

Role of AI and Quantum Technologies for Cybersecurity

From Intelligent Defence to Quantum-Resilient Security

Dr Deepak Mishra
Professor



Q-ENTANGLE 2026

INDIAN INSTITUTE OF SPACE SCIENCE AND TECHNOLOGY
THIRUVANANTHAPURAM, KERALA, INDIA 695547

September 9, 2026



- 1 Motivation and Evolution
- 2 Artificial Intelligence in Cybersecurity
- 3 Quantum Technologies and Cybersecurity
- 4 Quantum Threat to Cybersecurity
- 5 Post-Quantum Cryptography
- 6 Quantum Technologies for Security
- 7 AI + Quantum Convergence
- 8 Current Trends and Challenges
- 9 Future Outlook and Conclusion
- 10 References

Questions This Seminar Addresses



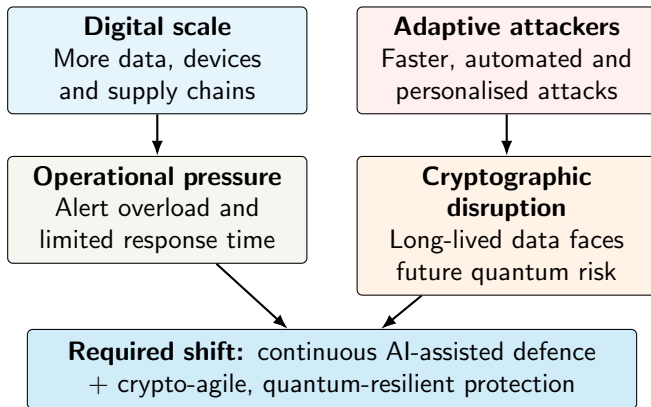
- 1 How is **artificial intelligence** changing both cyber defence and cyber attacks?
- 2 Why does **quantum computing** threaten widely used public-key cryptography?
- 3 How can organisations combine **AI, post-quantum cryptography and quantum technologies** to build resilient security systems?

Seminar focus

From intelligent threat detection to practical quantum-safe migration.

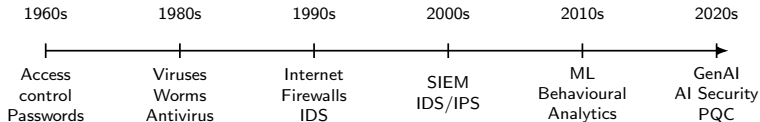


Why Cybersecurity Is Changing





Evolution of Cybersecurity

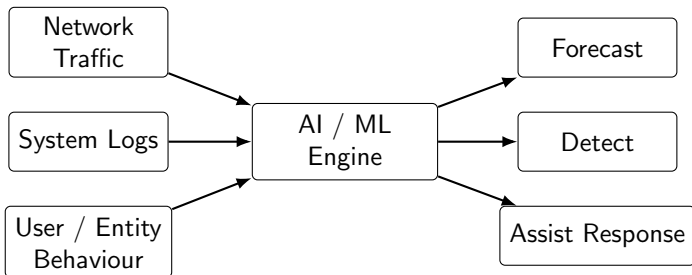


Key transition

Security evolved from rule- and signature-based protection toward **adaptive, data-driven defence**; quantum computing now adds a second strategic challenge: **cryptographic resilience**.



AI in Cybersecurity: The Basic Architecture



What the outputs mean

Detect: flag unusual events already observed.

Forecast: estimate expected future behaviour, not certain attacks.

Respond: automate routine tasks; govern high-impact actions.



Major AI Applications

Detection

- Malware classification
- Time-series anomaly detection
- Intrusion detection
- Phishing / fraud detection

Operations

- Alert prioritisation
- Threat intelligence summarisation
- Incident triage
- Automated response assistance

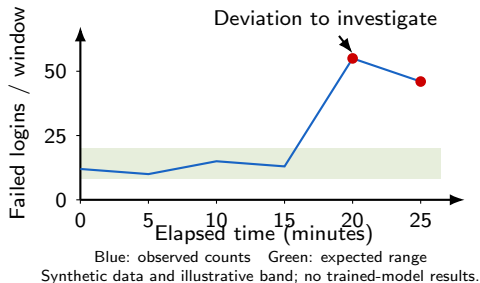
Emerging role of Generative AI

LLMs can assist analysts with log interpretation, threat-intelligence synthesis, natural-language queries and security workflow automation.



