Neapolis University Pafos, Cyprus
AI-Z-TRACE-CRIME
Jean Monnet Center of Excellence
Co-funded by the European Union

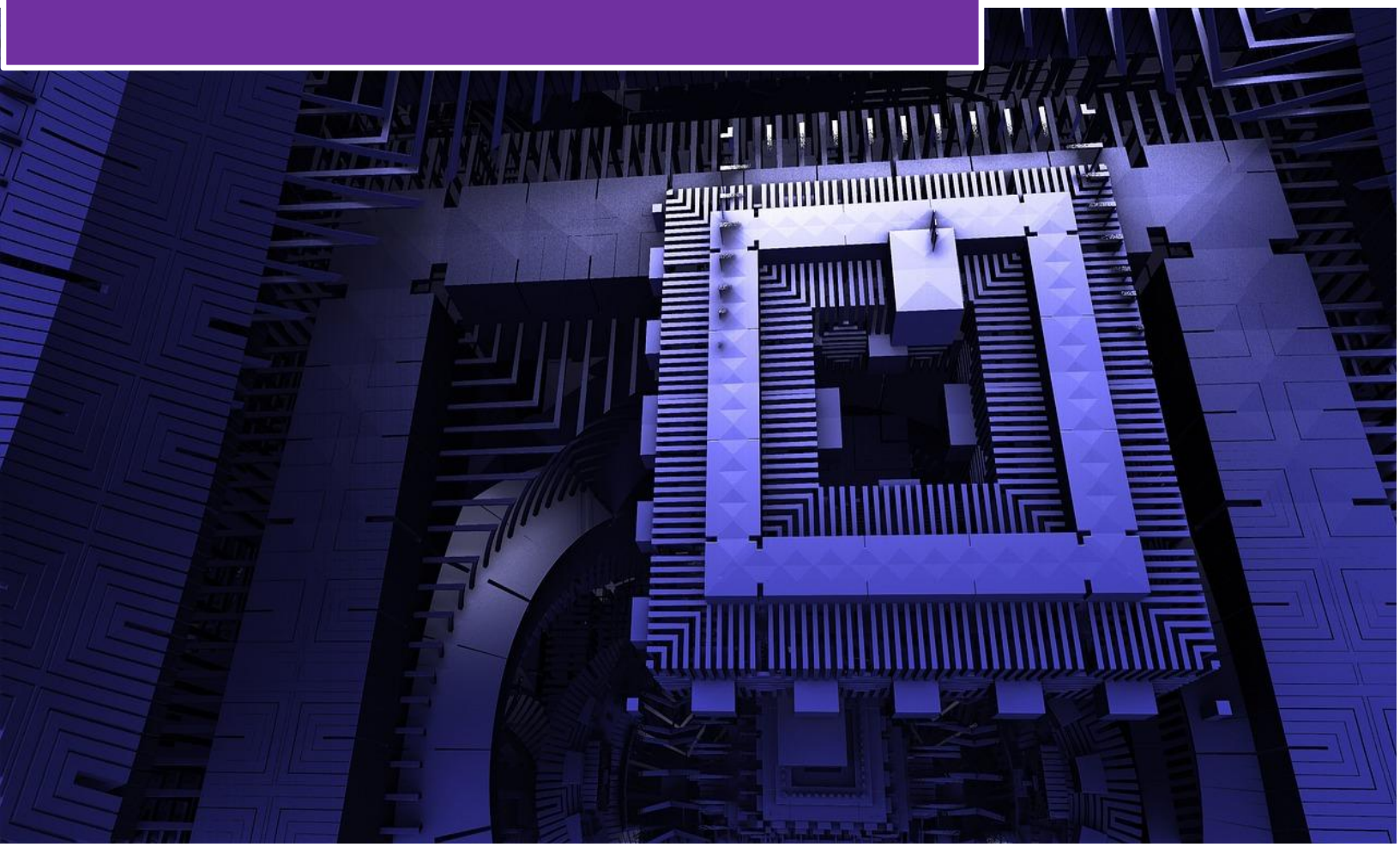
Policy Brief

Quantum Technologies:

Implications for Law Enforcement

NUP Jean Monnet / UNESCO Policy Briefs

45/2026



Co-funded by the European Union

Neapolis University Pafos

UNESCO Chair in Human Development, Security & the Fight against Transnational Crime and Illicit Trafficking in Cultural Property

unesco Chair

The NUP Jean Monnet / UNESCO working papers and policy briefs can be found at:

https://www.nup.ac.cy

Publications in the Series should be cited as:

AUTHOR, TITLE, NUP UNESCO/JEAN MONNET WORKING PAPER or POLICY BRIEF NO. x/YEAR [URL]

Copy Editor: G. Pavlidis

Neapolis University Pafos, School of Law

Pafos, 8042, Cyprus

Quantum Technologies:

Implications for Law Enforcement

Executive Summary

Europol's Innovation Lab Observatory Report 'The Second Quantum Revolution' (2023) analyses the profound implications of emerging quantum technologies for law enforcement and security. The report explores both the transformative opportunities and the disruptive risks arising from quantum computing, quantum sensing, quantum communication, and related innovations. It emphasises that quantum technologies will not only redefine digital forensics and data processing but also challenge the very foundations of encryption and cybersecurity.

The report was developed in collaboration with the European Commission's Joint Research Centre (JRC) to help law enforcement agencies understand how the second quantum revolution may reshape investigative methods, evidence collection, and data protection frameworks. By balancing innovation with preparedness, the report positions quantum technologies as both an enabler and a risk factor for future policing.

Keywords

Europol, Quantum Computing, Post-Quantum Cryptography, Quantum Sensors, Quantum Communication, Digital Forensics, Artificial Intelligence, Law Enforcement Innovation, Cybersecurity.

Background

Quantum technology represents a paradigm shift comparable to the introduction of the digital computer. While the first quantum revolution in the 20th century gave rise to technologies such as semiconductors and lasers, the second quantum revolution harnesses the principles of quantum superposition and entanglement to enable entirely new capabilities. Quantum computers can perform complex calculations exponentially faster than classical systems, quantum sensors can measure with unprecedented precision, and quantum communication promises unbreakable security.

For law enforcement, these technologies will affect both operational capability and threat landscapes. Quantum computing could undermine current cryptographic systems, exposing sensitive data to decryption risks. At the same time, quantum sensors and communication networks could enhance evidence integrity and cross-border coordination. The Europol Innovation Lab emphasises that understanding these dynamics is vital to maintaining security and public trust as quantum technologies mature.

Selection of quantum applications

Ultra-Secure Communication (QKD)
Quantum key distribution for tamper-proof encryption and secure networks.

Post-Quantum Cryptography Transition
Preparing systems for cryptographic resilience against future quantum attacks.

Quantum-Enhanced Drug Discovery
Molecular simulation for faster development of medicines and materials.

Quantum Optimization for Industry
Logistics, finance, energy grids, and supply chains using quantum algorithms.

Quantum Machine Learning (QML)
Improved pattern recognition, feature extraction and hybrid AI models.

Next-Generation Sensors & Metrology
Ultra-precise measurements for navigation, climate, space, medical imaging.

GPS-Independent Navigation
Quantum inertial sensors enabling highly reliable positioning.

Quantum Simulation of Complex Systems
Studying superconductors, chemical reactions, and exotic materials.

Environmental & Geophysical Monitoring
Quantum gravimeters and magnetometers for Earth observation, archaeology, and resource mapping.

Quantum Internet (Future Networking)
Distributed quantum computing, entanglement-based networks, and new communication paradigms.

