FINABEL
THE EUROPEAN LAND FORCE
COMMANDERS ORGANISATION

OCTOBER 2025

The End of State Secrets with Quantum Cryptography

Arjun Jayaraman
Defence & Security Research Department

RESEARCH REPORT

FINABEL
THE EUROPEAN LAND FORCE
COMMANDERS ORGANISATION

Defence & Security Research Department

Written by: **Arjun Jayaraman**
Supervised by: **Elise Alsteens & Kevin Whitehead**
Edited by: **Michael O'Daly**

FINABEL's Research Reports are concise, research-driven publications designed to keep Europe's defence community informed about the latest strategic, military, and geopolitical developments. Released three times per week, these short-form papers offer timely analysis on emerging trends affecting European land forces. Each Research Report is produced by the researchers of FINABEL's Permanent Secretariat, in the goal of supporting decision-making across the European defence landscape.

RESEARCH REPORT

1. Introduction

In September 2025, Harvard scientists announced that they had successfully created a quantum computer of 3,000 qubits. The scientists were able to keep the quantum computer running for more than two hours. (Pattinson, 2025) This was a significant achievement; quantum computers are notoriously unstable, due to the hypersensitivity of quantum particles to environmental stimuli. The breakthrough demonstrated the technical potential of error correction mechanisms that can keep a quantum computer running for extended periods. It also brought the possibility of quantum supremacy closer to reality. Considering this significant achievement, it is timely to analyse the impact of quantum technology on defence and the military. Quantum technologies can comprise several areas, including quantum cryptography, quantum sensing and quantum computing. This is the first of a series of three Info Flashes covering the impact of quantum tools on cryptography. The other two will cover quantum sensing (including positioning, navigation, and timing), and quantum computing (including military simulations, optimising logistics, and Artificial Intelligence integrations).

Quantum computers are far more efficient than classical computers. This is because of the principles of superposition, entanglement, and interference. If Europe's adversaries were to adopt a "harvest now, decrypt later" strategy, they could: (i) learn about state secrets (diplomatic, military, or political communications and information), which have national security implications; (ii) access personal information about a nation's citizens; and (iii) eavesdrop on "secure" communications in both peacetime and military contexts. Post-Quantum Computing (PQC) and Quantum Key Distribution (QKD) are ways to safeguard sensitive information against quantum tools. Given the threat, how is Europe approaching quantum communications, and is it enough? I argue that Europe is on the right track in establishing a secure quantum communications network and establishing bold policy goals, but that it should also create an enabling environment to facilitate quantum adoption.

2. Primer on quantum properties

It is first useful to understand how classical computers work. They typically process information in binary. For example, in binary, the letter A is "01000001", and B is "01000010". A simple word, like "good", is "01100111 01101111 01101111 01100100". Note that these numbers only last in two states: 0 or 1. Classical computers read through these numbers sequentially to make meaning of them.

Unlike classical computers, the building block of quantum computers – or qubits – can occupy both the 0 and 1 positions (Imashev, 2025). Technically, this is called superposition. Further, quantum computers need not read numbers or data sequentially, but all at once (Hanna, 2025). Together, this allows quantum computers to solve complex problems at a fraction of the time of classical computers. Consider a problem where both a classical and a quantum computer are required to find the most efficient way to get through a maze. A classical computer will try every path from the beginning to a potential end sequentially, stopping and restarting the process if the one path taken leads to a dead end. The quantum computer, however, will run through all possible paths simultaneously, terminating each path as it reaches its dead end or the end of

the maze. (Bashuk, 2003) This way, quantum computers can find solutions to problems faster than classical computers.

The quantum property of entanglement allows information regarding a particular atom to be immediately discernible based on how its partner atom is, regardless of their physical distance. Researchers, for example, might create two entangled atoms and place them in different locations. If these atoms are viewed from the same angle in their different locations, then viewers might find that the two atoms are always correlated and reflect information about each other. (Caltech, 2025).

