Quantum Countdown: Future-Proofing the Physical World (OT) for the Quantum Age

Shaun Six, President, UTSI
scs@utsi.com

UTSI INTERNATIONAL

Education Sponsor:

NOVUS Technical Services

Shaun Six, President, UTSI

Experience:

20 years in Critical Infrastructure, IT/OT Project Management, PMO, Innovation Consulting

- First TTX and Maturity Assessment at Devon Energy 2007
  - BCP, ERP, IRP
- Author of “Quantum Readiness” chapter for ICCSS v2 2026
- Speaker on AI for Decarbonization, PQC, and OT Innovation

BHP ICS – Communications Unit (Logistics)

- Cyber Attacks via malware, social engineering, “sneakerware”
- ICS Response to rig fire, well blowout, county-wide comms outage

Maturity Models and Frameworks:

- AI/Data Science – 2016 (ACN) “AI Hierarchy of Needs”
- PMO Maturity – (JLT)
- IM / Doc Control / EDMS (RedEye)
- OT Cybersecurity (UTSI) - Water/Wastewater, Upstream, Midstream, Downstream O&G
- Working on “Digital Twin” MA for a client and vendor
- Quantum Readiness Maturity and Roadmap

The Goose and the Golden Egg: OT vs IT

- Only 10% of the worlds OT Infrastructure is monitored (Dragos 2025 Year in Review report)
- ~ 90% of Water/Wastewater, Coops, Municipalities, etc… live below the “OT Cyber Poverty Line” (Dragos RSAC – Year In Review report)
- 50% of OT Exploits originate in IT, the other half are from internet facing connected devices (Dean Parsons – ICS Defense Force)
  - In response to an FBI Advisory regarding Iranian APTs targeting ICS (PLCs, Rockwell/Allen-Bradley)) security firm Censys said that an Internet scan it performed identified 5,219 such devices exposed to the Internet. A full 75 percent of them were located in the US. (arstechnica.com, article on FBI advisory April 7)
- Cryptography is used in nearly all assets: Every Server/Workstation, Data at rest, Data in Transit, Software, hardware, etc…

ENTELEC conference & expo

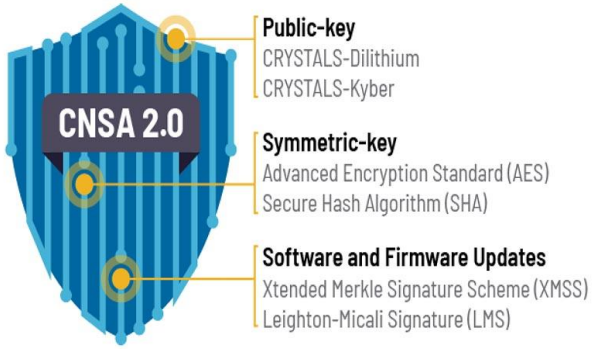
PQC and “Q-Day”

- Some pose that Q-Day will be a cataclysmic event when Quantum breaks all cryptography and nation-states or hacker groups bring the world’s infrastructure to its knees
- Others say it is just another Y2K, being blown out of proportion
  - Fun Y2K facts for context:
    - ~Over $300 Billion was spent to mitigate Y2K risks
    - Internet usage and dependency was negligible(6% of global population) and has grown exponentially to 70%
    - Connected devices: IoT went from not existing to 10s of Billions of connected devices
    - Digital institutional “e”commerce for large institutions, ~$10 Billion annually to over $6 Trillion as of 2025
    - The threat model itself is stealthier and harder to “patch”
- We believe the truth is in the middle, we will have multiple “Q-Days” as Quantum and “Quantum/Classical” hybrid solutions progress, targeting specific cryptographic standards individually

Quantum Trends

- **Acceleration of logical Qubit Progress:** increase in logical qubit advances, enabling demos, lower physical-to logical overhead, a tighter hardware-software co-design using AI
- **AI–Quantum Convergence Deepens:** AI is expected to embed across the stack, from error correction to quantum-enhanced simulation and hybrid workflows
- **Hybrid Quantum–HPC Architectures Become Standard:** Quantum systems could be used to pair with graphics processing units (GPUs) and supercomputers, making hybrid workflows standard
- **Modular Quantum System Design Gains Traction:** Firms are expected to network smaller processors in modular architectures to achieve scalable performance under real-world constraints

Quantum Safe Cryptography and Migration



1994

1°st Theoretical Shor Quantum Attack

2016

NIST PQC Competition

2024

NIST PQC Standard Released

2030

NIST prediction: possibility of 2048-bit RSA broken by 2030
NIST report on Post Quantum Cryptography

2035

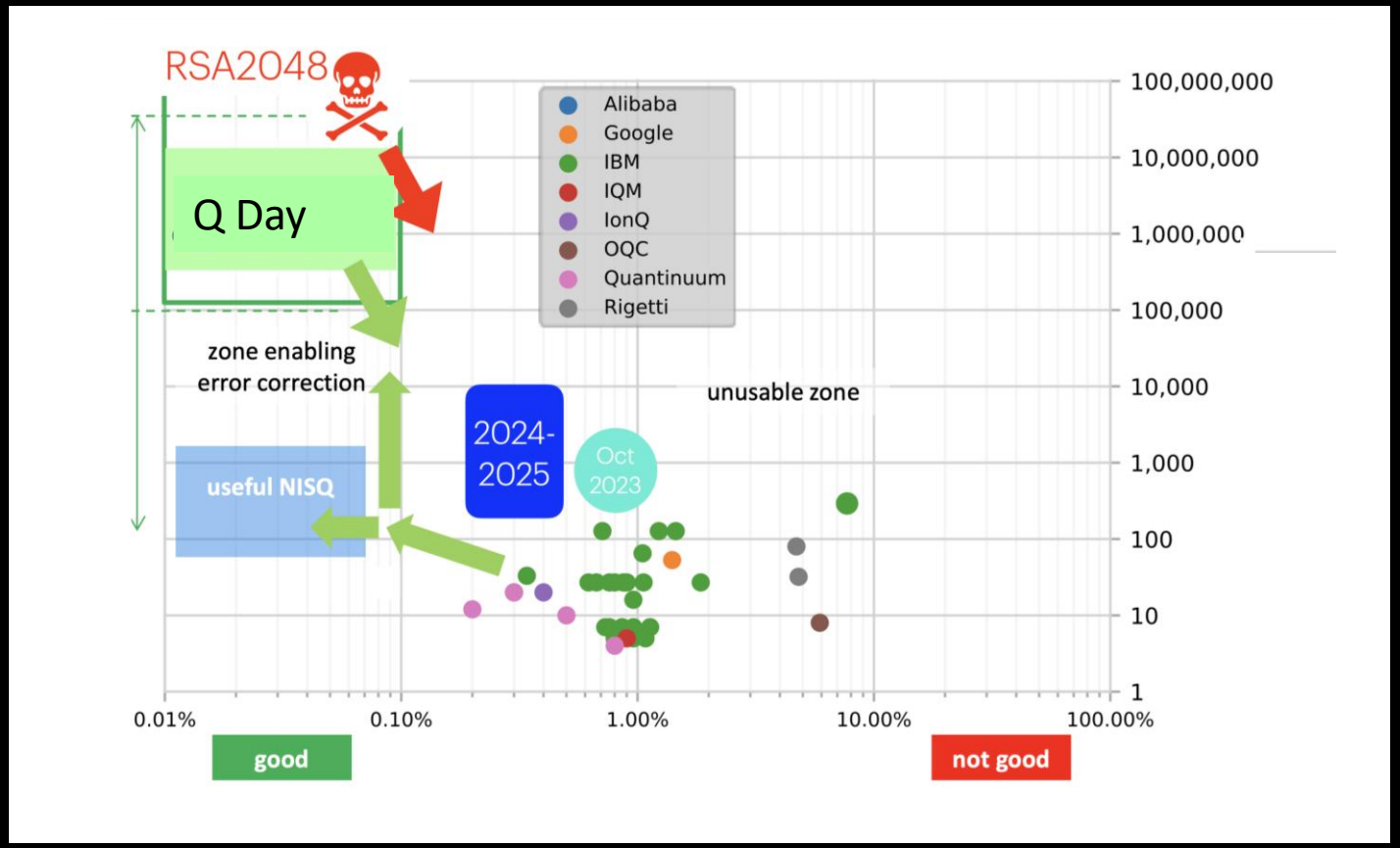
Legacy algorithms disallowed
NIST IR 8547 (Nov 2024)

