International SecurityLigue

39th General Assembly 2025

Leadership Forum

Extracting Opportunities from Challenges

16th September 2025, New York USA

International SecurityLigue

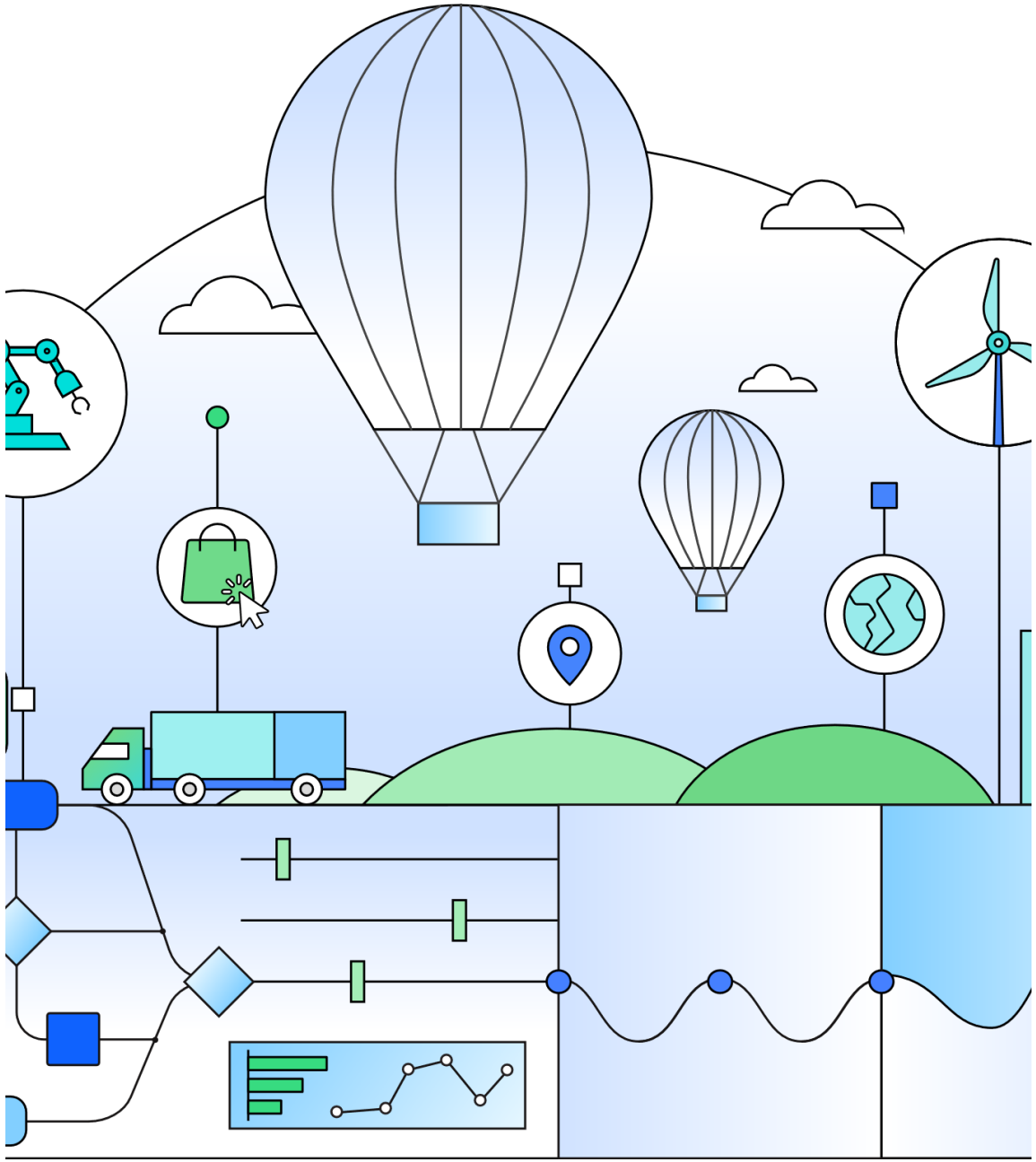
39th General Assembly 2025

Gerry Parham
IBM Institute for Business Value

Quantum Computing

The Next Frontier and Impact on Private Security Companies

10:30 – 11:30



IBM Institute for
Business Value

Quantum –
The next frontier in computing

Risks & opportunities for private security companies

Briefing for International Security Ligue stakeholders
September 2025

IBM

Gerald (Gerry) Parham
Global Research Leader,
Security and CIO
IBM Institute for Business Value
linkedin.com/in/gerryparham

About the IBM Institute for Business Value

Gerry is the Global Research Leader for Security & CIO within the IBM Institute for Business Value. He advises senior executives and board members on technology and security strategy, cyber risk, and cyber value chains.

With more than 20 years of experience in executive consulting, innovation, startups and intellectual property development, Gerald's thought leadership has been recognized for excellence and featured in leading media outlets such as *The Wall Street Journal.*

He holds Masters degrees in science and fine arts from the California State University and the University of Southern California, as well as a BA in writing from Johns Hopkins University.

The IBM Institute for Business Value (IBV) is a thought leadership think tank within IBM. We conduct primary research and create fact-based, data-informed assets to help leaders make smarter business decisions. Our objective, independent research insights lead the industry in quality, influence & trust.