Key Findings

The report identifies five core dimensions where quantum technologies will impact law enforcement:

• Cryptography and Cybersecurity: Quantum computers will eventually be capable of breaking widely used public-key cryptographic algorithms. This creates a long-term risk of “store-now, decrypt-later” attacks, where adversaries collect encrypted data today to decrypt it once quantum capability becomes available. Post-quantum cryptography (PQC) and quantum key distribution (QKD) are highlighted as essential mitigation strategies.

• Digital Forensics: Quantum computing may enhance complex pattern recognition, password recovery, and data decryption tasks in criminal investigations. However, it may also enable adversaries to conceal traces or manipulate digital evidence more effectively.

• Quantum Sensors: These sensors can detect minute environmental changes, improving forensic analysis (e.g., trace detection, imaging) and enhancing situational awareness during field operations. They could support search-and-rescue, surveillance, and border control missions while raising new privacy considerations.

• Quantum Communication: Technologies based on quantum entanglement offer secure information transfer resistant to interception. Quantum networks could revolutionise cross-border data sharing and evidence transmission by ensuring authenticity and integrity.

• Artificial Intelligence and Data Processing: Quantum machine learning (QML) has the potential to accelerate AI-driven analytics in crime prediction, data correlation, and facial recognition. The report cautions, however, that integration with existing systems must respect human oversight and ethical constraints.

Collectively, these developments represent a dual-use frontier—enhancing security capabilities while simultaneously creating new avenues for cyber exploitation.

Operational Implications

Quantum technologies will fundamentally alter how law enforcement collects, processes, and protects data. Europol highlights several operational implications:

• Transition Planning: Agencies must begin preparing for the migration from classical to post-quantum cryptography to ensure continuity of data protection.

• Capability Development: Early experimentation with quantum algorithms and NISQ (Noisy Intermediate-Scale Quantum) systems will enable familiarity before large-scale deployment.

• Forensic Integration: Quantum-enhanced analysis could support complex investigations, particularly in digital forensics, cryptanalysis, and cybercrime.

• Ethical and Legal Oversight: Quantum tools that increase surveillance capability must operate within the boundaries of EU data protection and human rights frameworks.

• Interdisciplinary Training: Officers, analysts, and policy-makers will require foundational understanding of quantum principles to assess opportunities and risks.

The report underscores that awareness and preparation are key to ensuring that law enforcement remains technologically resilient in the quantum era.

Strategic Recommendations

Building on its analysis, Europol and the JRC propose several strategic actions for EU law enforcement and policymakers:

• Establish Quantum Foresight Units: Develop institutional mechanisms to monitor advances in quantum research and assess potential security impacts.

• Invest in Post-Quantum Cryptography: Coordinate with ENISA, NIST, and standardisation bodies to transition to quantum-resistant encryption protocols.

• Promote Research Partnerships: Foster collaboration between law enforcement, academia, and quantum research centres to co-develop secure applications.

• Develop Ethical Guidelines: Ensure that quantum-enabled capabilities, particularly in forensics and surveillance, align with fundamental rights and proportionality principles.

• Enhance International Cooperation: Quantum technologies are inherently transnational; cooperation with allies will be critical for harmonising standards and sharing expertise.

• Leverage EU Funding Frameworks: Horizon Europe and the Digital Europe Programme can support quantum R&D tailored to security and justice applications.

These recommendations aim to balance technological readiness with governance and ethical responsibility.

Concluding Remarks

The second quantum revolution introduces both unprecedented capabilities and novel risks for European law enforcement. Quantum computing threatens to disrupt the security foundations of digital communication, while quantum-enhanced tools hold transformative potential for forensics, analytics, and secure data exchange.

Europol's report concludes that preparedness, not panic, should guide policy. By anticipating change, fostering research collaboration, and embedding ethical foresight into operational planning, the EU can ensure that quantum innovation strengthens rather than destabilises law enforcement and public trust.

The quantum era will redefine the boundaries between security and technology—demanding vigilance, adaptability, and cooperation at every level.

Further Reading

- Europol Innovation Lab (2023), 'The Second Quantum Revolution: The Impact of Quantum Technologies on Law Enforcement' (link)