AI-Based Time-Series Anomaly Detection

Illustrative scenario: monitor failed logins in five-minute windows.



How AI could help

1. **Learn** expected behaviour from earlier observations.
2. **Compare** new counts with the forecast; score deviations.
3. **Investigate** possible brute-force activity or benign causes.

From alert to governed response

Automate: enrich the alert and open an investigation ticket.

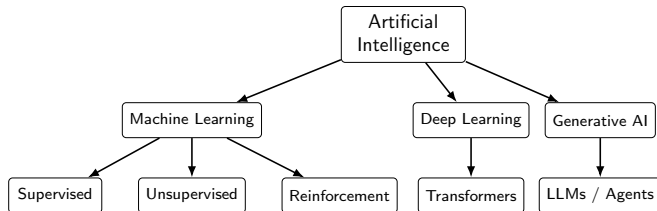
Require approval: high-impact containment, such as disabling an account.

Key point: forecasting estimates expected behaviour; anomaly detection flags deviations. An anomaly is not proof of an attack.

Sources: Method background: Hundman et al., KDD (2018). [1] Spacecraft telemetry study; the login example is illustrative.



AI Techniques Used in Security



- **Supervised learning:** learn from labelled examples; classify files as malware or benign.
- **Unsupervised learning:** discover patterns without attack labels; flag unusual network or login behaviour.
- **Reinforcement learning:** learn actions through rewards; explore response policies in controlled simulations.
- **Deep learning:** learn complex patterns in data; analyse sequences of security events.
- **Generative AI:** produce text and explanations; summarise alerts and assist analysts, with verification.

Note: these categories overlap; deep learning is part of ML.



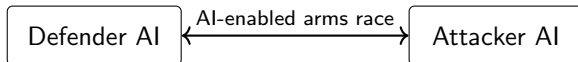
AI: Defender and Attacker

AI as Defender

- Detect abnormal behaviour
- Correlate events across systems
- Prioritise incidents
- Assist response and recovery

AI as Attacker

- Scalable phishing and impersonation
- Automated reconnaissance
- Malware and exploit assistance
- Adaptive social engineering



[2, 3]



Case Study: AI-Enabled Phishing

Observed trend

By early 2025, AI-supported phishing campaigns reportedly represented **more than 80%** of observed social-engineering activity worldwide.

Traditional phishing

Manual message creation



Limited personalisation

AI

AI-enabled amplification

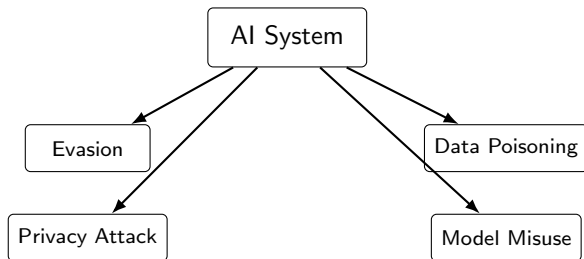
- Automatic generation
- Personalisation
- Translation
- Impersonation and synthetic media
- Campaign scalability

Why it matters: AI reduces the effort required to produce convincing, targeted messages at scale.

Sources: ENISA, *Threat Landscape 2025*, Executive Summary, p. 6; AI discussion, pp. 14–15. [3]



Security Risks of AI Systems



- AI introduces new attack surfaces across data, training, models and inference.
- Security depends on robustness, provenance, monitoring and secure deployment.