Agenda

Quantum –
The next frontier in computing

Risks & opportunities for private security companies

1. **Introduction**
2. **Where there is opportunity, there is risk**
3. **Where there is risk, there is opportunity**
4. **Potential next steps**

Leaders are looking to supercharge growth via emerging technologies

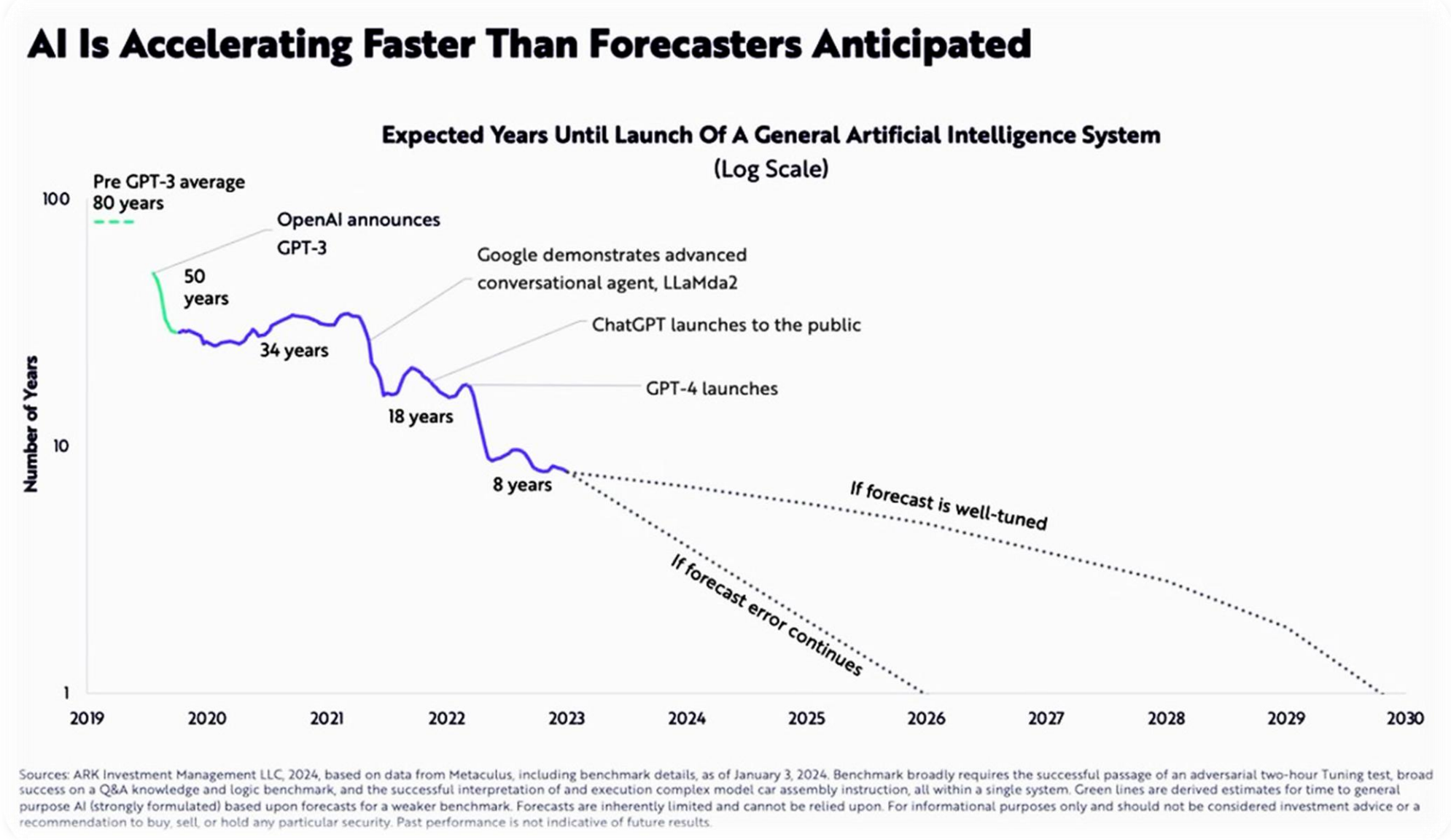
"One of the biggest threats is not any adversary, but our own lack of imagination."

Koos Lodewijkx – CISO, IBM

"These AI capabilities create the opportunity to dramatically change how a business operates over the next three years. The best business and technology organizations will use this to 100X their business. The best security organizations will be part of 10X-ing, 100X-ing, 1000X-ing these businesses. It's incumbent on us as security leaders to be that force that helps make that possible, that creates the trust those organizations need to 10, 100,1000X themselves."

Chris Betz – CISO, AWS

AI can handle tasks twice as complex every few months. What does this exponential growth mean for how we use it?



Quantum computers can handle tasks that take today's most powerful computers millions of years (if at all).