36 years to prepare

8 years
to create standards

6 years for migration

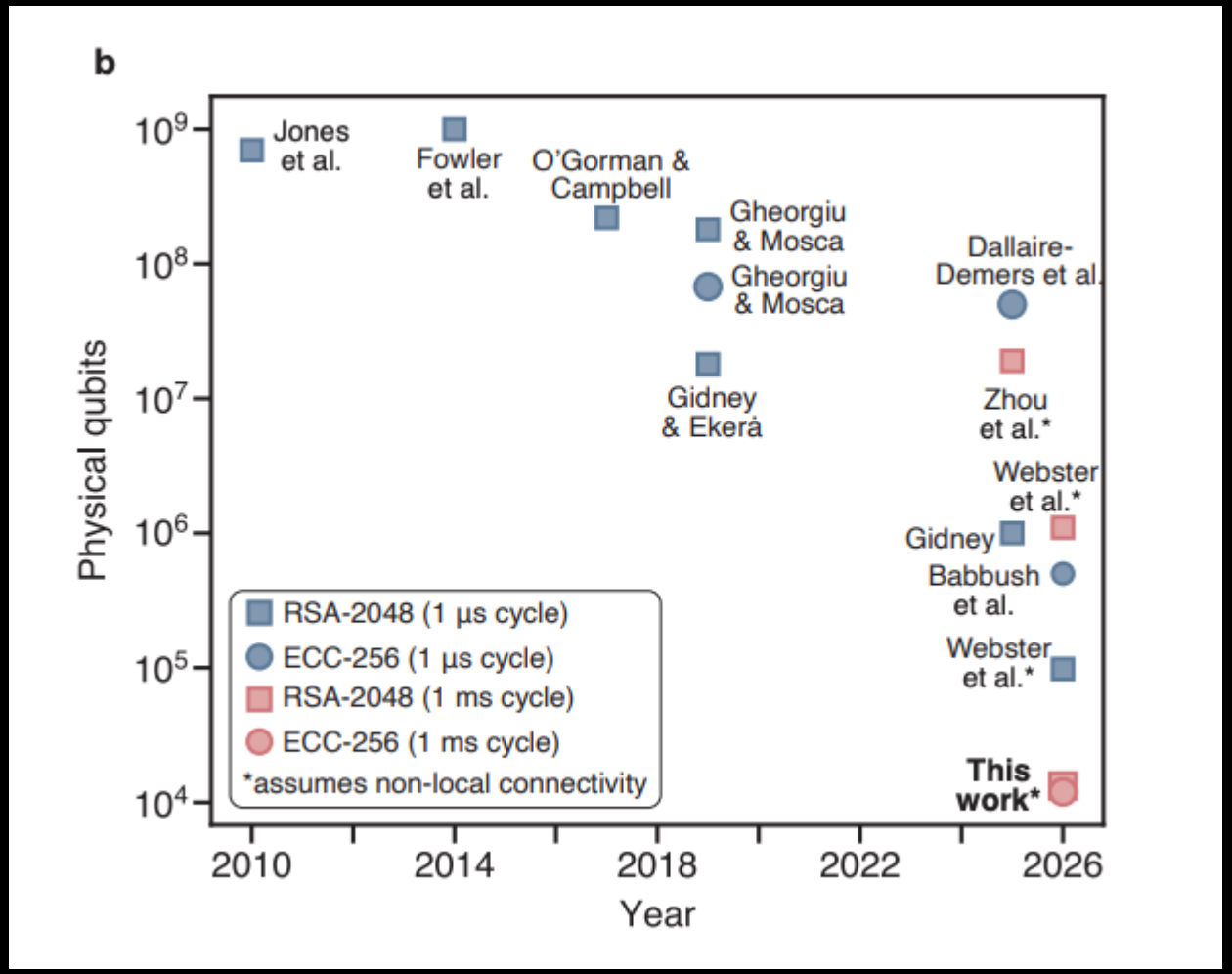
The State of the Arts (SeQure Quantum)