[2]



Why Quantum Computing Matters

Classical bit

0 or 1

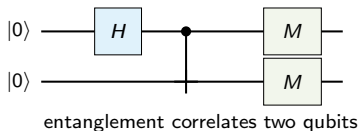
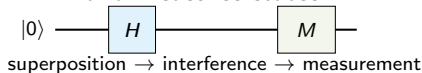
Qubit

A quantum state can be represented as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

A quantum circuit creates and measures states

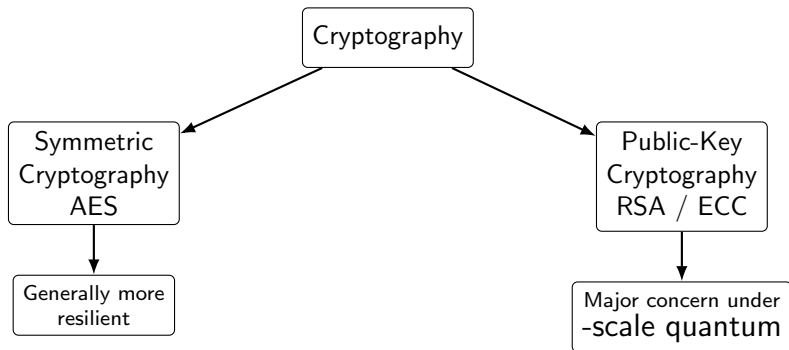


Security relevance

Certain quantum algorithms can change the computational difficulty underlying widely deployed public-key cryptography.



Cryptography Today: Where Is the Quantum Risk?

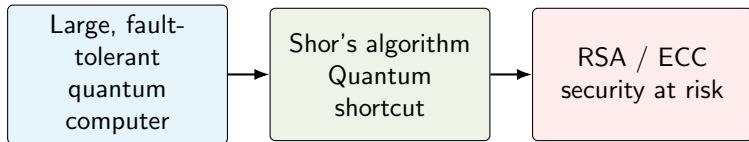


Key point

Quantum threat is **algorithm-specific**: it is especially serious for public-key schemes based on factoring or discrete-logarithm assumptions.



Shor's Algorithm: The Security Risk



- **RSA's idea:** multiplying large primes is easy; recovering them from the product is intended to be hard.
- **What Shor changes:** quantum algorithms efficiently solve factoring and discrete logarithms, undermining RSA and ECC.

Takeaway

This is a threat to specific public-key systems, **not all encryption**. Practical attacks require sufficiently capable quantum hardware.

Sources: P. W. Shor, FOCS (1994), pp. 124–134. [4]



Shor's Algorithm: A Toy Example ($15 = 3 \times 5$)

Goal: find the factors of $N = 15$. Choose $a = 2$ (no common factor with 15).

1. Find the period

Compute powers of 2; keep the **remainder after dividing by 15**.

Power x	0	1	2	3	4
2^x	1	2	4	8	16
Remainder	1	2	4	8	1

The sequence 1, 2, 4, 8 repeats: its **period is $r = 4$** .

2. Recover the factors

Half the period is 2, so $2^2 = 4$.

Find the greatest common divisors:

$$\gcd(4 - 1, 15) = \boxed{3}$$

$$\gcd(4 + 1, 15) = \boxed{5}$$

Check: $3 \times 5 = 15$.

This final step is classical arithmetic.

Where is the quantum part? Quantum order finding helps recover the period; a classical computer extracts the factors. Runs may need repeating.

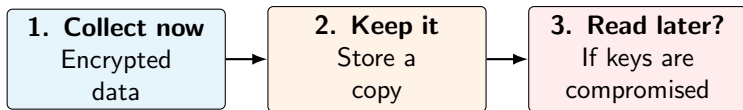
Toy example only: the table explains the pattern, not a quantum speedup.

Sources: IBM Quantum, *Shor's algorithm*, factoring $N = 15$ [5]; Shor (1994) [4].



Harvest Now, Decrypt Later

The concern: stolen data can remain valuable long after it is collected.



Illustrative example: long-lived mission data

A mission record must stay confidential for 20 years. If its key protection is broken during that period, an intercepted copy may become readable.

Why prepare before the quantum computer arrives?

