AI Security a Post-Quantum Cryptography:

Budoucnost kybernetické bezpečnosti

Dominik Turan, GVSE Solutions Engineer

04-23-2026

Agenda

1. Vliv AI na bezpečnost a síť
2. Vliv kvantových počítačů na bezpečnost

Security fused into the network

Securing users, clients & apps

Protecting user access and application interactions

- Hypershield-ready
- Scalable segmentation
- Software-Defined Access
- Security Group Tags
- UZTNA
- AI device classification
- Common policy
- Next-gen firewall

Securing network connectivity

Safeguarding and optimizing network connections

- Quantum-resistant:
  - MACsec
  - IPsec
  - WAN MACsec

Securing the device

Protecting and ensuring compliance of devices

- Quantum-resistant secure boot
- Compensating controls

Zero Trust Capabilities

Policy & Governance

- Change Control
- Data Governance Policy + Encryption
- Data Retention Policy
- QoS
- Redundancy / Replication
- Business Continuity
- Disaster Recovery
- Risk Classification Policy
- Segmentation

Identity

- AAA
- Certificate Authority
- NAC
- Provisioning
- Privileged Access
- MFA
- Asset Identity
- Configuration (CMDB)
- IP Schemas

Vulnerability Management

- Endpoint Protection
- Malware Prevention and Inspection
- Vulnerability Management
- Authenticated Vulnerability Scanning
- Database Change

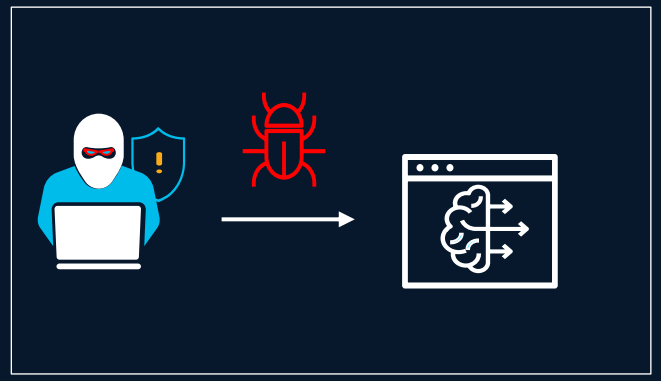
Enforcement

- CASB
- DDoS
- DLP
- DNS Security
- Email Security
- Firewall
- IPS
- Proxy
- VPN / RA
- SOAR
- File Integrity Monitor
- Segmentation

Analytics

- App. Performance Monitoring
- Audit, Logging, and Monitoring
- Change Detection
- Network Threat Behavior Analytics
- SIEM
- Threat Intelligence
- Traffic Visibility
- Asset Monitoring & Discovery

From Theory to Practice: AI-related Threats

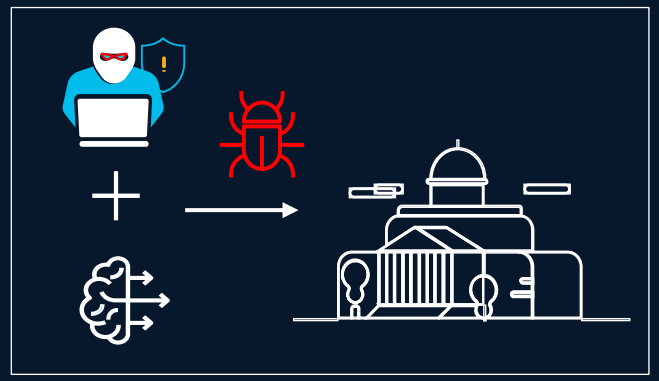


Adversarial ML/Security of AI:
Identifying vulnerabilities within AI models, and systems

First research evidence:
Evasion of Machine Learning driven Spam Filters (2004)

New Malware Spotted in The Wild Using Prompt Injection to Manipulate AI Models Processing Sample

Source: https://cybersecuritynews.com



Offensive AI: Using AI to drive attacks against different types of targets, e.g., organizations

First research evidence:
Using AI for CAPTCHA cracking (2008)