Quantity of Qubits

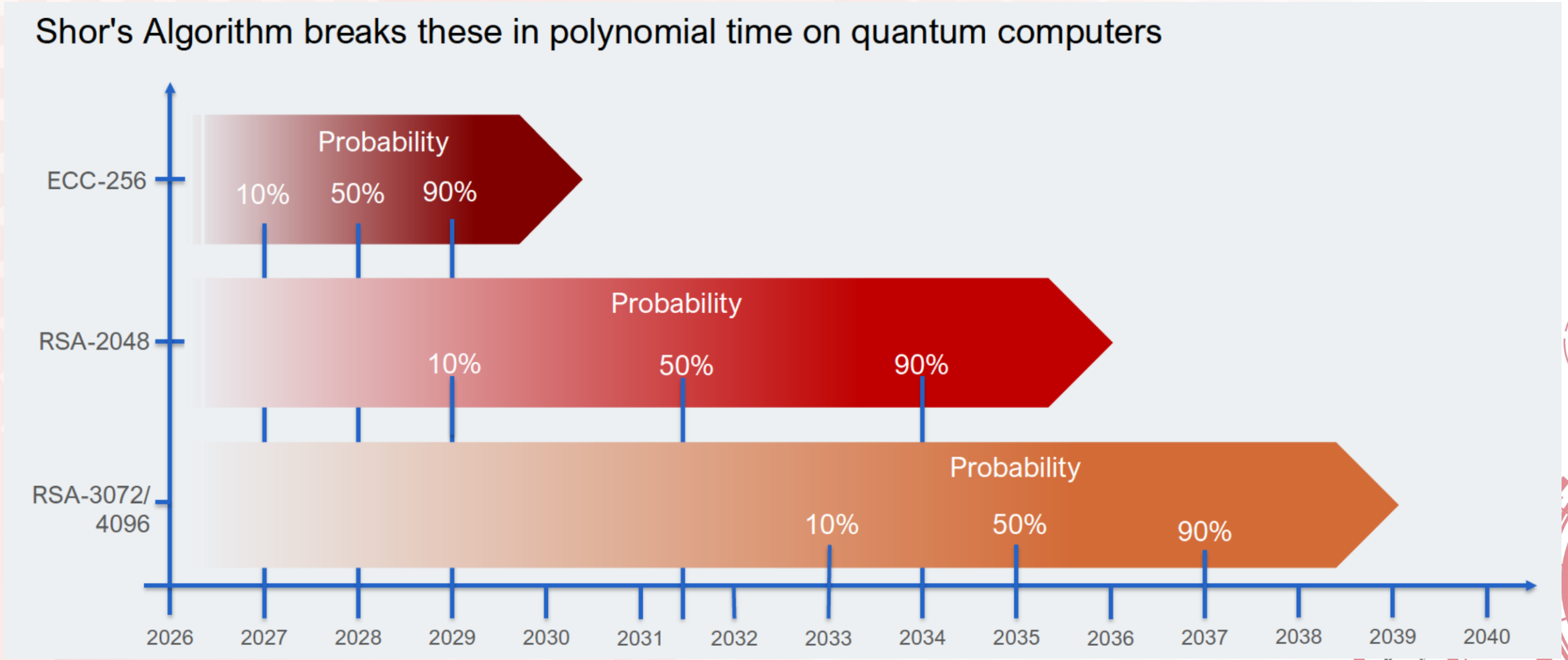
Quality in logical operations

The State of the Arts (Pauli Group)



Estimated number of physical qubits to run Shor's algorithm versus year of publication for prior resource estimates [31, 19, 32, 33, 34, 35, 18, 36, 37] and the current work.

Which Algorithms Break First?



Shared with permission from the image creator, Ines Atug; https://www.linkedin.com/in/ines-atug/

Biden vs Trump. What's Changed?

- Moving from a "compliance-first" model to an **assertive, private-sector-led deterrence** model.

- Shift from technical recommendation > foundational pillar of national security

Feature	Biden Strategy (2023)	Trump Strategy (2026)
Core Philosophy	**Risk Management:** Focuses on defending systems and setting mandatory standards.	**Risk Imposition:** Focuses on disrupting adversaries and imposing costs on hackers.
Regulatory Style	**Prescriptive:** Emphasized new regulations and shifting liability to software makers.	**"Common Sense":** Aims to "streamline" and reduce "costly checklists" for businesses.
Offensive Stance	**Government-Led:** Used "all instruments of power," but largely within federal agencies.	**"Unleashed":** Actively encourages private-sector participation in disrupting adversary networks.
Blockchain/Crypto	**Cautionary:** Focused on "responsible innovation" with a heavy emphasis on illicit finance.	**Proactive:** Explicitly supports the security of private cryptocurrencies and bans a US CBDC.
China & Threat Actors	**Explicitly Named:** Detailed the threats from China (Volt Typhoon), Russia, and Iran.	**Adversary Neutral:** Shorter (7 pages) and focuses on the *methods* of deterrence rather than naming specific nations.

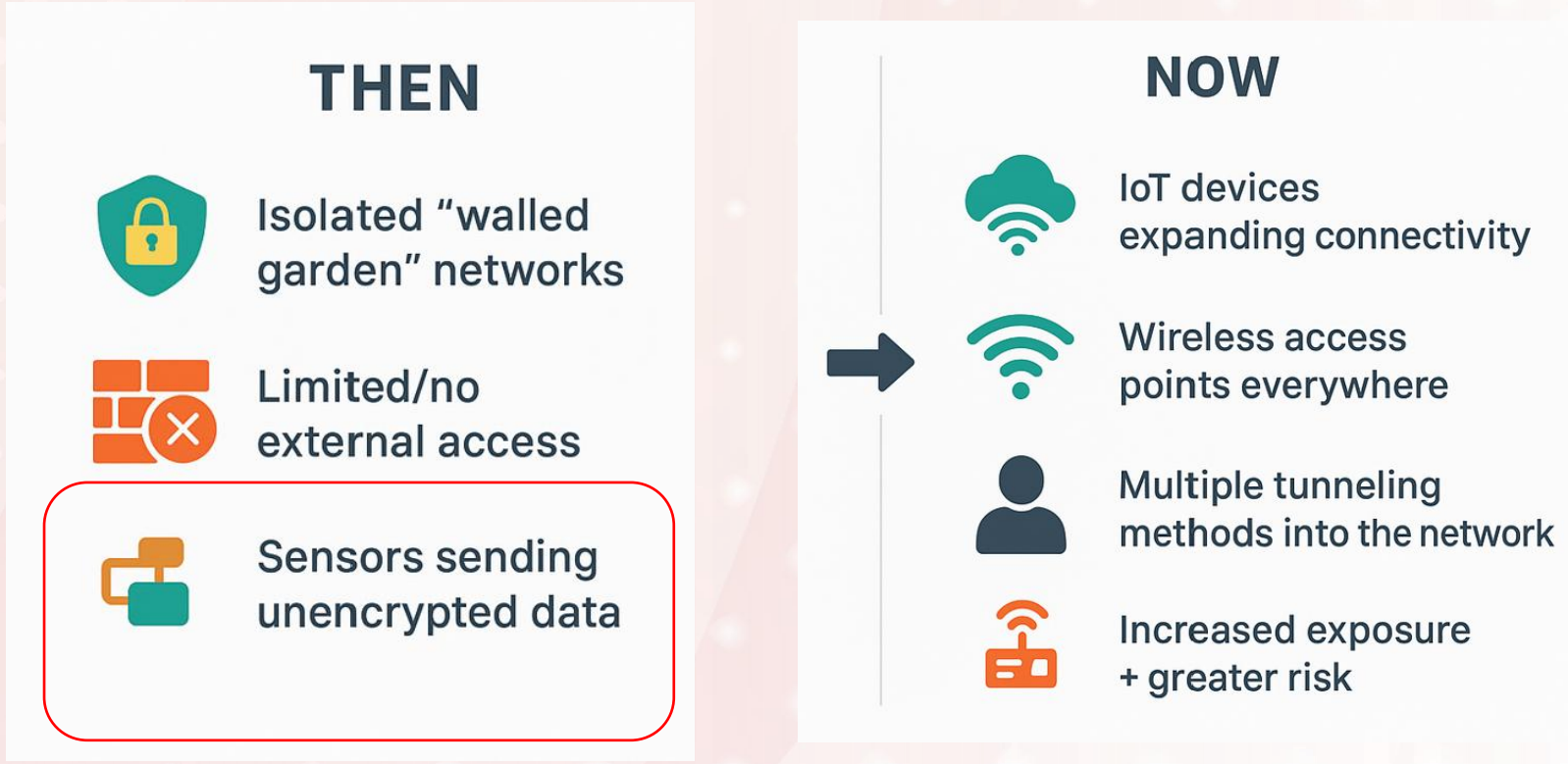
New White House Cyberstrategy

"We will accelerate the modernization, defensibility, and resilience of federal information systems by implementing cybersecurity best practices, **post-quantum cryptography**, zero-trust architecture, and cloud transition."