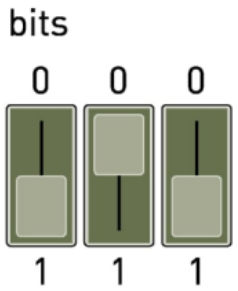
CLASSICAL COMPUTER

0

1

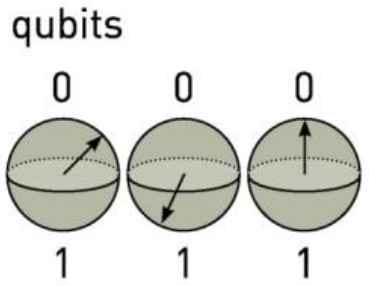
Classical Bit

Classical bits can only be 0 or 1



bits are independent of each other

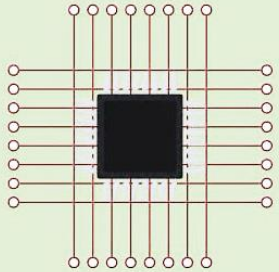
Calculates with transistors which operate like switches – either on or off

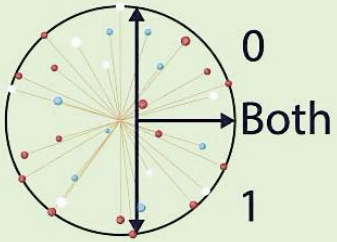


qubits are in a combined state together

Calculates with thousands of qubits which can represent an infinite amount of outcomes at once

QUANTUM COMPUTER





Qubit

Qubits follow the superposition principle and can exist as "0" and "1" at the same time

https://www.berkeleynucleonics.com/august-23-2024-quantum-computing-vs-classical-computing
https://quantumpoet.com/quantum-computing-introduction/

Why quantum computers are faster at solving problems

Quantum computers are faster than traditional computers for optimization problems, such as finding the more efficient options for supply chains.

Each ◇ represents an option.

A **traditional computer** tries each combination individually.

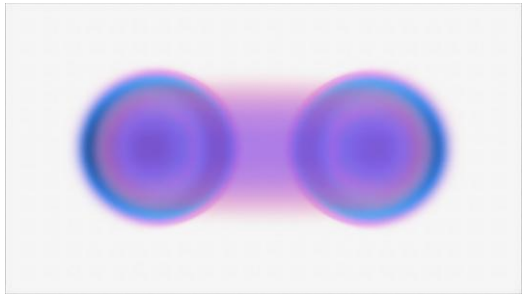
A **quantum computer** tries all combinations at once.

Source: Google Quantum AI
Peter Champelli/THE WALL STREET JOURNAL

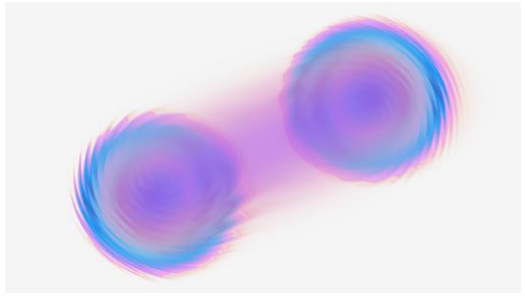
Uniquely quantum

Some problems are classically intractable and will never be solvable with traditional computers

Superposition
A quantum system existing in a complex linear combination of two states until it is measured



Entanglement
Information shared jointly between entangled pairs or groups



Interference
Interaction that affects likelihood of solutions

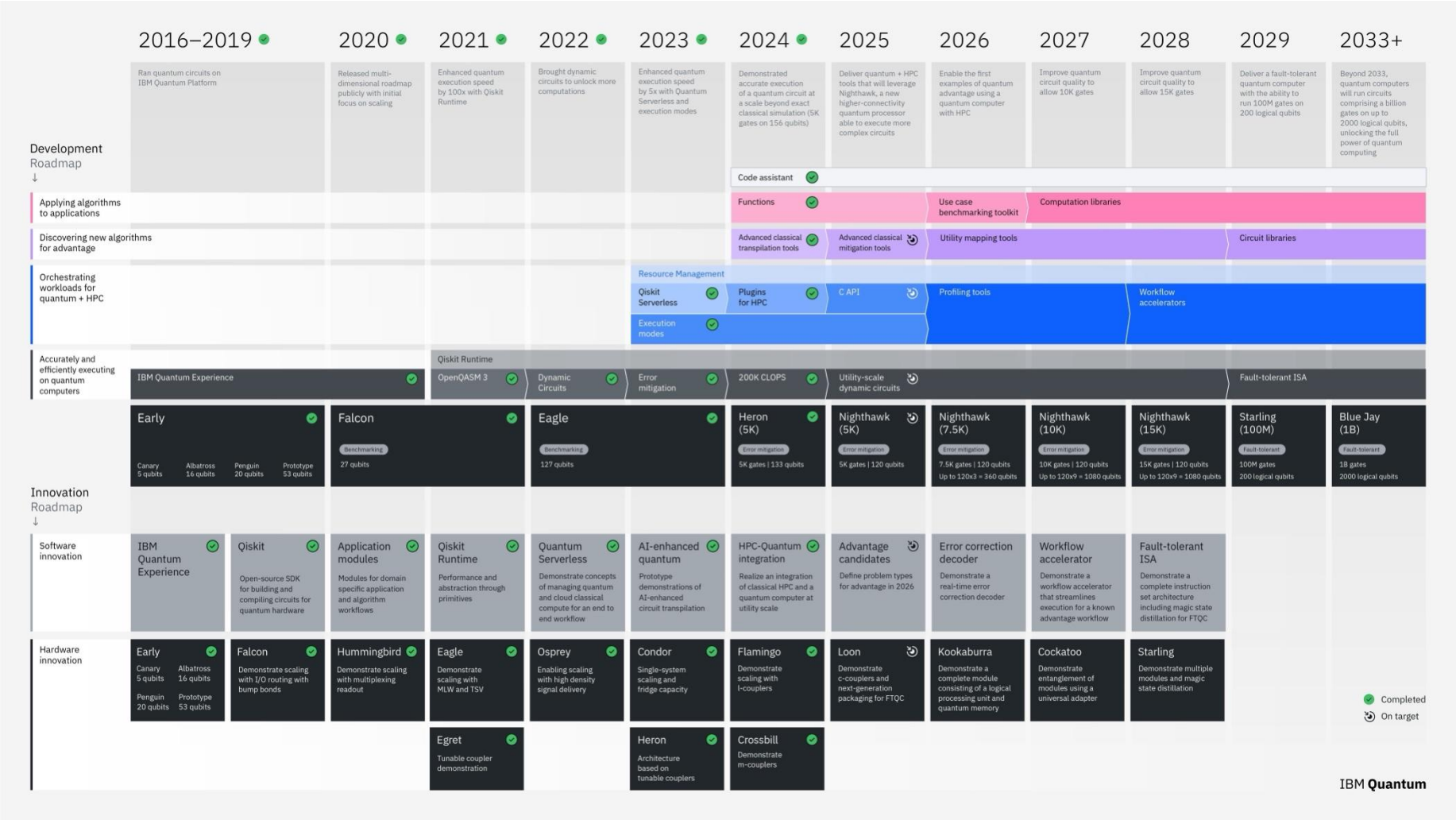
Moore's law: the number of transistors in a classical integrated circuit doubles about every two years
... but we are approaching the end due to physical limitations