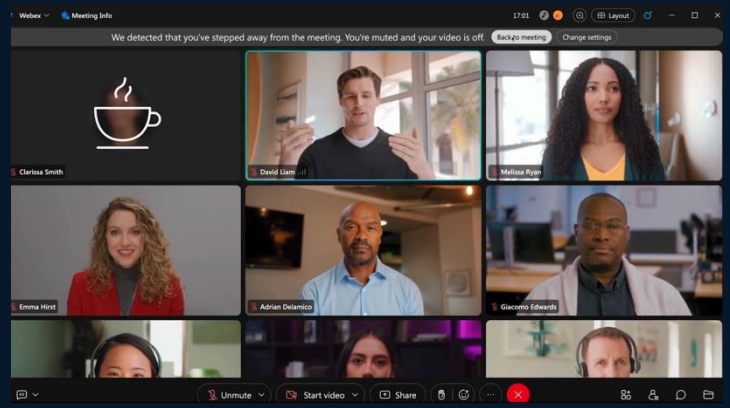
Disrupting the first reported AI-orchestrated cyber espionage campaign

13. Nov. 2025

Source: https://www.anthropic.com/news

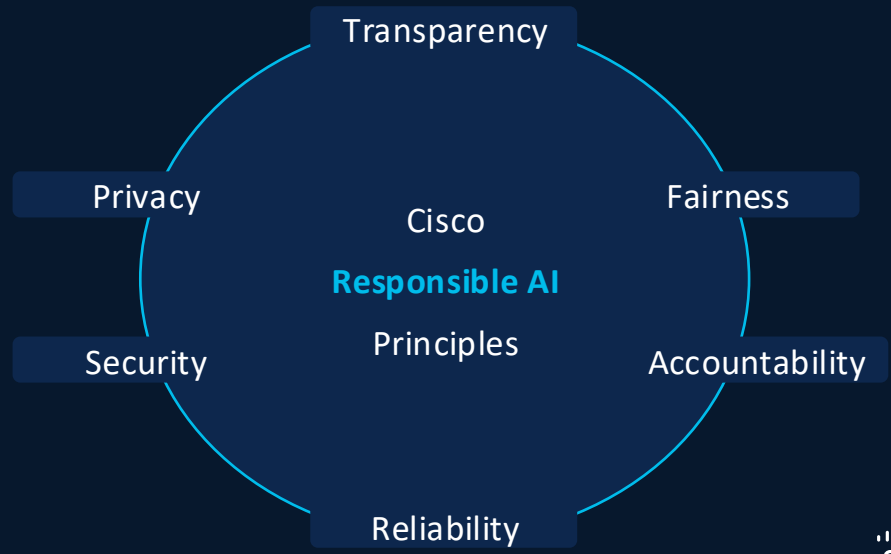
AI for networks – where is it helping ?

- ***Cyber Security*** - (Assist, Detect, Control, Encrypted traffic,…)
- ***Networking*** - (Assist, Manage, Optimize RRM in WiFi, Control, …)
- ***Observability*** - (Baseline, Anomaly detection, RCA, Mitigation steps proposal,…)
- ***Industrial IoT*** - (Preventive maintenance,…)
- ***Physical Security*** - (Camera – Image analysis, Object recognition, Search,…)
- ***Collaboration*** - (LLM x **RMM**, WEBEX AICodec, Summarization, Knowledge bots ,…)



Networks for AI (learning)

- ***SLM*** - Standard networking
- ***LLM*** – New loss-less low latency fabrics
  - Simplified stack & specific protocols