(Source: President Trump's Cyber Strategy for America, Pillar III)

Pillar	Objective
I. Shape Adversary Behavior	Use offensive cyber capabilities to disrupt hackers before they strike.
II. Common Sense Regulation	Streamline rules to reduce "costly checklists" for U.S. businesses.
III. Modernize Federal Networks	Mandates **Post-Quantum Cryptography** and Zero Trust.
IV. Secure Critical Infrastructure	Hardens the energy grid, water, and telecom supply chains.
V. Sustain Superior Technology	Direct support for **Blockchain**, AI, and Quantum Computing.
VI. Build Talent & Capacity	Rapidly expanding the cyber workforce via vocational/private partnerships.

Process Control Network



Smarter Mouse = Smarter MouseTrap

Evolving Attacker Tactics

- NIST estimates Nation States are 2-3 years ahead of commercially available product, though this is heavily disputed

- Chinese University students crack 22-bit encryption key using D-Wave Quantum Annealing System- accelerating “Q-day” timelines

- AI-powered recon to assess and bypass processes and protection systems

Adaptive Defensive Measures

- Smarter, AI-powered detection tools, Asset Inventory, SBOM, CBOM, AIBOM, etc…

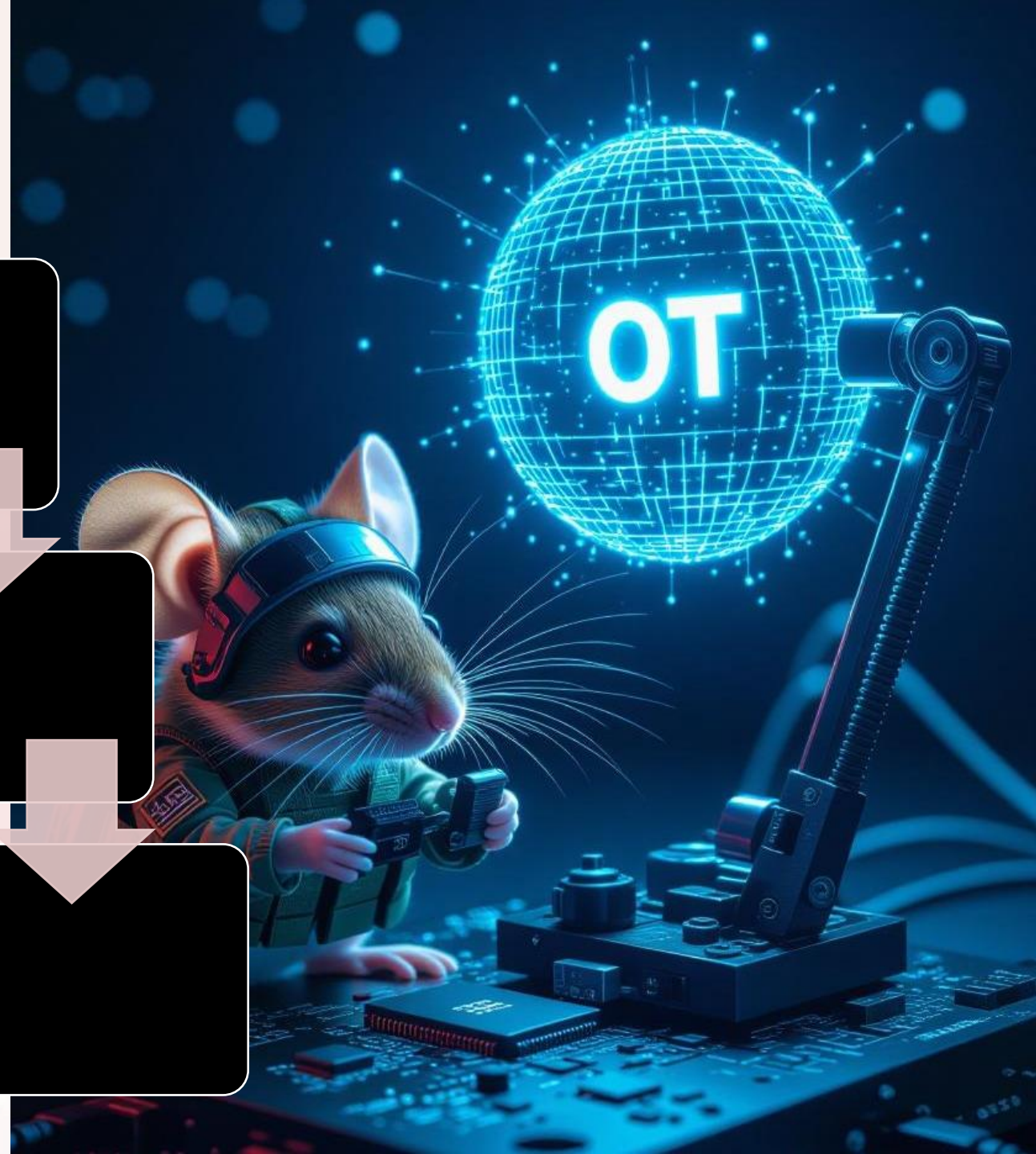
- Proactive monitoring to detect and counter new threats.

- Assessments and testing that include TTX, IRPs, Digital Twins, CRQ, etc..

Continuous Security Improvement

- Continually adapt by implementing rapid response and intelligent monitoring to stay ahead of attackers.

- **Incorporating CI into all frameworks for continual review and capturing/ranking cryptographic risks and prioritization (CIE from greenfield)**



Zero Trust in the Quantum Era

"Never trust, always verify."
Every user, device, and request must prove identity and authorization continuously.
No matter where they come from.

Advanced Cryptographic Authentication

Zero trust models use mathematically generated cryptographic keys that are challenging to crack for device authentication.

Quantum Computing Threats

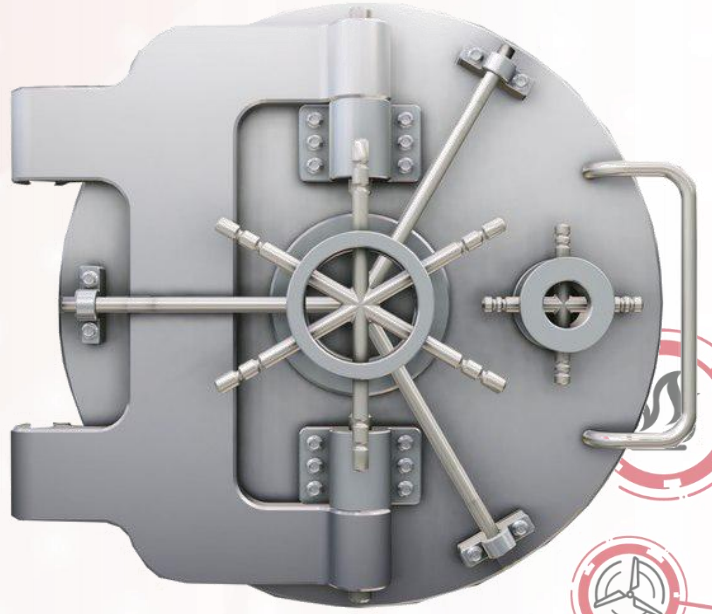
Although it's not high risk today, quantum computing may soon break traditional cryptographic defenses, creating new security risks as it becomes faster, cheaper and more commonplace.

