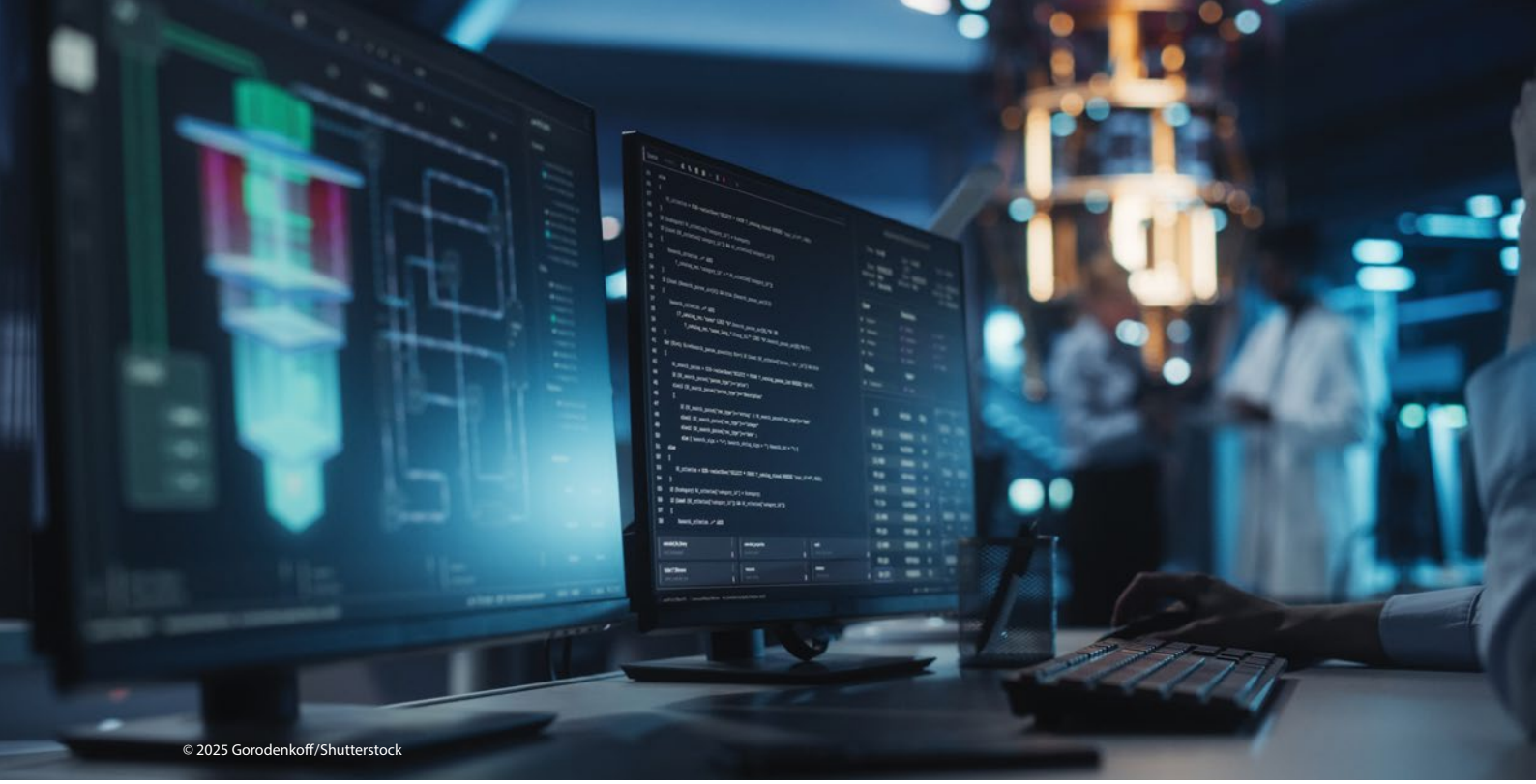


Quantum Technologies for NATO Air and Space Power

Military Risks, Operational Implications, and the Imperative for Allied Action

By Lieutenant Colonel Nakul Nayyar, CAN AF, JAPCC
& 1st Lieutenant Dr. Matthias Rößler, DEU AF, JAPCC