A new lineup for AgenticOps

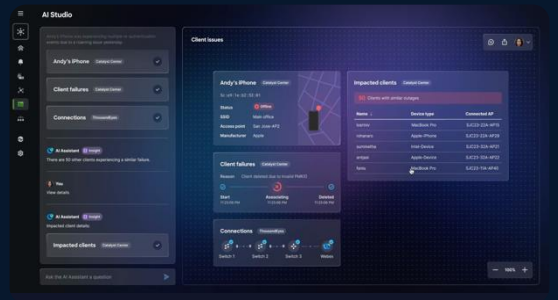
PUBLIC BETA
NEW CAPABILITIES

cisco AI Assistant

AI Assistant

Accelerate network operations

NEW



AI Canvas

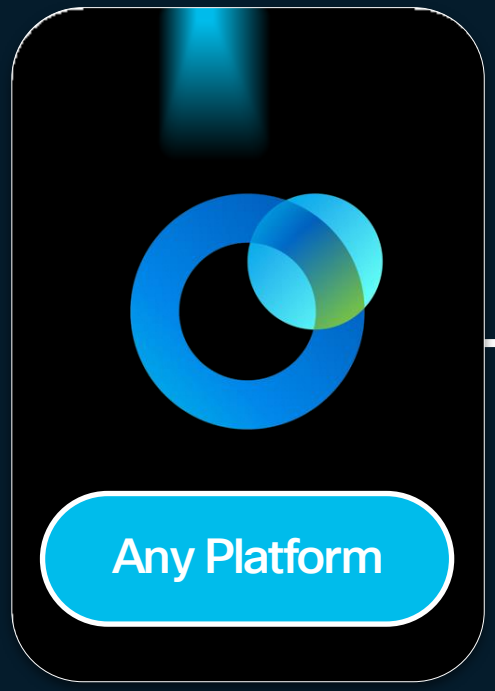
Cross-domain collaborative troubleshooting

POWERED BY EXPERT AI MODEL*

Cross-Platform Correlation for Troubleshooting

Correlate Data Across All Platforms

Originating Platform



All Platforms

Firewall
Security & connection events

Duo
Authentication & compliance

Secure Access
Private & SAAS Resource Access

Identity Intelligence
User trust level, identity checks & reasons

ISE
Authentication Insights

XDR
Related Threat Incidents

Cisco Meraki
Topology, client details, location, etc.

ThousandEyes
WAN, Internet, App Insights

Catalyst Center
Topology, client details, location, etc.