Prioritise long-lived secrets and migrate vulnerable cryptography early. Today's intercepted copies cannot be recalled later.

Sources: NIST, first PQC standards announcement (2024). [6]



Post-Quantum Cryptography (PQC)



Definition

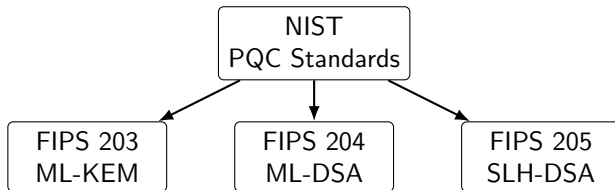
PQC uses classical cryptographic algorithms designed to remain secure against both classical and future quantum attacks.

Important distinction

PQC is not the same as quantum cryptography. PQC can run on conventional computing and networks; QKD uses quantum communication principles.



NIST's First PQC Standards



- **FIPS 203 / ML-KEM**: key establishment
- **FIPS 204 / ML-DSA**: digital signatures
- **FIPS 205 / SLH-DSA**: hash-based digital signatures

Current status

NIST approved the first three PQC standards on 13 August 2024 and selected HQC for standardisation on 11 March 2025.

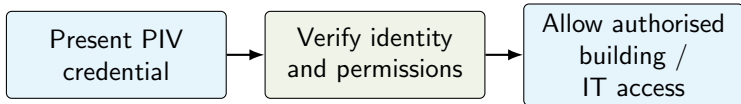
Sources: NIST, approval of FIPS 203, 204 and 205 (13 Aug. 2024). [6]
NIST Post-Quantum Cryptography project (HQC selection). [7]



PIV: An Identity Card Preparing for PQC

What is PIV, and where is it used?

Personal Identity Verification (PIV) is a US federal identity credential for employees and contractors. It is used to verify identity for access to **government buildings, IT systems and applications**.



Why does quantum-safe migration matter?

Protect identity: the credential relies on cryptographic keys.

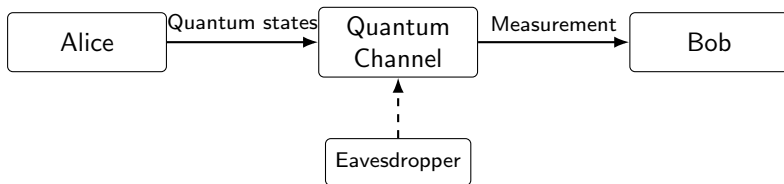
Upgrade gradually: NIST's 12 June 2026 proposal adds PQC alongside existing keys so older systems can still work.

Status: preliminary working materials, not a final PQC-PIV standard.

Sources: NIST, PIV overview [8]; PQC updates to PIV, working drafts (12 June 2026) [9].



Quantum Key Distribution (QKD)



Core idea

Quantum states cannot be measured or copied arbitrarily without disturbing them. In QKD, this property can reveal eavesdropping during key establishment.

[10]



PQC vs QKD: Different Roles

PQC changes the algorithms; QKD changes how keys are shared.

Question	PQC	QKD
How?	Quantum-resistant mathematical algorithms	Quantum signals share secret keys
What for?	Key establishment; digital signatures	Key distribution, not data encryption itself
Needs?	Conventional computers with upgraded software / hardware	Optical hardware and links; authenticated classical channel
Example	Server connections; software signatures	Optical key-sharing link between two equipped sites

Practical takeaway

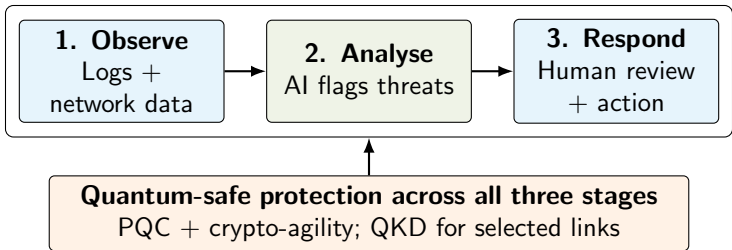
Prioritise PQC for broad migration. Assess QKD for specific links; it does not replace PQC across an organisation.