Approaching the physical limit: IBM created the world's first 2 nm node chip in 2021, with transistors as small as 10 silicon atoms

10

These Quantum concepts can reduce the number of computational steps required for certain algorithms
&
At a ~100 qubit scale, with sufficient circuit depth and complexity, classical computers can no longer simulate exactly

Over the next 4 years, IBM will build the world's first large-scale, fault-tolerant quantum computer.



IBM has the most viable path to realize fault-tolerant quantum computing.

By 2029, we will deliver IBM Quantum Starling — a large-scale, fault-tolerant quantum computer capable of running quantum circuits comprising 100 million quantum gates on 200 logical qubits.

https://www.ibm.com/quantum/blog/large-scale-ftqc

Where there is opportunity, there is risk.

Our digital world depends on cryptography, which is used in trillions of transactions on billions of devices

Internet
Domain name system (DNS), Hypertext Transfer Protocol (HTTPS), Telnet, file transfer protocol (FTPS)

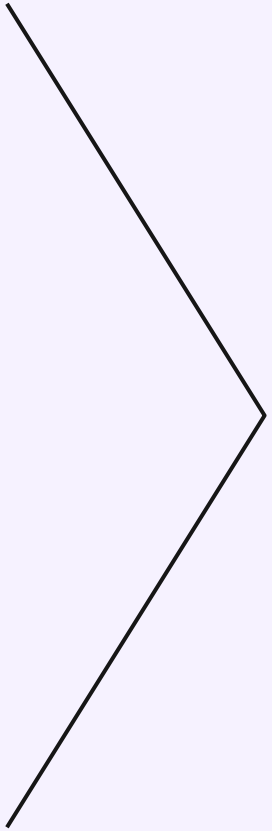
Digital signatures
Electronic identification and trust services (eIDAS), PDF advanced electronic signature (PAdES), advanced electronic signatures

Critical infrastructure
Code updates, control systems, car systems

Financial systems
Payment systems: EMV, CHAPS, Fedwire, TARGET2, EURO1; SWIFT; settlement systems

Blockchain
Wallets, transactions, authentication

Enterprise
Email: PGP, identity management, PKI, LDAP; virus scanning patterns; PKI services; bespoke applications



Systems have long update cycles

Passports: 10 years from issue

Road vehicles: 15–20 years

Aircraft/rail: 25–30 years

Some critical infrastructure: 50+ years

Data needs to stay secure for a long time

HIPAA: 6 years from last use per Security Rule

Tax records: 7–10 years in most countries; Sarbanes-Oxley Act set the precedent in the US

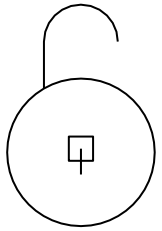
Legitimate interest under GDPR: 20+ years

Toxic Substances Control Act/Occupational Safety and Health Act: up to 30 years

What will a cyber criminal be able to do?

Adversaries might:

- Launch extortion attacks by threatening to disclose harvested data
- Create fake software signatures introducing malware
- Create indistinguishable fraudulent land records or lease documents
- Create fraudulent transactions on blockchains
- Manipulate bank transactions
- Remote control critical infrastructure



Decrypt lost or harvested confidential historical data through cracking encryption keys *(Harvest now, decrypt later)*