The third property is quantum interference, where electrons that travel as waves interfere with each other to indicate a most probable solution to a problem (Krelina, 2025). Any attempt to measure such interference, or eavesdrop, involves tampering with or attempting to observe the particles in superposition, forcing them to return to a classical state. Practically speaking, users could compare interference patterns to find out if a link between them is secure. (Bennet and Brassard, 1984)

3. How does quantum computing break modern encryption?

Two types of encryptions are used for data security: symmetric and asymmetric encryption. Quantum computing can break asymmetric encryption easily (Parker, 2023). It is more challenging for it to break symmetric encryption; however, the entire system remains weak as the keys underpinning symmetric encryption are exchanged with asymmetric encryption. Under symmetric encryption, Agent A and Agent B will have a similar encryption and decryption key and can share information between each other using these keys. For example, Agent A may encrypt a file containing secret information with, for example, an Advanced Encryption Standard (AES) key, which can be a 128-bit key or a 256-bit key. The key in the case of the former can take on 2 possibilities, while it can take on 2 possibilities for the latter (Imashev, 2025). Anyone hoping to decrypt this file will require the exact key Agents A and B have. Adversaries who wish to obtain this key will take trillions of years to find one key among 2 or 2 possibilities. In contrast, quantum computers can use Grover's Algorithm, which reduces the number of steps a computer takes to find an item in an unordered database (such as the correct decryption key).

With this method, a quantum computer enjoys quadratic efficiency in decrypting AES- encrypted files. Hence, Grover's algorithm allows quantum computers to decrypt 128-bit encrypted files with 264 steps, which degrades security. However, decrypting 256-bit encryption remains intractable as the computer would have to go through 2128 possibilities. However, for Agent A and Agent B to have the same key in the first place, they would have to exchange the key over an asymmetric channel, which can be easily hacked by malicious actors.

The bigger and more urgent problem is with asymmetric encryption. These systems depend on Rivest-Shamir-Adelman (RSA) encryption, among some others. RSA encryption relies on how difficult it is for computers to identify two exact factors for a large multiple. Classical computers will find the problem intractable. However, quantum computers can use Shor's Algorithm – an algorithm designed to resolve the

integer-factorisation problem – to exponentially reduce the time taken to arrive at the factors required to decrypt the information (Thales, 2025). What might take a classical computer several billion years to decrypt may take a sufficiently powered quantum computer using Shor's Algorithm just hours or minutes (Kelly, 2025). This is a significant threat to encrypted communications, given that secret information is either shared or stored using RSA encrypted keys.

4. How does quantum computing affect national security?

Quantum cryptography marks the end of easily kept state secrets. State secrets, which may be stored in encrypted files, are now prone to being decrypted by nation-states with sufficiently powerful quantum computers (Hanna, 2025). Then, adversaries could access or even publish, for example: (i) top secret war plans, including potential orders of battle and security considerations; (ii) blueprints for cutting edge military technology or new innovations; (iii) lists of covert agents operating within a certain geography; (iv) the actual capabilities of various weapons systems and military units; and (v) diplomatic communications among allied nations (Biden, 2022; Hanna, 2025; Parker, 2025). Such information will allow an adversary to better tailor offensive war plans, understand their opponents' weak spots, eliminate moles in their government, steal military technology if more advanced than their own, and better forecast alliance relations in case of conflict. Hence, quantum computing risks the interception and publication of state secrets.

Quantum cryptography also brings an end to secure communications. For example, adversaries could eavesdrop on electronic and encrypted communications between security agencies and militaries, intelligence briefings, as well as other platforms sharing secret information (Parker, 2025). During wars, quantum-enabled forces would be able to listen into their adversaries' radio communication, obtaining intelligence on troop positions and movements, respond quickly to attempted surprise attacks, and even replace genuine information with junk, confusing its enemy and potentially causing fratricide.

Hence, quantum-enabled adversaries can collect important information and confuse its enemies in peacetime and war.

5. What is PQC and QKD, and how does it protect information from quantum tools?

5.1. *PQC*

PQC uses advanced algorithms to make decryption intractable even for quantum computers (NIST, 2024a). For example, instead of using factorisation problems that can be easily broken (Thales, 2025) by a sufficiently powered quantum computer and Shor's Algorithm, PQC might rely on, for example: (i) lattice-based cryptography, which relies on the difficulty of some problems among a repeating set of grid points across several dimensions (such as the Shortest Vector Problem) (Imashev, 2025) or (ii) hash-based cryptography, which relies on the computational inability of hash keys to be reverse engineered into their original input (Lavanyan & Selvi, 2024). Hence, there are mathematically complicated algorithms that are intractable for quantum computers and can be used to encrypt sensitive information.