Neither is a complete security system: endpoints, authentication and implementation still need protection.

Sources: NIST, PQC project [7]; NSA, QKD technical limitations [11].



AI + Quantum: The Convergence



- **AI detects:** identifies suspicious activity and prioritises alerts.
- **Quantum-safe cryptography protects:** secures communications and identities; crypto-agility supports algorithm upgrades.
- **People govern:** validate high-impact response decisions.

Together: intelligent defence with quantum-resilient trust.



Formal Verification: Trust in AI and PQC

Assurance layer: prove specified security properties of a model or implementation using mathematical reasoning, under explicit assumptions.

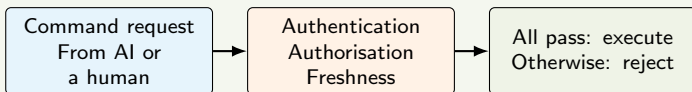
AI assurance

Verify that bounded input changes cannot alter a classifier's decision.
[12]

PQC assurance

Verify code correctness, memory safety and constant-time behaviour.
[13]

Illustrative example: spacecraft command acceptance



Property to prove: $\text{Execute} \Rightarrow \text{Authenticated} \wedge \text{Authorised} \wedge \text{Fresh}$
A replayed command must be rejected even if its signature is valid.

Scope matters: proof covers stated properties and assumptions, not every attack; testing and monitoring remain necessary.



Space-Cybersecurity Use Cases

Mission area	AI-enabled role	Quantum-safe role
Spacecraft operations	Flag unusual command / telemetry sequences for investigation	PQC authentication for commands and software updates
Ground segment / SOC	Alert correlation, intrusion detection and analyst assistance	Cryptographic inventory, PQC-protected links and crypto-agility
Onboard processing	Prioritise useful observations and reduce unnecessary downlink	Protect the integrity and confidentiality of mission data
Optical and strategic links	Adaptive monitoring of link behaviour and interference	QKD for selected high-value links where specialised hardware is justified

Important distinction

These are **candidate use cases**; architecture, assurance and deployment readiness must be evaluated for each mission.

Sources: Background for these proposed applications:

ISRO, POEM-4 payloads (2024) [14]; SMOPS 2026 [15];

300 m QKD demonstration (2022) [16]; NIST, PQC project [7].



Relevant Work at ISRO / Department of Space

Quantum communication demonstrations

- **Free-space links:** 300 m demonstrations at SAC in 2021 and 2022. [16]
- **2022 experiment:** entanglement-based QKD for text, image and video applications. [16]

AI and mission operations

- **Onboard AI:** TakeMe2Space's POEM-4 payload supports uploaded ML models and in-orbit inference. [14]
- **SMOPS 2026:** AI/ML for autonomous operations with human-machine synergy. [15]

Security connection: quantum links support key distribution; onboard AI and mission automation also need secure models, commands and updates.

Sources: ISRO, QKD demonstration (2022) [16]; POEM-4 payloads (2024) [14]; SMOPS 2026 [15].



Relevant Work at IIST

Research and training

- **M.Tech.:** quantum computing, communication, cryptography and sensing for space. [17]
- **Quantum optics:** squeezed/entangled light; sensing, imaging and communication. [18]
- **2025 result:** correlated quantum random-number streams up to **6 Mbit/s**. [19]
- **Systems and Networks Lab:** satellite networks, edge computing, 5G/6G and quantum computing. [20]

Security connection: these capabilities support research into trusted randomness, secure communication and intelligent monitoring.

Sources: IIST, M.Tech. Quantum Technology [17]; Quantum Optics research [18]; *Quantum Fluctuations Turned into Secure Random Numbers* (2025) [19]; Systems and Networks Lab [20].



CVVR Lab: Watermarking and FedAMF

Robust image watermarking

Exploring the learning capabilities of convolutional neural networks for robust image watermarking

H. Kandi, **D. Mishra**, S. R. K. Sai Gorthi; *Computers & Security*, 65, 247–268 (2017). [21]

Idea: CNN-learned codebooks embed and recover image watermarks.