Preparing for and Testing Next-Gen Security

We are collaborating with partners like Sequre Quantum to educate / raise awareness and integrate and test advanced security technology in our SCADA lab to address emerging threats.

Lock and Key Cryptography

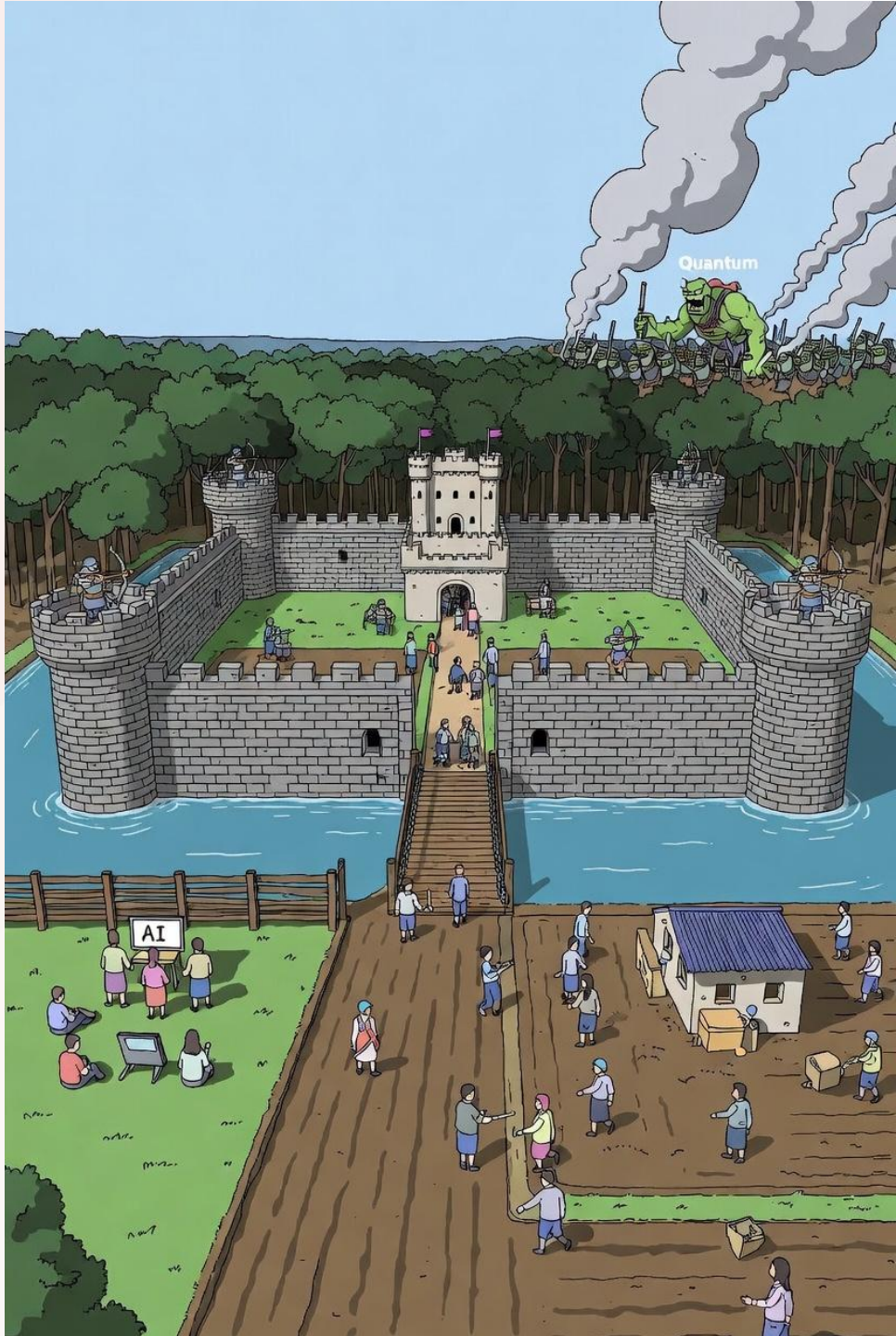
Facing new technological challenges, we must strengthen both the lock —cryptography— and the key and lock mechanism —cryptographic keys— to ensure true security.



QRNGs with traditional OT Best practices will mitigate the risk by strengthening encryption used for:

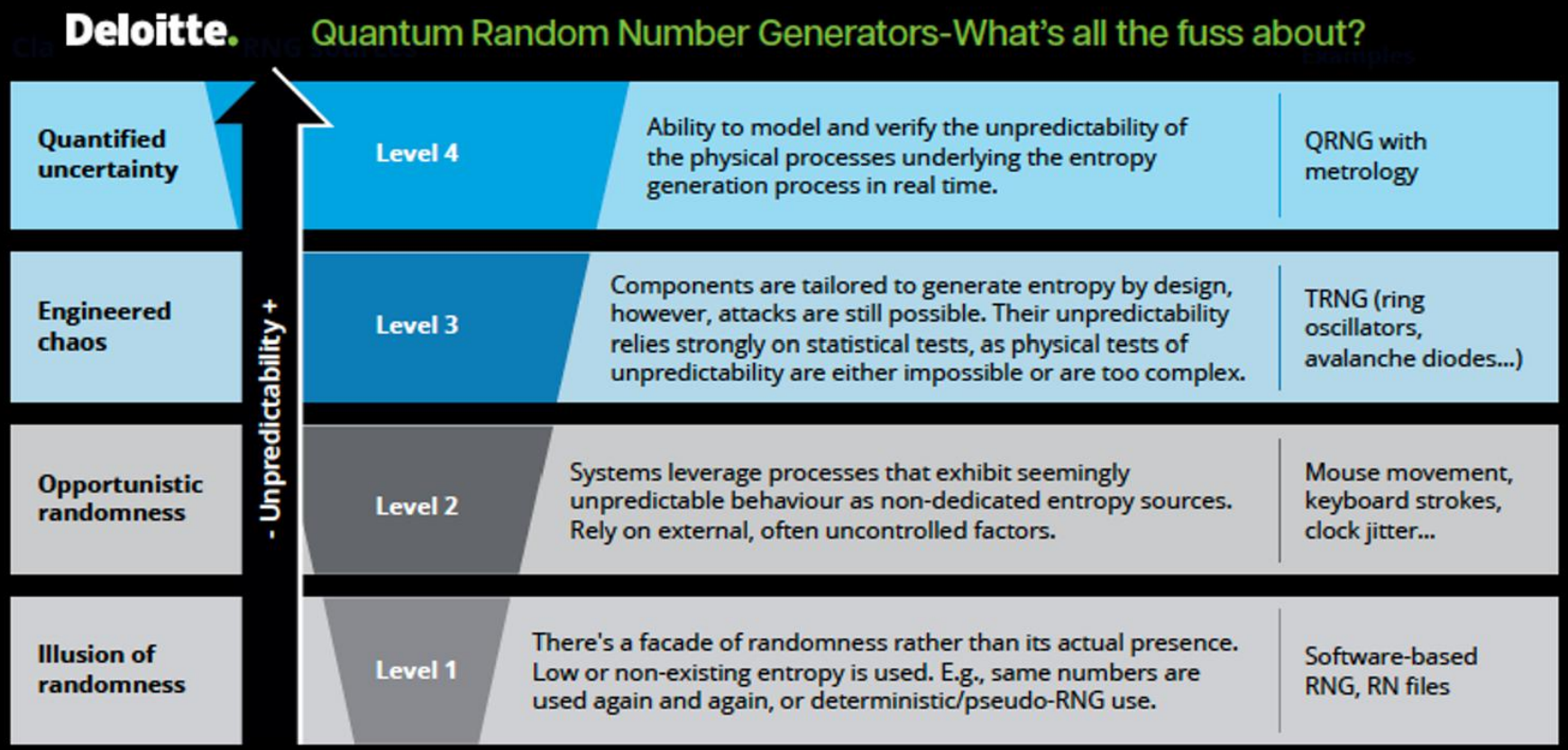
- **Zero Trust** (drawbridge)
- **Network Monitoring** (Guard towers)
- **Zones and Conduits** (the moat)
- **Data in Transit** (crossing the bridge)
- **Data at Rest** (treasure inside the walls)