5.2. *QKD*

QKD is the distribution of keys to encrypted files via a quantum channel (Bub, 2007; QNu Labs, 2023). It is not the encrypted file that is shared over a quantum channel, but the key to authenticate the identity of the sender and recipient (Lo and Lütkenhaus, 2007) and decrypt the file. QKD relies on interference to ensure that the key is safely transmitted.Take that Agent A would like to send Agent B some information. While quantum-encrypted information might be shared on a public channel, the decryption key would be shared over a quantum channel. The key is coded into photons set into superposition and sent from Agent A to Agent B over a fibre-optic cable. Agent B can then shoot these photos onto a photon collector and use that to decrypt any files. However, before doing so, Agent A and Agent B must perform a check: they must compare the photon signature sent and the one received; should the patterns be different, they must discard the key and start over, given that the different patterns suggest the presence of an attempted eavesdrop. (QNu Labs, 2024) Even if eavesdroppers manage to steal the quantum-encrypted file, they would be unable to decrypt it. Hence, QKD is a way for parties to be aware of whether there has been an attempt at eavesdropping on attempted secure communications (Barney and Gillis, 2025).

6. What has Europe done so far, and is it enough?

6.1. *What has Europe done so far?*

Europe has embarked on creating a European Quantum Communications Infrastructure (EuroQCI) (Melnic, 2021). The EuroQCI will comprise a terrestrial fibre-optic network and a space-based network. The former is to facilitate communications where messages can be reliably communicated over land, given that fibre optic cables can transmit light only for 80 – 100km before requiring repeating. States could also use satellites to transmit and receive messages after the launch of the Eagle-1 satellite. These messages will be controlled by a Quantum Hub, which is responsible for ensuring that users are legitimate and that the network is physically capable of handling the message to be transmitted. (European Commission, 2024) While countries are innovating and developing the network domestically so that they can account for regional or national priorities, regional-level initiatives provide a standardisation element. For example, NOSTRADAMUS – a part of the EuroQCI network – provides standards and testing for QKD infrastructure in Europe, ensuring that information is secure and that the system functions as intended.

NATO and European agencies have set PQC as a priority. NATO has noted quantum technologies as a priority under its DIANA accelerator, crowding in the private sector to create novel solutions for the military (NATO, 2024). The European Defence Fund also funded Quantum Agile and Resilience Military Communications (Q-ARM), an initiative coordinated by Almaviva, an Italian information and communication technology group. The project started in 2025 and is due to last for 36 months with a funding of approximately €5 million. (European Defence Fund, 2024) Furthermore, preferred PQC algorithms have already been established by the US-based National Institute of Standards and Technology, which conducted several challenges in 2019 to crowdsource effective PQC algorithms. They announced several "selected algorithms", such as CRYSTALS-KYBER and CRYSTALS-DILITHIUM, which are

lattice-based encryption standards for keys and digital signatures, respectively (NIST, 2024b). Hence, technically transitioning to such a system should be easier than innovating PQC algorithms from scratch.

6.2 What are the strengths and weaknesses of Europe's approach?

6.2.1 *Quantum Communications Networks*

On the one hand, EuroQCI brings together continental resources to focus on one concept of operations: to build a terrestrial network of trusted quantum communication nodes, managed by a central Quantum Hub, that is facilitated by satellite communication if distances are too far. (European Commission, 2024) However, the key weakness of this approach is the existence of several hubs. Each hub represents a weakness that an adversary can exploit, whether it be through physically hijacking a "trusted node" to gain access to classified information, or whether it be temporarily blinding a satellite to prevent it from receiving or transmitting any photons to facilitate quantum communication. This key installation risk should be overcome with high security for quantum-based assets, which will be resource intensive.

It is too early to tell if Q-ARM will be a success; it is off to the right start by involving many partners across the European continent, ensuring better interoperability and reducing redundancies.

6.2.2. *PQC and QKD*

NATO and European agencies have taken a step in the right direction to prioritise the development of quantum technologies to better implement PQC and QKD for more secure military communications. They have also established the Transnational Quantum Community for researchers to share lessons on their quantum research, moving the continent towards quicker development of quantum tools (NATO, 2024). However, it is unclear what agencies are doing outside of these policy moves. The quantum supply chain is plagued with several problems, including the lack of availability of infrastructure and expertise.

7. A Reality Check

The quantum threat is not going to be immediate because takes time, money, materials, and expertise to build Fault-Tolerant Quantum Computers (FTQC). This is because qubits are hypersensitive to environmental stimuli (e.g. noise and thermal fluctuations) and must be placed in specific environments to function (Gill et al., 2024). If not, they can fail and require error correction mechanisms to be fixed or replaced with a functioning qubit (Pattinson, 2025 and Saki et al., 2019). The failure of qubits could lead to decoherence and a return to classical computing. The Harvard experiment mentioned at the opening of this paper managed to keep a quantum computer running for only two hours (Pattinson, 2025). Given that some tasks may take even an FTQC months or years to complete, researchers will have to continue to find ways to perform error corrections and create an FTQC. That said, some experts estimate that it will take only 5 to 6 years for a state to build the first FTQC (Mosca, 2018).