Security link: ownership marking and robustness to image distortions.

FedAMF: learning across visible and infrared images

FedAMF: Federated Alignment with Multi-Part Feature for Visible-Infrared Person Re-Identification

B. Neelima, N. Murali, **D. Mishra**; IEEE NCC 2026, 454–459. [22]

Idea: federated learning and feature alignment for matching people across visible and infrared imagery.

Security link: distributed visual analytics without pooling raw images.

Discussion point: avoiding raw-data sharing is not, by itself, a formal privacy guarantee; model updates and access still need safeguards.



CVVR Lab: Hiding Multimedia in Images

Video-in-image hiding

Hiding Video in Images: Harnessing Adversarial Learning on Deep 3D-Spatio-Temporal Convolutional Neural Networks

R. Gandikota, **D. Mishra**, N. B. Brown; CVIP 2022 proceedings, Springer (2023), 58–71. [23]

Idea: adversarially trained embedder/extractor networks hide video information in an image and recover it; the study includes a 3D-CNN model.

Audio-in-image hiding

Hiding Audio in Images: A Deep Learning Approach

R. Gandikota, **D. Mishra**; PReMI 2019, Springer, 389–399. [24]

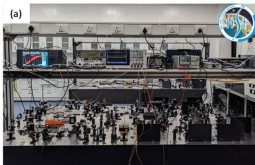
Idea: a GAN-based model embeds audio in a host image; an extractor recovers the audio, with robustness studied under image distortions.

Lecture connection: AI for multimedia information hiding. These are not encryption or quantum-safe security guarantees.



IIST: AI + Quantum Research Opportunities

Quantum Optical Technology Lab



Quantum light, sensing and imaging
Quantum communication and cryptography

Computer Vision and Virtual Reality Lab (CVVR)



Computer vision and machine learning
Image analysis and virtual reality

Our opportunity

IIST has complementary strengths in **AI and quantum technology**. Integrating them can open new interdisciplinary research directions.

Proposed security research: AI-assisted quantum-link monitoring; mission-log anomaly detection; hybrid quantum–classical security methods.

Sources: IIST, Quantum Optics research [18]; CVVR Lab [25]. Quantum-lab photo supplied by presenter.



Emerging Research: Quantum + AI

Potential directions

- Quantum machine learning
- Quantum optimisation for security workloads
- AI-assisted quantum network monitoring
- Quantum-enhanced cryptanalysis research

Important caveat

Many quantum-AI security applications remain **research or early-stage**; practical advantage depends on quantum hardware quality, scale, error correction and the workload.



Current Trends: 2025–2026

AI trends

- Generative AI in security operations
- AI-assisted threat intelligence
- Security for AI agents and LLMs
- Adversarial ML and AI red-teaming
- AI-enabled phishing and fraud

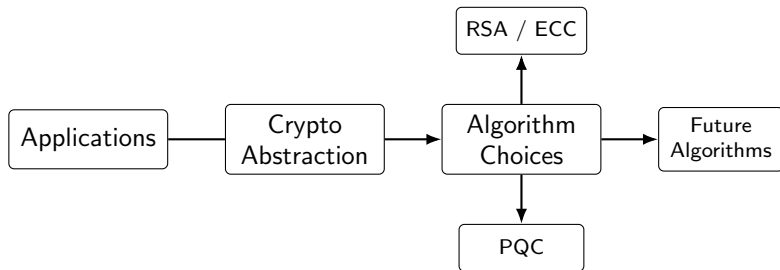
[3, 26, 7]

Quantum trends

- PQC deployment and migration
- Cryptographic inventory and crypto-agility
- Hybrid classical + PQC deployments
- QKD research and specialised networks
- Quantum-readiness planning



Crypto-Agility: Preparing for Change



Principle

Build systems so cryptographic algorithms can be replaced **without redesigning the entire application or infrastructure.**