Gain access to critical infrastructure through fraudulent authentication

Manipulate legal history by forging digital signatures

Quantum computing risks

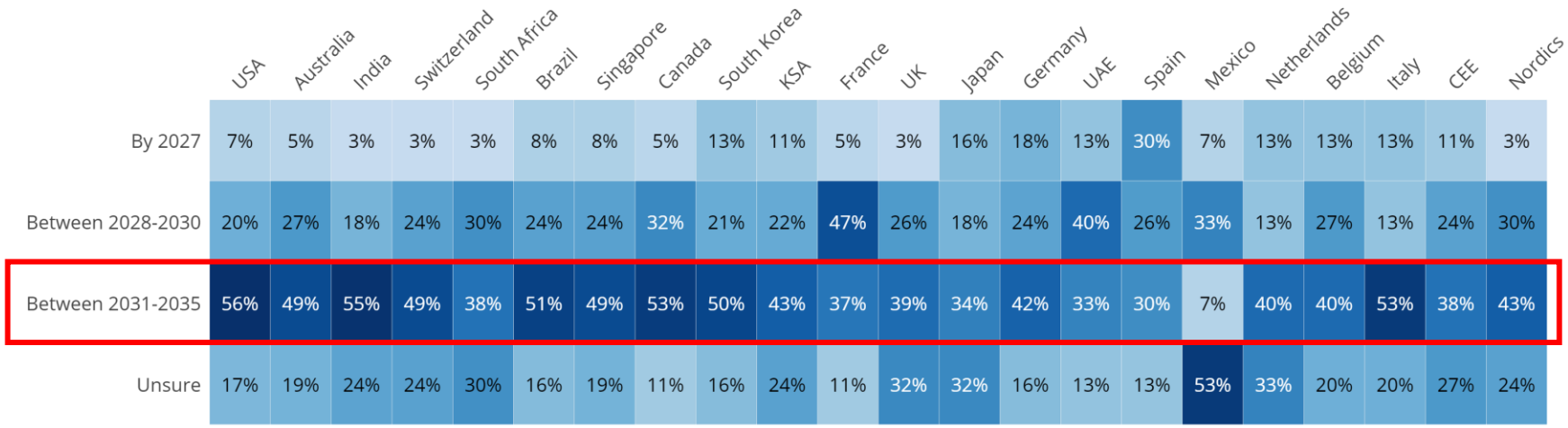
1. **Breaking Asymmetric Encryption:** Quantum computers can use algorithms like Shor's to quickly factorize large integers, rendering public-key encryption methods like RSA, ECC, and DH obsolete.
2. **Compromising Data Integrity:** Quantum computing could enable attackers to forge digital signatures, leading to the potential falsification of documents, transactions, and identity verification.
3. **Decrypting Sensitive Data:** Encrypted data intercepted today could be stored and decrypted when quantum computers become powerful enough, compromising long-term data confidentiality.
4. **Vulnerability in Blockchain Systems:** Many blockchain systems rely on cryptographic algorithms that are vulnerable to quantum attacks, potentially undermining the security and trust in blockchain-based technologies like cryptocurrencies.
5. **Security of IoT Devices:** IoT devices often use lightweight cryptography, which may not be designed to withstand quantum attacks, exposing entire networks to breaches.
6. **Weakening of Secure Communications:** Quantum computers could decrypt secure communications, such as HTTPS and VPNs, leading to a loss of privacy and safe internet usage.
7. **Disrupting Critical Infrastructure:** Government, healthcare, financial, and utility systems relying on traditional cryptography could become vulnerable to quantum-powered cyberattacks.
8. **Emergence of Quantum-Enabled Cyberattacks:** Adversaries with access to quantum technology could launch sophisticated attacks faster and more effectively than current security measures can handle.
9. **Global Security Implications:** Nations with advanced quantum capabilities could exploit vulnerabilities in less-prepared countries, leading to geopolitical risks and unbalanced power dynamics.

https://www.paloaltonetworks.com/cyberpedia/what-is-quantum-computings-threat-to-cybersecurity