Nevertheless, Europe cannot rest easy for two reasons: (i) the "harvest now, decrypt later" strategy; and (ii) adoption timelines for PQC and QKD. First, the "harvest now, decrypt later" strategy is when states steal and store troves of currently encrypted information. They continue this until they secure a quantum advantage, after which they will begin to decrypt these files (DuBose and Rao, 2025), which may yield relevant information. Hence, currently quantum-unprotected information is vulnerable, and adversary states may already be harvesting sensitive, encrypted data of allied nations. Second, it takes time for organisations to implement PQC methods.

Incorporating new and advanced encryption standards, such as lattice or hash-based encryption, is not as simple as a software update (Ivezic, 2019). The process requires hardware updates, software updates, and a corps of experts who can continuously monitor and update the system. These costly adoption measures might be out of reach for certain companies, even if they are in priority sectors. QKD methods are similarly costly: operationalising the various nodes of the EuroQCI is a resource-intensive process, which will require many people-hours to construct, operate, and guard (Lafleur, 2025). Finally, despite the policy framework (which is helpful), Europe has yet to create an enabling environment for quantum adoption. Vendors may not be ready to provide the infrastructure required for quantum adoption. Materials may not be available due to supply chain crunches. (Ivezic, 2019) Finally, Europe must train experts in the field quickly, alongside enabling mobility across the EU (European Commission, 2025).

8. Conclusion

The quantum revolution represents a sea change in computing. Quantum computers function differently from classical computers and have the processing power to break modern-day encryption. This would spell the end of state secrets (especially with "harvest now, decrypt later" strategies) and secure communications. To combat this, states can use one of several PQC strategies or QKD to make it difficult for even quantum computers to decrypt classified information. Quantum computers are at least 5 years away, due to engineering complications. However, Europe cannot rest easy. It is doing well to establish a quantum communications network. However, there is a key-installation risk as the network could be disrupted if one node cannot be trusted. Europe has also mandated the adoption of quantum tools by 2030, which is bold. However, more can be done to create an enabling environment that facilitates quantum adoption, including making equipment and expertise available.

Bibliography

Barney, N., & Gillis, A. S. (2025, July 2). What is Quantum Key Distribution? QKD Explained. Search Security. https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD

Bashuk, M. A. (2003). Solving a Maze With a Quantum Computer (Version 1). arXiv. https://doi.org/10.48550/ARXIV.QUANT-PH/0304146

Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, 560, 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

Biden, J. R. (2022, May 4). National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. The White House. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

Bub, J. (2007). QUANTUM INFORMATION AND COMPUTATION. In Philosophy of Physics (pp. 555–660). Elsevier. https://doi.org/10.1016/B978-044451560-5/50009-9

Caltech. (n.d.). What Is Entanglement and Why Is It Important? Caltech Science Exchange. Retrieved 2 October 2025, from http://scienceexchange.caltech.edu/topics/quantum-science-explained/entanglement

Derian, J. D., & Rollo, S. (2023). Quantum Warfare. In A. Gruszczak & S. Kaempf, Routledge Handbook of the Future of Warfare (1st edn, pp. 319–329). Routledge. https://doi.org/10.4324/9781003299011-34

DuBose, R., & Rao, M. M. (2025, May 21). Harvest now, decrypt later: Why today's encrypted data isn't safe forever. https://www.hashicorp.com/en/blog/harvest-now-decrypt-later-why-today-s-encrypted-data-isn-t-safe-forever

European Commission. (2024, November 21). EuroQCI ConOps (Concept of Operations) | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/miscellaneous/euroqci-conops-concept-operations

European Commission. (2025, September 23). Quantum | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/quantum

European Defence Fund. (2024). Q-ARM - Quantum Agile and Resilient Military Communications. https://defence-industry-space.ec.europa.eu/document/download/c421855b-0df4-4a57-abd2 4598a842ff80_en? filename=FACTSHEET_EDF_2024_LS_RA_DIS_QUANT_STEP_101224135_Q_ARM.pdf

Gill, S. S., Cetinkaya, O., Marrone, S., Claudino, D., Haunschild, D., Schlote, L., Wu, H., Ottaviani, C., Liu, X., Machupalli, S. P., Kaur, K., Arora, P., Liu, J., Farouk, A., Song, H. H., Uhlig, S., & Ramamohanarao, K. (2025). Quantum Computing: Vision and Challenges (pp. 19–42). https://doi.org/10.1016/B978-0-443-29096-1.00008-8