Challenges Ahead

AI

- Adversarial attacks
- Hallucination / error
- Privacy
- Explainability
- Model supply chain

Quantum

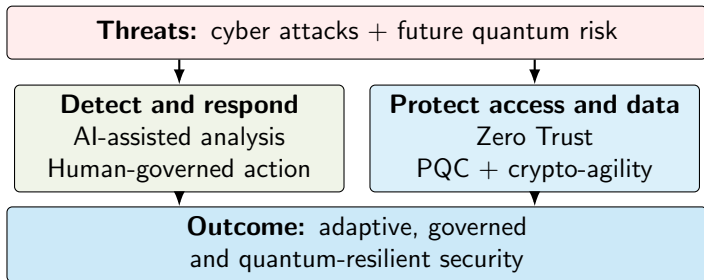
- Hardware scale
- Error correction
- Cost / access
- Standards transition
- Interoperability

Together

- Skilled workforce
- Migration cost
- Governance
- Trust
- Long-term planning



Future Cybersecurity Architecture



- **Two complementary roles:** AI supports detection and response; quantum-safe cryptography strengthens long-term protection.
- **Keep people in control:** govern high-impact actions and continuously monitor the system.
- **Plan for change:** use crypto-agility for upgrades; consider QKD only for selected high-value links.

Key note: intelligent defence and resilient protection must work together.



Key Takeaways

- 1 AI supports intelligent defence:** detection, time-series forecasts and governed response.
- 2 AI must also be secured** against adversarial attacks, privacy risks and misuse.
- 3 Quantum computing threatens** widely used public-key cryptography.
- 4 Start PQC migration early** and design for crypto-agility.
- 5 Combine complementary tools:** AI, quantum-safe protection and selected quantum-enabled technologies.

Final message

**AI strengthens detection and response.
Quantum-safe and quantum-enabled technologies strengthen
protection.**



Selected References I

- [1] Kyle Hundman et al. *Detecting Spacecraft Anomalies Using LSTMs and Nonparametric Dynamic Thresholding*. 2018. DOI: [10.1145/3219819.3219845](https://doi.org/10.1145/3219819.3219845). arXiv: 1802.04431.
- [2] Apostol Vassilev et al. *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*. Tech. rep. NIST AI 100-2e2025. National Institute of Standards and Technology, 2025. DOI: [10.6028/NIST.AI.100-2e2025](https://doi.org/10.6028/NIST.AI.100-2e2025).
- [3] European Union Agency for Cybersecurity. *ENISA Threat Landscape 2025*. Oct. 1, 2025. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025> (visited on 09/01/2026).
- [4] Peter W. Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994), pp. 124–134.
- [5] IBM Quantum. *Shor's Algorithm*. URL: <https://quantum.cloud.ibm.com/docs/en/tutorials/shors-algorithm> (visited on 09/09/2026).
- [6] National Institute of Standards and Technology. *Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography*. Aug. 13, 2024. URL: <https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved> (visited on 09/01/2026).
- [7] National Institute of Standards and Technology. *Post-Quantum Cryptography*. 2025. URL: <https://csrc.nist.gov/Projects/post-quantum-cryptography> (visited on 09/01/2026).
- [8] National Institute of Standards and Technology. *Personal Identity Verification of Federal Employees and Contractors*. URL: <https://csrc.nist.gov/projects/piv> (visited on 09/09/2026).
- [9] National Institute of Standards and Technology. *Working Drafts: Post-Quantum Cryptography Updates to the PIV Standards*. June 12, 2026. URL: <https://csrc.nist.gov/News/2026/pqc-updates-to-piv-standards-working-drafts> (visited on 09/02/2026).