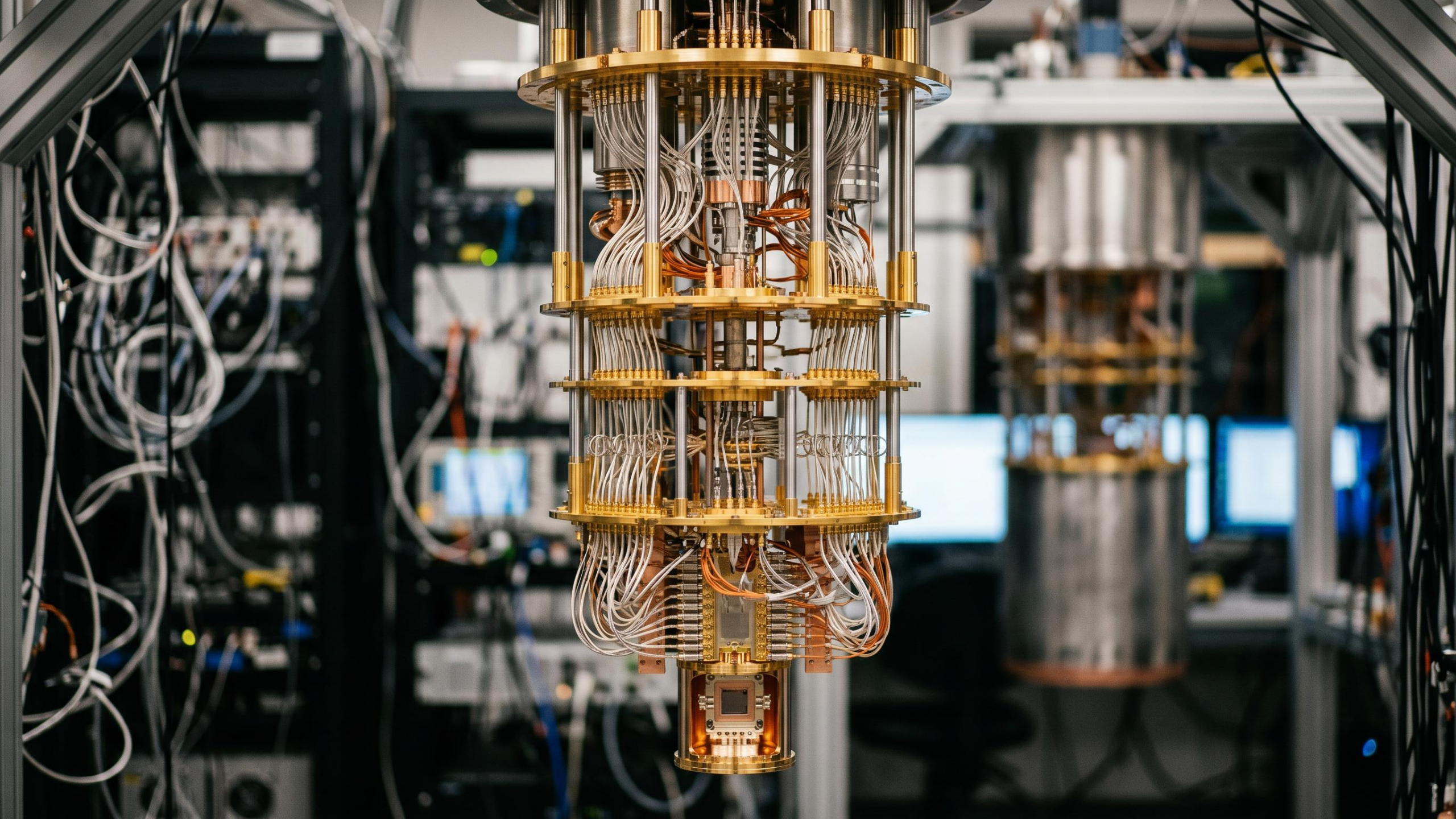
SD-WAN
WAN Details

splunk>
Third-Party platform insights

webex
Voice and video experience

Cross-Platform Troubleshooting

Troubleshooting Clients, Devices, & Apps Often Requires Data From Multiple Platforms



People are making incremental efforts in developing a

Quantum Computer.

Once they have one which is sufficiently large and reliable,
they could use it to

Break Current Encryption!

(public key algorithms)

From Theory to Practice: Quantum Computing

- **In 1994 the** Mathematician Shor published a quantum algorithm that solves the underlying mathematical problems of today's asymmetric key algorithms

- Significant threat to asymmetric key algorithms (RSA, Diffie-Hellman, ECC)

Harvest Now, Decrypt Later!

Algorithms for Quantum Computation:
Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)

1 Introduction

Since the discovery of quantum mechanics, people have found the behavior of the laws of probability in quantum mechanics counterintuitive. Because of this behavior, quantum mechanical phenomena behave quite differently than the phenomena of classical physics that we are used to. Feynman seems to have been the first to ask what effect this has on computation [13, 14]. He gave arguments as to why this behavior might make it intrinsically computationally expensive to simulate quantum mechanics on a classical (or von Neumann) computer. He also suggested the possibility of using a computer based on quantum mechanical principles to avoid this problem, thus implicitly asking the converse question: by using quantum mechanics in a computer can you compute more efficiently than on a classical computer. Other early work in the field of quantum mechanics and computing was done by Benioff [1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as efficient when the number of steps of the algorithms grows as a polynomial in the size of the input. The class of problems which can be solved by efficient algorithms is known as P. This classification has several nice properties. For one thing, it does a reasonable job of reflecting the performance of algorithms in practice (although an algorithm whose running time is the tenth power of the input size, say, is not truly efficient). For another, this classification is nice theoretically, as different reasonable machine models produce the same class P. We will see this behavior reappear in quantum computation, where different models for quantum machines will vary in running times by no more than polynomial factors.

There are also other computational complexity classes discussed in this paper. One of these is PSPACE, which are those problems which can be solved with an amount of memory polynomial in the input size. Another important complexity class is NP, which intuitively is the class of exponential search problems. These are problems which may require the search of an exponential size space to find

Source: Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th symposium on foundations of computer science*. IEEE.

What is Quantum Computing?

Quantum computing uses special units called **quantum bits (qubit)** that can be in multiple states at once. This allows quantum computers to process information much faster and solve complex problems that regular computers cannot handle.

Superposition (of qubits)

classical
0100110101

quantum
$$p_0 0000000000 + p_1 0000000001 + p_2 0000000010 \cdots + p_{2^N} 1111111111$$

Entanglement

We know the state of the system, not the individual pieces

Source: https://newsroom.ibm.com/media-quantum-innovation

Let's get the concepts right: Quantum...