Protecting the Golden Goose



Quantum Random Number Generators

QRNGs recognized as the apex of RNGs

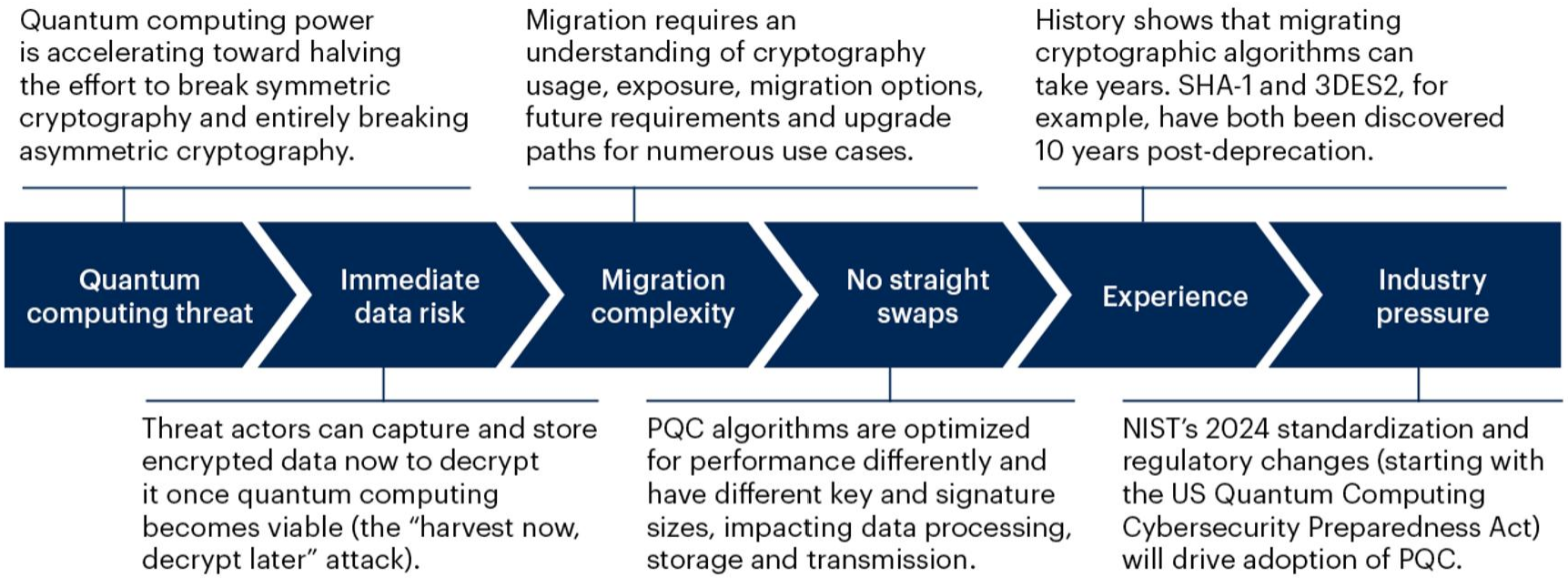


Preparing for Post Quantum

Basic OT Cyber best practices apply are even more critical now (ISA 99-type segmentation, micro-segmentation, zones and conduits, etc.. .)

- NIST CSF style assessments (all include supply chain risks)
- Network Architecture Review (IEC 62443 3-2)
- Asset inventory
- SBOM
- CBOM