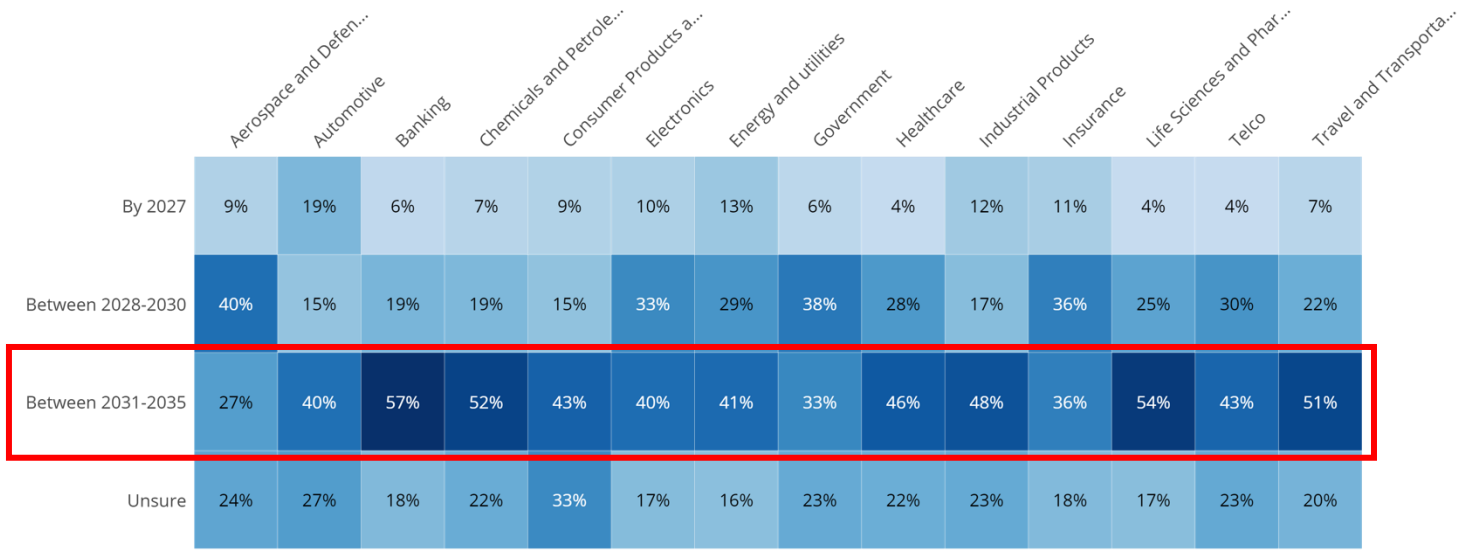
Insights from upcoming IBM IBV research

- 62% of respondents believe vendors will handle quantum-safe transition requirements.
- 56% continue to view quantum-safety as purely a technical issue (not a business & operations risk).

Q2A : When do you believe quantum advantage will be achieved in your industry?



Q2A : When do you believe quantum advantage will be achieved in your industry? by QCountry : Quota Country
sample size = 750



Q2A : When do you believe quantum advantage will be achieved in your industry? by D4 : What is your organization's primary industry?
sample size = 750

Where there is risk,
there is opportunity.

The intersection of physical and digital security

Situation -

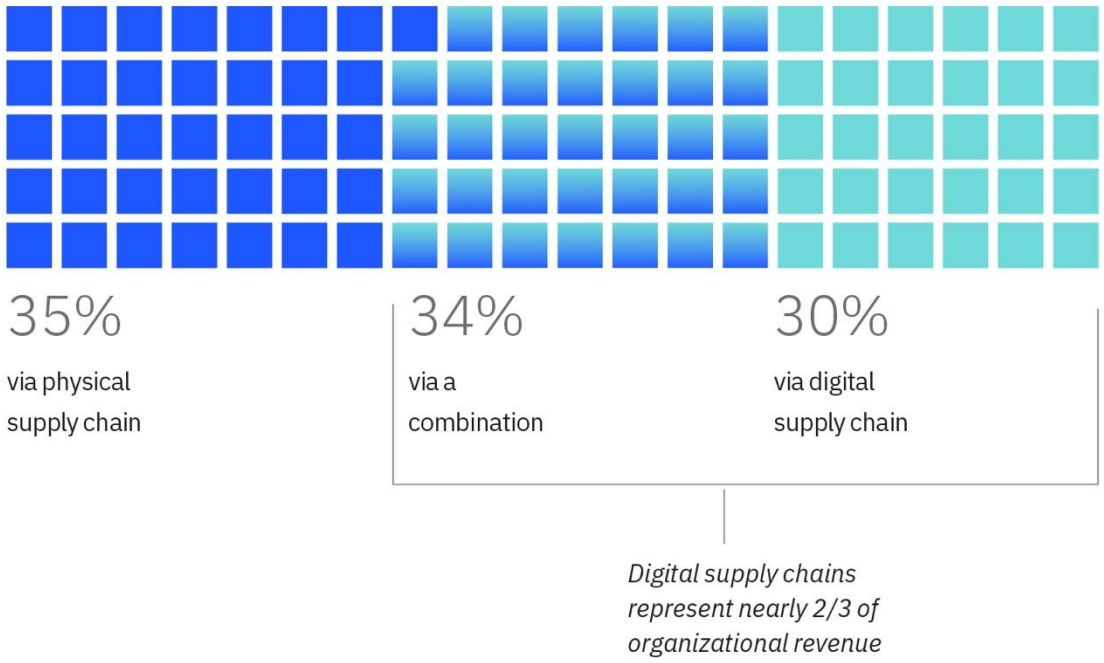
- Rapid changes in the operations environment
- Many physical security processes have digital dependencies or rely upon digital intermediation

Key questions –

1. How much of your current revenue is based on digital technologies? Think sensors, IoT devices, drones, AI, facial recognition.
2. Physical vs digital revenue mix? Think which services are driving growth?
3. How much visibility do you have into third-party (or n-party) risk? Think of your dependencies when delivering critical services or your work with external partners.

The majority of organizational revenue is now digital or digitally-intermediated.

Percentage of organizational revenue



Q. Estimate the proportion of your organization's revenue that is enabled and delivered as follows: via physical supply chains, via digital supply chains, and via a combination of physical and digital supply chains. 2023. Percentages do not equal 100% due to rounding.

Where are we today?

Quantum computing

Some orgs are investing now to build skills and to gain competitive advantage later.

- First out of the gate = Government, financial services, insurance
- Hybrid = Classical + quantum operations
- Technologies converge = Quantum AI

Quantum safe

All organizations are vulnerable, not just those pursuing quantum computing use cases.

- Retrospective decryption (aka “harvest now, decrypt later”)
- Time value of data – some industries rely on long-lifecycle assets (think passports, health records, contractual documents, critical safety records)

Short-term (now)	*Medium-term (5-7 years)*	*Long-term (8-10 years)*
Private security companies can focus on quantum-safe encryption and client advisory services.	Expect quantum computing applications in optimization and AI-driven surveillance.	Expect quantum computing-enabled forensics and intelligence analysis.