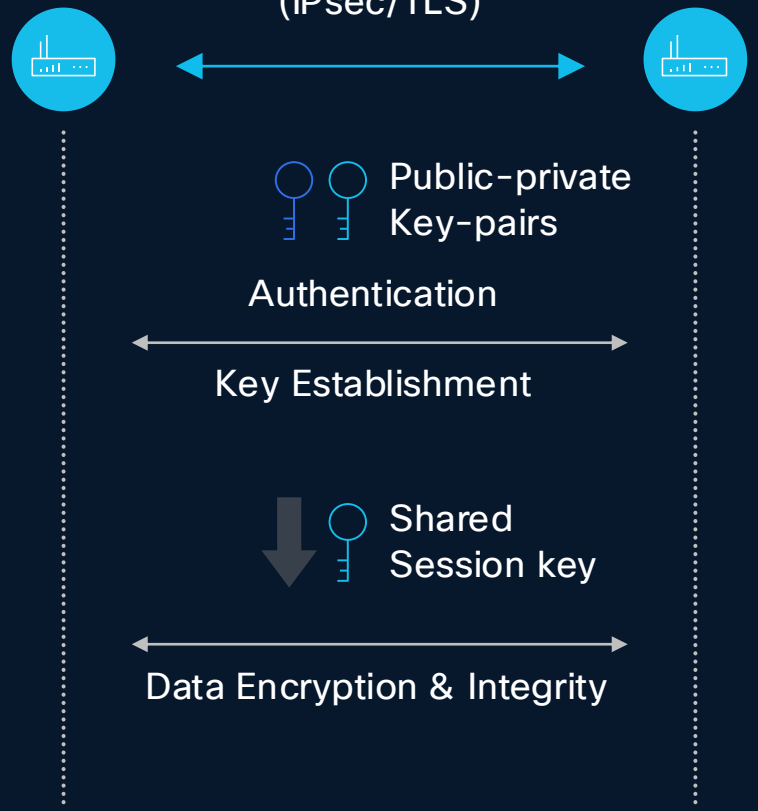
Quantum Computer
Powerful computer, based on quantum mechanics, allowing parallel processing and super fast execution of certain problems.

Quantum Networking
A network that connects quantum computers securely, connecting multiple quantum processors for increased computational power and efficiency.

Post-Quantum Cryptography
Cryptographic algorithms designed to be secure against quantum computer attacks.

Quantum Key Distribution (QKD)
Uses quantum mechanics to securely exchange encryption keys between two or more elements.

Quantum computing's impact on cryptography



Quantum-Resistant?

Asymmetric Cryptography

- Based on mathematically related public-private key-pairs
- Used for control plane operations
  - Authentication, Key establishment
- Example: RSA, DH, ECC

Large reliable Quantum computers can break RSA, DH, ECC!

Symmetric Cryptography

- Based on shared key
- Used for bulk data encryption & integrity
- Protection level based on key strength
  - Key size & entropy
- Example: AES-GCM

Symmetric crypto with large and high-entropy keys is resistant to Quantum computer attacks

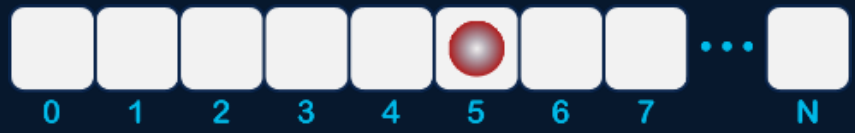
Today internet security relies on hard mathematical problems – Quantum Changes the Rules

Classical		Quantum Computers
RSA / ECC / DH	Today's **public-key cryptography** assumes: • Factoring large numbers is computationally infeasible • Solving discrete logarithms is infeasible	**Shor's Algorithm** **Efficiently factors large integers**
AES / SHA-256 / HMAC	Today's **symmetric cryptography** assumes: • Brute-force search requires exponential time • Ex. 128-bit security means ~2^{128} operations • Hash collision resistance grows exponentially	**Grover's Algorithm** **Quadratically speeds up brute force search** Reduces effective key strength (e.g., 128-bit - 64-bit)

Security-Concerning Quantum Algorithms

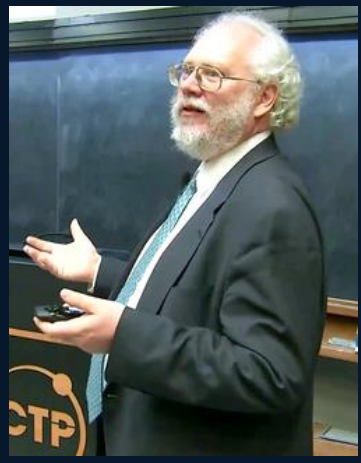
Grover's Algorithm

- searches an unstructured database (or an unordered list) for a specific result
- Exhibits **quadratic** speed-up vs. digital (classical compute)
- theoretically threatens **symmetric** key algorithms, such as the Advanced Encryption Standard (AES)