Hanna, H. (2025, January). The Emerging Potential for Quantum Computing in Irregular Warfare. Insights, 3(1), 7. IBM. (2025, June 10). What Is Quantum Computing? | IBM. https://www.ibm.com/think/topics/quantum-computing

Imashev, A. (2025). Quantum computing and cybersecurity: Exploring implications, potential threats and future directions. International Journal of Science and Research Archive, 16(1), 890–900. https://doi.org/10.30574/ijsra.2025.16.1.2046

Ivezic, M. (2019, October 14). Challenges of Upgrading to Post-Quantum Cryptography (PQC). PostQuantum - Quantum Computing, Quantum Security, PQC. https://postquantum.com/post-quantum/pqc-challenges/

Kelly, S. (2025). Breaking RSA: How Quantum Computing Threatens Today's Digital Security. https://www.researchgate.net/publication/393519992_Breaking_RSA_How_Quantum_Computing_Threatens_Today's_Digital_Security

Krelina, M. (2021). Quantum technology for military applications. EPJ Quantum Technology, 8(1), 24. https://doi.org/10.1140/epjqt/s40507-021-00113-y

Lafleur, A. (2025, March 5). Space-Based Quantum Key Distribution: Market Map and Competitive Landscape 2025. Space Insider. https://spaceinsider.tech/2025/03/05/space-based-quantum-key-distribution-market-map-and-competitive-landscape-2025/

Lewis, J. A., & Wood, G. (2023). Quantum Technology Applications and Implications. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-05/230526_Lewis_Quantum_Technology.pdf?VersionId=iCOWm7k02Ms846I0Eb5DLeyD6dZN8K5F

Lo, H.-K., & Lütkenhaus, N. (2007). Quantum Cryptography: From Theory to Practice. https://doi.org/10.48550/ARXIV.QUANT-PH/0702202

Melnic, V. (2021, July 13). Towards a New EU Quantum Communication Infrastructure—Finabel [Finabel]. https://finabel.org/towards-a-new-eu-quantum-communication-infrastructure/

Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

NATO. (n.d.). NATO releases first ever quantum strategy. NATO. Retrieved 6 October 2025, from https://www.nato.int/cps/en/natohq/news_221601.htm

NIST. (2024a). NIST Releases First 3 Finalized Post-Quantum Encryption Standards. NIST. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

NIST. (2024b). What Is Post-Quantum Cryptography? NIST. https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

Parker, E. (2023). When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret. https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html

Parker, E. (2025). U.S.-Allied Militaries Must Prepare for the Quantum Threat to Cryptography. https://www.rand.org/pubs/commentary/2025/06/us-allied-militaries-must-prepare-for-the-quantum-threat.html

Pattison, K. (2025, September 25). Clearing significant hurdle to quantum computing. Harvard Gazette. https://news.harvard.edu/gazette/story/2025/09/clearing-significant-hurdle-to-quantum-computing/

QNu Labs. (2023). Quantum Key Distribution (QKD) Explained step by step, Request a Demo from QNu Labs—YouTube. YouTube. https://www.youtube.com/watch?v=MfTXwVMi0uE

Quantum Flagship. (n.d.). European funding opportunities for quantum technologies. Quantum Flagship. Retrieved 6 October 2025, from https://qt.eu/funding-opportunities/

Saki, A. A., Alam, M., & Ghosh, S. (2019). Study of Decoherence in Quantum Computers: A Circuit-Design Perspective (Version 1). arXiv. https://doi.org/10.48550/ARXIV.1904.04323

SSH Academy. (n.d.). Military Grade Encryption Explained. Retrieved 3 October 2025, from https://www.ssh.com/academy/military-grade-encryption-explained

Thales. (2025). Data Threat Report (p. 34). http://cpl.thalesgroup.com/sites/default/files/content/campaigns/data-threat-report/2025-thales-data-threat-report.pdf

The Royal Institution (Director). (2024, January 30). The future of measurement with quantum sensors—With The National Physical Laboratory [Video recording]. https://www.youtube.com/watch?v=JfJWOgJF_KA

van Amerongen, M. (2021, June 3). NATO Review—Quantum technologies in defence & security. NATO Review. https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html

Young, R. (2025). Quantum Technologies in the UK Risks and Opportunities for National Security. Royal United Services Institute. https://static.rusi.org/quantum-technologies-and-national-security-march-2025.pdf

F I N A B E L

THE EUROPEAN LAND FORCE
COMMANDERS ORGANISATION