Potential applications of quantum computing

Private security companies face challenges in how they integrate technology and data into their core services, particularly in surveillance, data protection, threat detection, and predictive risk modeling.

Cybersecurity & Encryption

- Quantum-Safe Communications – Implementing or testing post-quantum cryptography to secure client data, surveillance feeds, and access control systems from future quantum attacks.
- Breaking Legacy Encryption (Red-Teaming) – Using quantum algorithms (like Shor's) in controlled environments to test the resilience of clients' security systems and accelerate vulnerability discovery.

Predictive Risk & Intelligence Gathering

- Behavioral Pattern Analysis – Quantum machine learning (QML) could process large-scale video surveillance, biometric, or access data to identify anomalous patterns faster than classical methods.
- Quantum-Assisted Intelligence Analysis - Solving complex graph-based problems (e.g., link analysis between suspicious actors).

Surveillance & Monitoring

- Enhanced Computer Vision – Applying QML to speed up image recognition for facial identification, object detection, or suspicious activity recognition in large surveillance networks.
- Signal Processing – Quantum algorithms could improve analysis of weak or noisy signals (e.g., audio surveillance, drone feeds, or radio frequencies).

Potential applications of quantum computing

Private security companies face challenges in how they integrate technology and data into their core services, particularly in surveillance, data protection, threat detection, and predictive risk modeling.

Operations & Logistics

- Patrol Optimization – Quantum optimization for route planning, camera / sensor placement, resource allocation, and response times for guard deployments, vehicle patrols, or drone fleets.
- Crowd management -- Optimizing mass movement of crowds in emergency response situations.

Simulations & Scenario Modeling

- Incident Response Simulation – Faster simulation of security breach scenarios (e.g., coordinated intrusions) to improve training and readiness.
- Advanced Threat Modeling – Using quantum-enhanced optimization (via quantum annealing or hybrid models) to simulate complex security scenarios, such as crowd control, incident response, or physical intrusions.
- Supply Chain Security – Modeling vulnerabilities in client logistics and facility operations by simulating complex interdependencies (quantum optimization of weakest links).

Strategic Services

- Data Forensics – Quantum algorithms could accelerate the reconstruction or analysis of corrupted/encrypted digital evidence for investigations.
- Secure Client Services – Offering “quantum-resilient” consulting to high-value clients (e.g., banks, critical infrastructure, VIPs) as a premium differentiator.
- Quantum Key Distribution (QKD) - Offering secure communications via Quantum Key Distribution (QKD-enabled networks for VIP or sensitive operations).

A future-focused case study –
Major sporting events / Public venues

Key challenges

- Complex environment with many signals. The ability to listen and integrate signals intelligence with internal and external command and control functions is critical.
- Situational awareness - Ability to work in parallel with other providers and entities from multiple jurisdictions
- Venue integration – facilities, logistics, public services

Key requirements

Threat monitoring

- Physical threats
- Hybrid physical + digital threats
  (who owns?, how are signals collated?)