Shor's Algorithm:

- factorizes large numbers
- Exhibits **exponential** speed up over digital
- theoretically threatens the security of asymmetric key algorithms, such as the classical Public Key Infrastructure (PKI) including:
  - Diffie-Hellman (DH)
  - Elliptic Curve Cryptography (ECC), and
  - Elliptic Curve Diffie Hellman (ECDH)



Quantum Speed-Up

Well-designed quantum circuits can perform operations maximize quantum advantages and can thus exhibit significant speed-ups, as compared to their digital counterparts

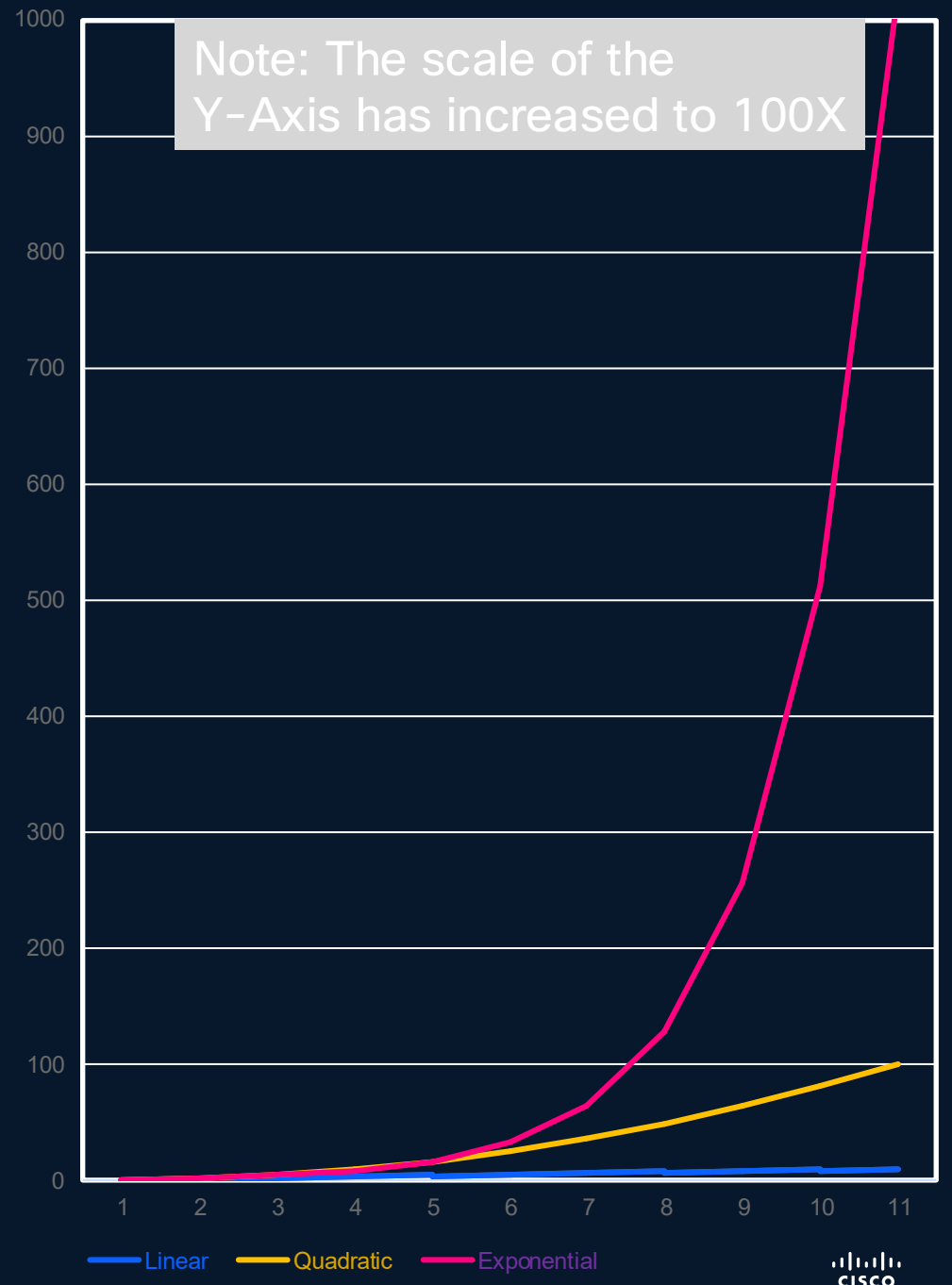
Speed-ups may be:

- **Linear**
- **Quadratic**
- **Exponential**

Linear
$y=x$

Quadratic
$y=x^2$

Exponential
$y=2^x$



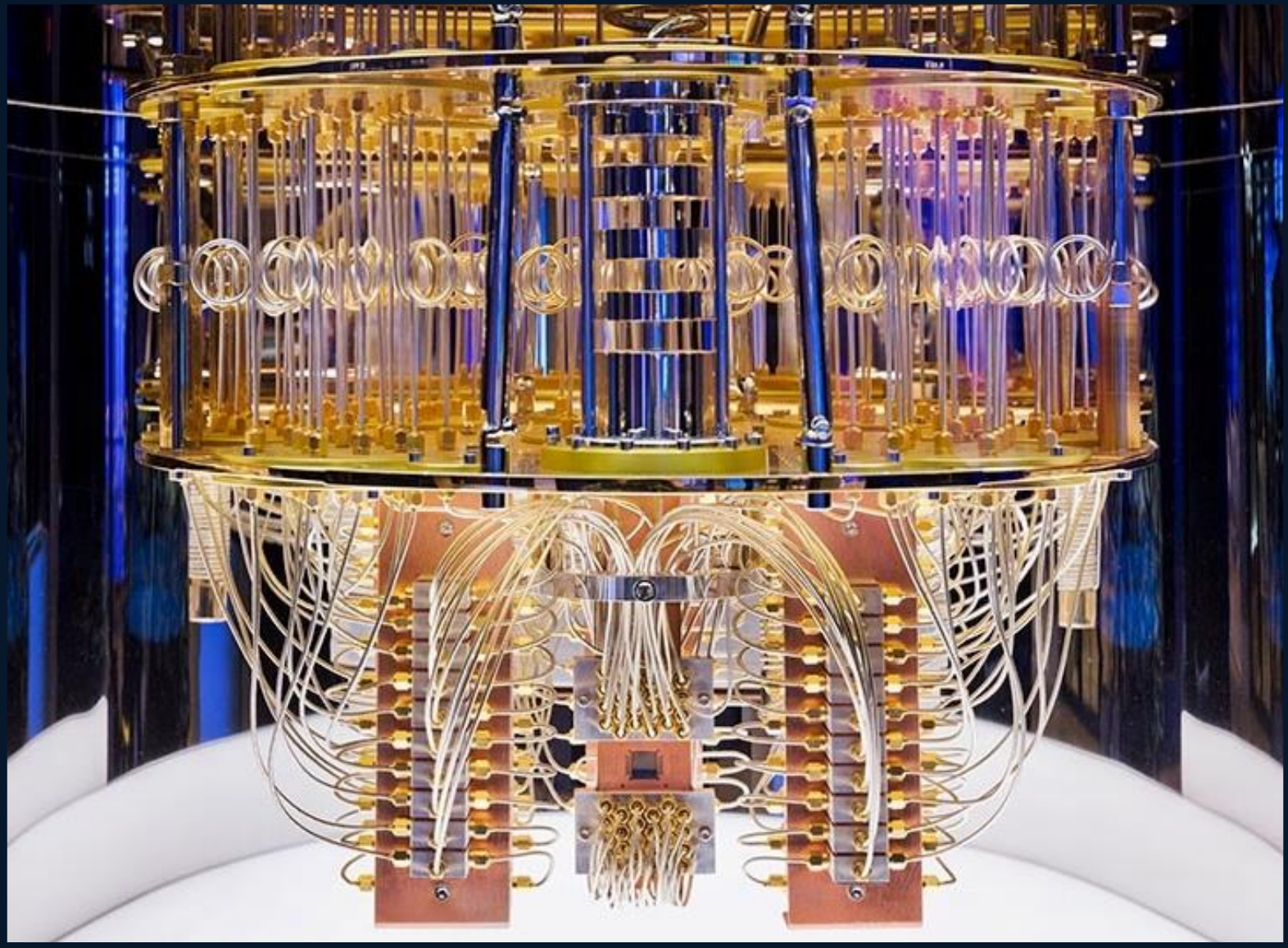
How Much Faster is a Quantum Computer?