Selected References II

- [10] Charles H. Bennett and Gilles Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing". In: *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (1984), pp. 175–179.
- [11] National Security Agency. *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*. URL: <https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/> (visited on 09/09/2026).
- [12] Guy Katz et al. *Towards Proving the Adversarial Robustness of Deep Neural Networks*. 2017. arXiv: 1709.02802. URL: <https://arxiv.org/abs/1709.02802>.
- [13] Manuel Barbosa et al. *Formal Verification of Post-Quantum Cryptography*. Third NIST PQC Standardization Conference. 2021. URL: <https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/meijers-formal-verification-pqc2021.pdf>.
- [14] Indian Space Research Organisation. *POEM-4 Payloads in the PSLV-C60 / SpaDeX Mission*. Dec. 22, 2024. URL: https://www.isro.gov.in/POEM_4_Payloads_spadex.html (visited on 09/02/2026).
- [15] Indian Space Research Organisation. *International Conference on Spacecraft Mission Operations 2026*. 2026. URL: https://www.isro.gov.in/Spacecraft_Mission_Operations_SMOPS_2026.html (visited on 09/02/2026).
- [16] Indian Space Research Organisation. *Department of Space Demonstrates Entanglement-Based Quantum Communication over 300 m Free Space*. Jan. 27, 2022. URL: <https://www.isro.gov.in/DeptofSpace.html> (visited on 09/02/2026).
- [17] Indian Institute of Space Science and Technology. *M.Tech. in Quantum Technology*. 2026. URL: <https://www.iist.ac.in/academic-programme/m-tech-quantum-technology> (visited on 09/02/2026).
- [18] Indian Institute of Space Science and Technology. *Quantum Information and Quantum Optics*. 2026. URL: <https://iist.ac.in/research-areas/quantum-optics-quantum-information-quantum-technologies> (visited on 09/02/2026).



Selected References III

- [19] Indian Institute of Space Science and Technology. *Quantum Fluctuations Turned into Secure Random Numbers at IIST*. Oct. 31, 2025. URL: <https://www.iist.ac.in/research-highlights/quantum-fluctuations-turned-secure-random-numbers-iist> (visited on 09/02/2026).
- [20] Indian Institute of Space Science and Technology. *Systems and Networks Lab*. 2026. URL: <https://www.iist.ac.in/laboratory/systems-and-networks-lab> (visited on 09/02/2026).
- [21] Haribabu Kandi, Deepak Mishra, and Subrahmanyam R. K. Sai Gorthi. "Exploring the learning capabilities of convolutional neural networks for robust image watermarking". In: *Computers & Security* 65 (2017), pp. 247–268. DOI: 10.1016/j.cose.2016.11.016.
- [22] Bhairi Neelima, Nirmala Murali, and Deepak Mishra. "FedAMF: Federated Alignment with Multi-Part Feature for Visible-Infrared Person Re-Identification". In: *2026 National Conference on Communications (NCC)*. IEEE, 2026, pp. 454–459. DOI: 10.1109/NCC68160.2026.11478905.
- [23] Rohit Gandikota, Deepak Mishra, and Nik Bear Brown. "Hiding Video in Images: Harnessing Adversarial Learning on Deep 3D-Spatio-Temporal Convolutional Neural Networks". In: *Computer Vision and Image Processing (CVIP 2022)*. Vol. 1776. Communications in Computer and Information Science. Springer, 2023, pp. 58–71. DOI: 10.1007/978-3-031-31407-0_5.
- [24] Rohit Gandikota and Deepak Mishra. "Hiding Audio in Images: A Deep Learning Approach". In: *Pattern Recognition and Machine Intelligence (PRMI 2019)*. Springer, 2019, pp. 389–399. DOI: 10.1007/978-3-030-34872-4_43.
- [25] Indian Institute of Space Science and Technology. *Computer Vision and Virtual Reality Lab*. URL: <https://www.iist.ac.in/laboratory/computer-vision-and-virtual-reality-lab> (visited on 09/09/2026).
- [26] National Institute of Standards and Technology. *AI Research - Security and Resilience*. 2026. URL: <https://www.nist.gov/artificial-intelligence/ai-research-security-and-resilience> (visited on 09/01/2026).
- [27] National Institute of Standards and Technology. *Migration to Post-Quantum Cryptography*. URL: <https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc> (visited on 09/09/2026).



Questions?



Thank you.