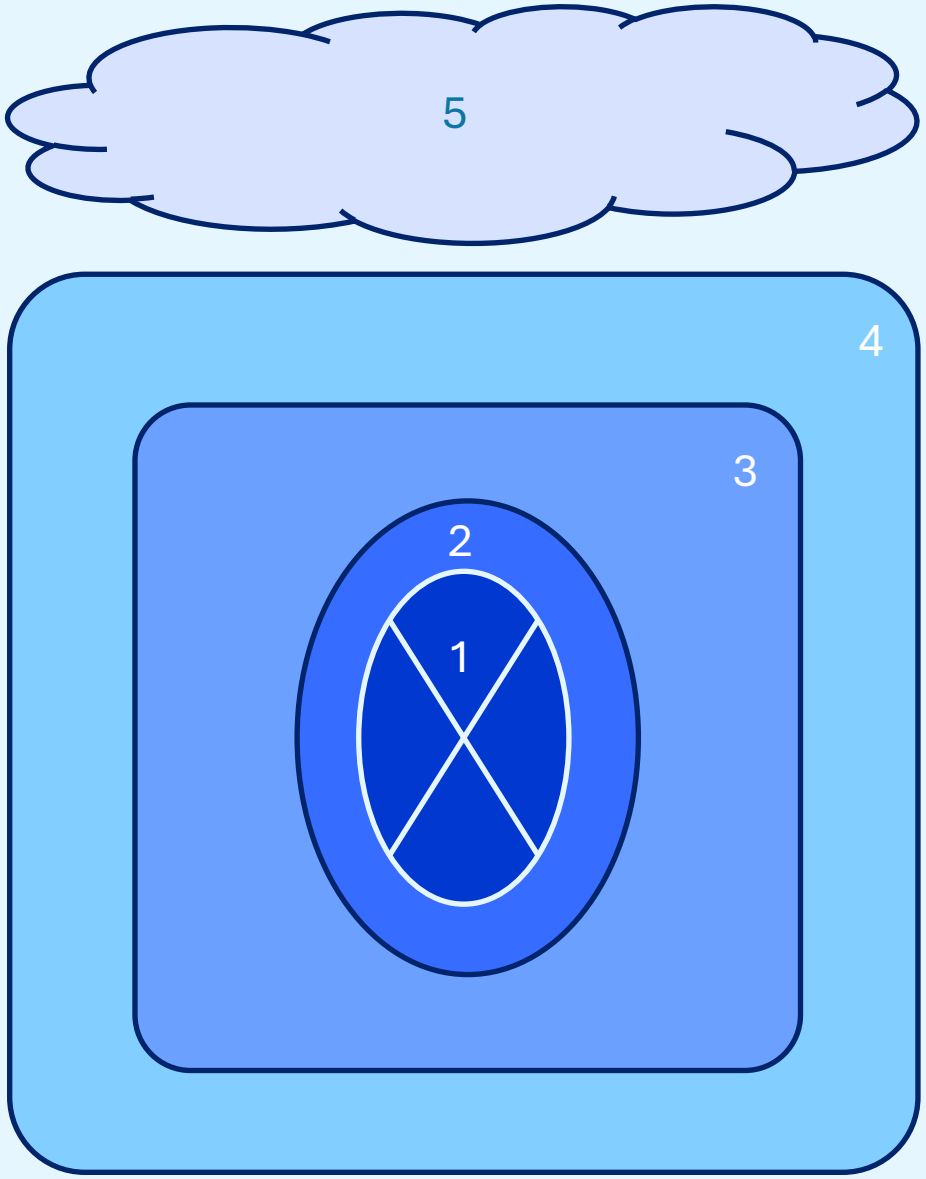
Crowd management / routing / pathing

- Digital identity & entitlement verification
- Public notifications

Security posture management

- Risk management — disaster planning, business continuity, operational resilience services
- Incident response (steady state)
- Emergency response (life & death)

The event footprint



Potential attack surface

1. Inside the venue (which quadrant?)
2. Venue interior/exterior support (which entrances / exits, services, facilities, logistics?)
3. Transit integration / parking (which streets, stations?)
4. Surrounding neighborhood / community (what infrastructure?)
5. Online / digital / virtual presence (how integrated?)

Key considerations

As a prime vendor or subcontractor, how well do you integrate to…?

1. Event security / infrastructure
2. Venue security / infrastructure
3. Team security / infrastructure
4. Community security / infrastructure
5. Centralized operations center / incident response infrastructure
6. Crisis / emergency management infrastructure

For these jurisdictions…

1. Metro
2. County
3. State
4. Federal

2025–2030: What a quantum security roadmap might look like for the private security industry

Phase 1: Awareness & Readiness (2025–2026)

Goal: Build internal knowledge, assess client risk, and prepare foundational offerings.

Strategic Actions:

- **Train Leadership & Technical Staff**
  - Quantum fundamentals, post-quantum cryptography (PQC), quantum threat landscape.
- **Assess Cryptographic Exposure**
  - Inventory clients' crypto assets and communication protocols.
  - Identify "store-now, decrypt-later" vulnerabilities.
- **Build Vendor Partnerships**
  - Engage with quantum tech vendors (e.g., IBM Q, D-Wave, QuSecure).
- **Offer Quantum Readiness Assessments**
  - Evaluate client posture for post-quantum threats.
  - Provide reports on QKD feasibility and PQC adoption plans.

Sample Services to Launch:

- "Quantum Risk Snapshot"
- PQC Migration Roadmaps
- Executive Briefings on Quantum Threats

Phase 2: Capability Development (2026–2028)

Goal: Build and integrate early quantum-enabled services.

Strategic Actions:

- **Prototype Use Cases**
  - Quantum optimization for route planning or surveillance deployment.
  - Use hybrid quantum-classical ML for anomaly detection.
- **Implement Quantum-Safe Architectures**
  - Test PQC in VPNs, secure email, and endpoint comms.
  - Integrate NIST-approved PQ algorithms into security stacks.
- **Offer Quantum-Enhanced Analytics**
  - Use quantum algorithms to accelerate client data analysis.
- **Develop Secure Comms Solutions**
  - Pilot QKD-based secure communication with key clients.

Technologies to Monitor:

- IBM Qiskit / Azure Quantum / D-Wave systems
- PQC libraries (e.g., CRYSTALS-Kyber, Falcon)
- Quantum-safe VPNs or messaging (e.g., ISARA, PQShield)

2025–2030: What a quantum security roadmap might look like for the private security industry

Phase 3: Monetization & Differentiation (2028–2030+)

Goal: Deliver premium quantum-enabled services and scale leadership.

Strategic Actions:

- **Launch Managed Quantum Security Services**
  - Quantum-resilient SOC operations.
  - Encrypted VIP communications using PQC/QKD.
- **License Quantum ML Engines**
  - As part of proprietary threat intelligence platforms.
- **Offer Regulatory Compliance Services**
  - Support clients in complying with quantum-security standards.
- **Establish a "Quantum Security Lab"**
  - R&D hub for custom client simulations, PQ migration testing, and threat research.

Premium Services:

- Quantum Threat Intelligence-as-a-Service
- Quantum-Assisted Risk Modeling for Executives
- Quantum Vault (secure client data storage & retrieval)

Make the world quantum safe

2025 IBM Quantum Safe POV

Launching @ IBM TechXchange - Oct 6-9, 2025

https://www.ibm.com/quantum/quantum-safe

https://www.ibm.com/ibv

International SecurityLigue

39th General Assembly 2025

Alper Cetingok
Moderator

Mark Mullison
CIO Allied Universal

Manjit Rajain
Chairman Tenon Group

Gerry Parham
IBM Institute for Business Value

Quantum Computing & Implications to private Security Industry Panel Discussion and Q&A

10:30 – 11:30