Post Quantum Context and Urgency

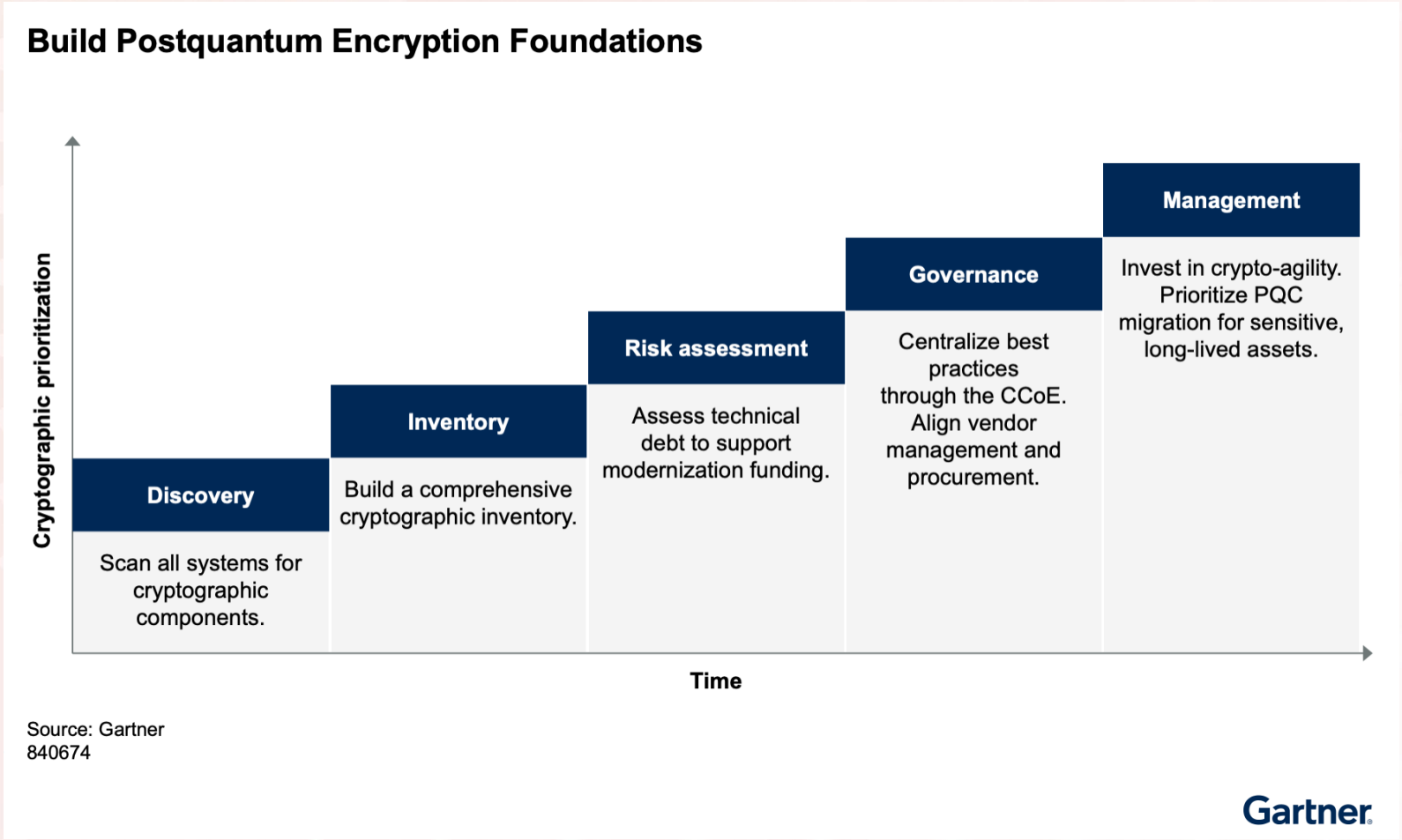


Source: Gartner

818124_C

Gartner

Crypto Inventory Management



Sample Inventory

Sample Inventory

System name	Application name	Algorithm	TLS 1.3-capable	Criticality	Impact if broken

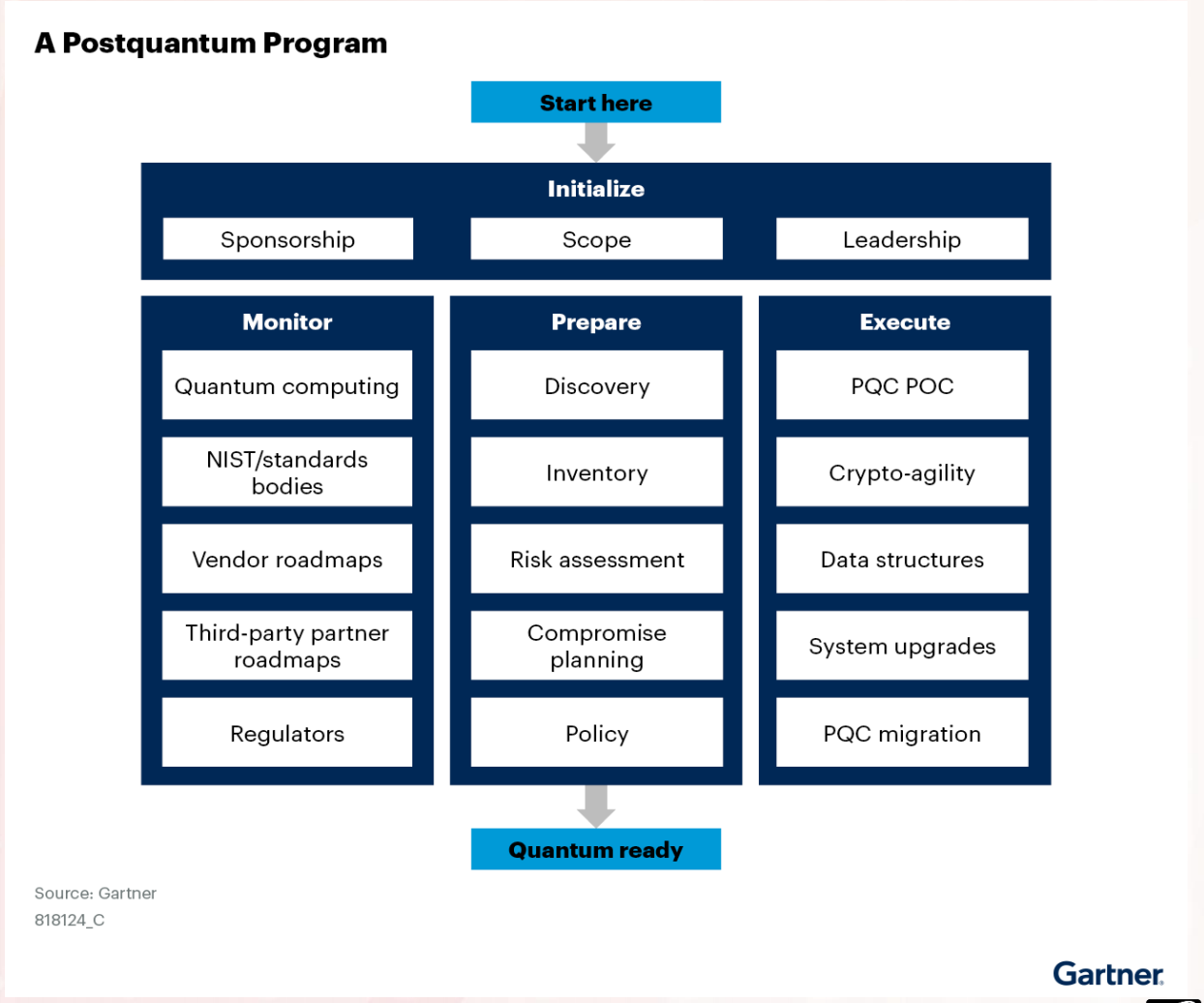
Source: Gartner

818386_C

Gartner

ENTELEC conference & expo

Building / Launching a Postquantum Response



Gartner

ENTELEC conference & expo

The Six Dimensions of Crypto-Agility

1. Inventory

Know What You Have

- Maintain a complete catalog of keys, certificates, and cryptographic protocols
- Enable continuous discovery and tracking
- Map dependencies across systems and infrastructure
- Typical challenge: legacy components and hidden cryptography

2. Substitutability

Replace Without Rewrite

- Use modular architectures
- Provide algorithm-independent APIs
- Avoid hardcoded cryptography
- Example: switching from RSA to ML-KEM through configuration only

3. Configurability

Adjust Without Code Changes

- Modify parameters at runtime
- Support cipher-suite negotiation
- Apply policy-driven algorithm selection
- Example: choosing algorithms during a TLS handshake

4. Automation

Scale Operations

- Automate key rotation
- Automate certificate renewal
- Enforce policies automatically
- Without automation, large-scale crypto management becomes unmanageable

5. Monitoring

Monitor & Validate

- Track cryptographic events in real time
- Analyze algorithm usage
- Validate compliance
- Maintain a complete audit trail for all changes