In 2021, the world's largest quantum computer had 127 qubits

This machine was 158M times faster than its classic counterpart

Example Task Execution Times:

- Classic Computer: 2,500 years
- Quantum Computer: 1 minute



$2^{127} = 1.7 \times 10^{38}$ values

170,000,000,000,000,000,000,000,000,000,000,000

Themes of the post-quantum threat

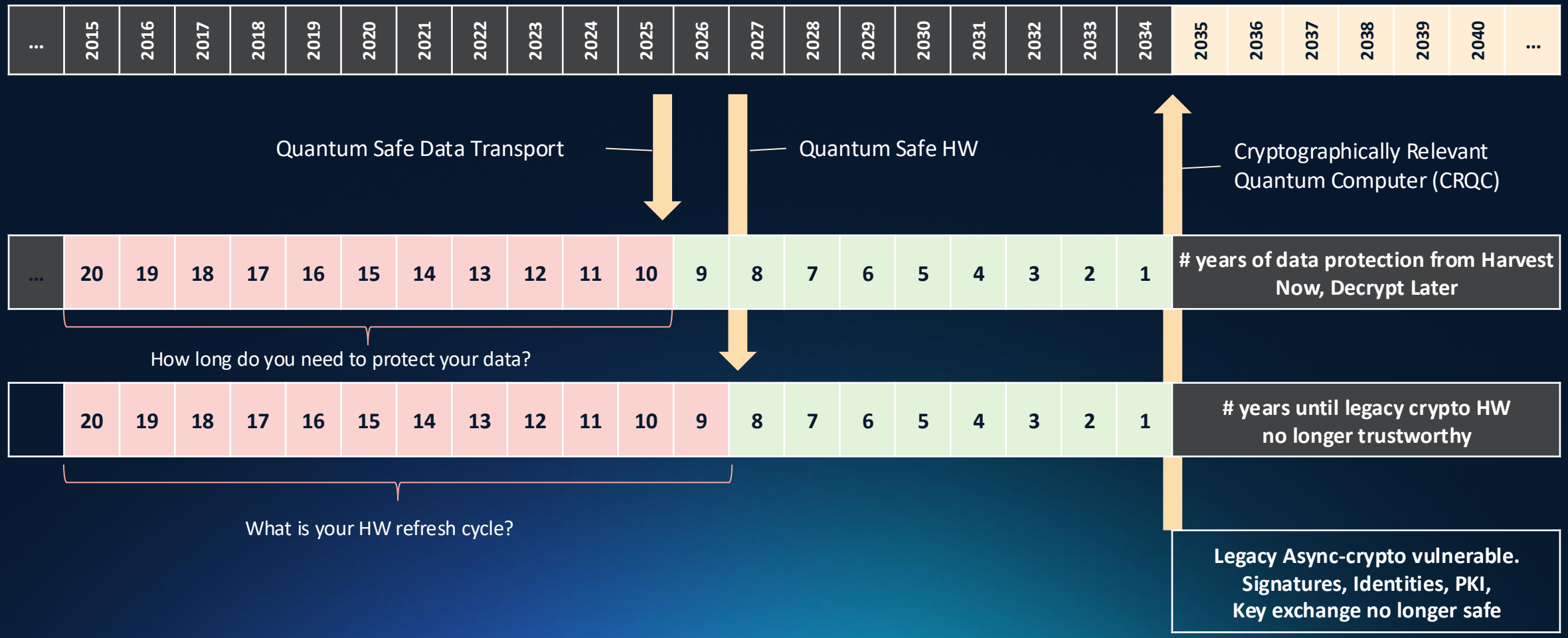
Software signing and verification

Identity

Transport / Key Exchange

Why Worry Now?

Time is of essence to address the current problem: “Harvest Now, Decrypt Later”



With Y2K we knew when but didn’t know what would happen…

With quantum we know what will happen, but don’t know when…

Preparing for Quantum Computing Security Threats

Hybrid: Combination of traditional cryptographic and PQC algorithms.


CISCO