6. Governance

Control & Compliance

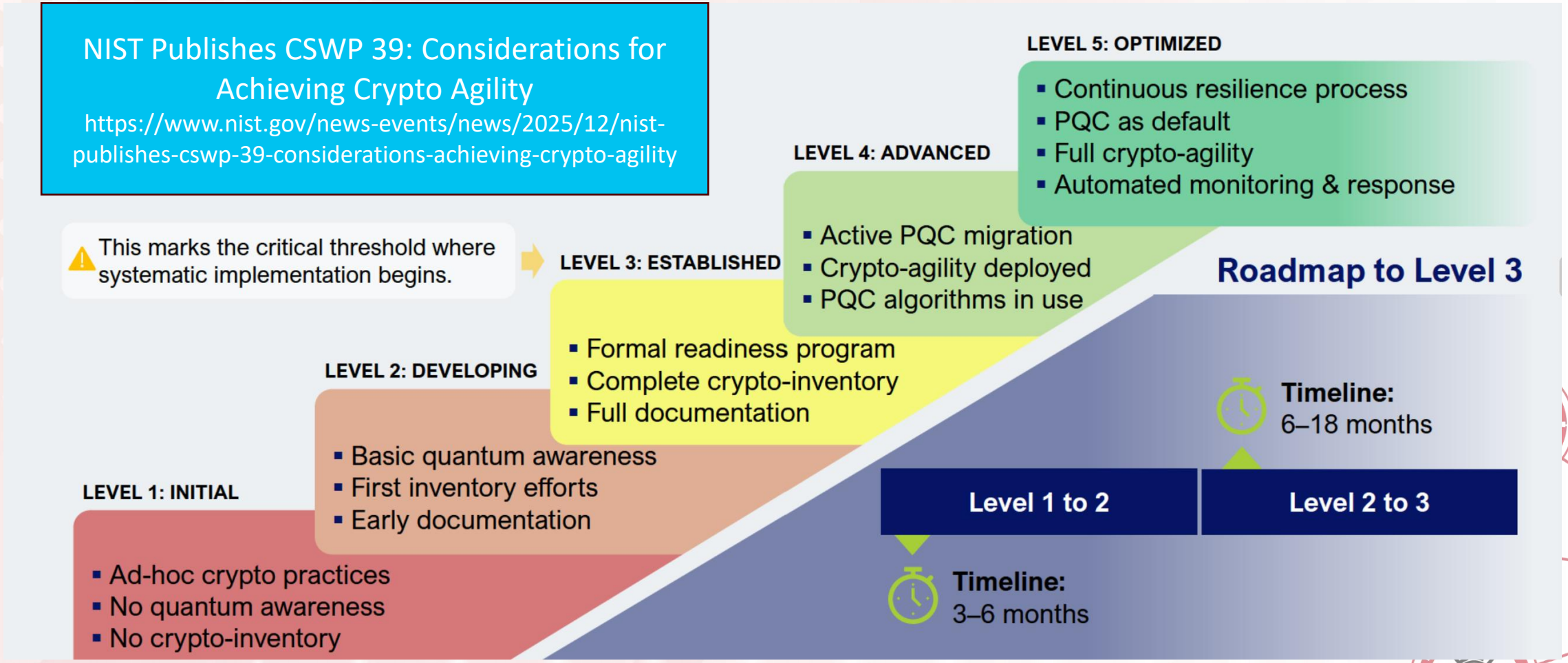
- Establish a clear policy framework
- Define roles, responsibilities, and decision authority
- Align with regulatory requirements
- Document exceptions and deviations

https://www.linkedin.com/in/ines-atug

ENTELEC conference & expo

Q-Day Readiness Assessment Framework

NIST Publishes CSWP 39: Considerations for Achieving Crypto Agility
https://www.nist.gov/news-events/news/2025/12/nist-publishes-cswp-39-considerations-achieving-crypto-agility



Dimension 6: Governance

- The Q-Day Readiness Assessment framework is composed of the six crypto agility dimensions
- Maturity is measured across defined levels within each dimension
- In line with the “weakest link” principle, a maturity level is considered achieved only if all questions answered at the level are “Yes”.

Maturity Level	Questions	Answer
1 - Initial	Are cryptography requirements documented? Is there basic awareness of regulatory requirements (e.g., NIS2, GDPR)?	Yes
2 – Developing	Is a documented cryptography policy available? Are roles and responsibilities defined (e.g., in a RACI)? Are regulatory requirements being tracked? Is there a process for documenting exceptions? Is basic training provided to relevant staff?	Yes
3 – Established	Is a clear policy framework for cryptography established and communicated across the organization? Is a quantum-readiness program in place with an executive sponsor? Are vendor requirements for PQC readiness defined? Is crypto governance integrated into the ISMS (ISO 27001)? Are escalation paths for critical cryptographic findings defined	No
4 – Advanced	Is there a cross-functional quantum-readiness team? Are third-party risks assessed systematically? Is risk-based prioritization for migration implemented? Are KPIs for crypto agility defined at the management level? Are deviations and exceptions centrally documented and approved?	Yes
5 – Optimized	Is crypto governance embedded in the enterprise risk strategy? Are policies automatically enforced (policy-as-code)? Is continuous compliance with automated attestation in place? Is the organization proactively adapting to new regulatory requirements? Is the effectiveness of governance continuously measured and improved? Is the organization “crypto-agile by design”?	No

QRNG Testing Use Case in the UTSI Lab

- Conducted a FIPS test in our SCADA Lab
- “Lowest score I’ve seen in15 years” - DARPA OT Tester
- Moving forward: Joint venture in blockchain, increase capabilities to integrate and goal is to seed traditional RSA cryptography with QRNGS vs PRNGS

Download our
Quantum Whitepaper

- Existing certifications SP800-90B do not address the entropy source randomness for a photonic source, I.e Quantum Source. And further 90A or 90B do not address “how” to measure the quality and consistency of randomness.

“When we started this journey back in 2022, adopting QRNG for full-stack cryptography security we also addressed the need for strong keys. However, we quickly came to realize there is no standard or QRNG vendor that we knew of then who had built a verification process to test the quality of randomness. I’m sure hopeful that the industry is now addressing this issue, and Sequre Quantum is leading the way with a continuous testing and qualification of QRN material with a standardized approach to prove their source is based on quantum physics”

~Large multinational hardware/software cybersecurity provider

Quality QRNG tools should self-test and certify both the source is truly quantum and the numbers generated are truly random

SeQRNG Self-Testing Quantum Random Generation

The most secure device on the market:

- Active self-testing
- Robust against hardware malfunctions and attacks
- Compliance QES2 Int. Telecomm Union [ITU-T X.1702] NIST 800-90B, NIST 800-22
- Easy integration via API

GLI GAMING LABORATORIES INTERNATIONAL®

Key Takeaways

1	The risk is now: “Harvest now, decrypt later”
2	The transition to Quantum Safe technologies has already begun – having a framework and readiness plan in place is critical
3	PQC is a foundational pillar of U.S. National Security (a strategic decision, not a technical one)
4	Security begins with true randomness - QRNGs can help mitigate risk
5	“CBOM” and SBOMs should be included in recurring reviews, included in OT Assessments and ran in tandem with Asset Inventory in a “continual improvement”/evergreen OT Cyber program

Thank You!

Shaun Six
scs@utsi.com
Utsi.com

Don’t forget to download our Quantum Whitepaper!