Once confined to academic laboratories, recent advances in quantum technologies have the potential to affect key enablers of NATO Joint Air and Space Power. Among those key enablers are Air Command and Control (Air C2), intelligence-sharing, satellite communications, and cybersecurity.[1] Quantum computing, quantum communications, and quantum sensing are distinct fields within the universe of quantum technologies with differing levels of maturity, operational applications, and timelines for potential military relevance. Tracking this uneven technological evolution is essential for NATO to maintain its operational freedom of action and deliver joint air effects across the continuum of competition. This article focuses on quantum computing and secure Air C2, where centralised command, distributed control, and decentralised execution all depend on cryptographic integrity.

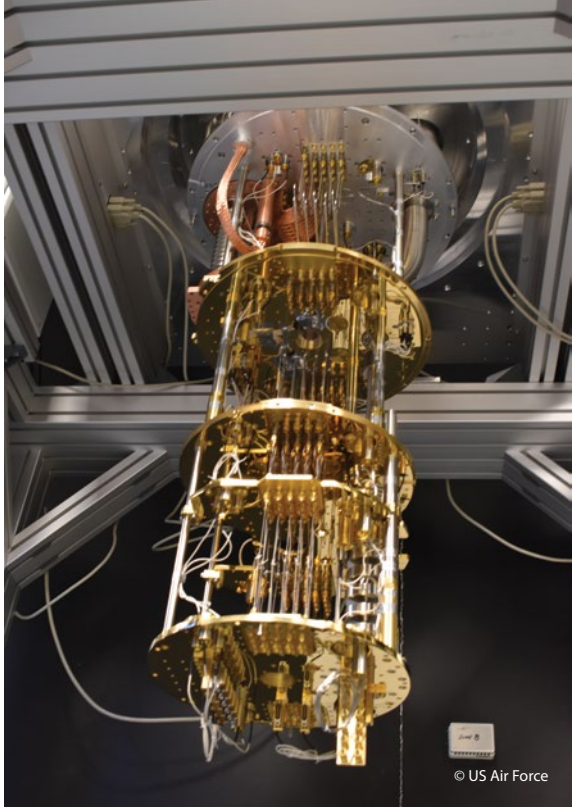
Unlike previous technological transitions, quantum computing does not merely introduce a new capability. It challenges the very assumptions underpinning NATO's digital Air C2 architecture, which relies on the premise that the encryption securing its communications is computationally infeasible to break. Consequently, preparing for the quantum era is not simply a technical modernisation effort, but an urgent operational imperative that requires synchronising post-quantum cryptography (PQC) standards, updating Allied joint doctrine, and establishing binding NATO procurement mandates.

Command and Control (C2) of allied air operations – the architecture this article argues is exposed to quantum-enabled cryptographic risk.

Secure Communications and Cryptographic Resilience in Air C2

Air C2 communications rely on cryptographic mechanisms to ensure confidentiality and integrity across NATO and coalition networks. In essence, a cipher scrambles a message according to a rule that only the intended recipient can reverse. Modern ciphers are trusted not because they are unbreakable, but because breaking them takes too long to be worth attempting. The dominant public-key cryptographic schemes in use, including Rivest-Shamir-Adleman (RSA) and elliptic-curve cryptography, derive their security from mathematical problems that classical computers cannot solve within operationally relevant timeframes.

Quantum computing represents a fundamentally different approach to computation, compared to the methods classical computers use today. Classical computers use binary bits for computation, which can only exist as either 0 or 1. Quantum computers, by contrast, use quantum bits, or qubits, which can exist in multiple states simultaneously through the principles of superposition[2] and entanglement.[3] This allows quantum computers to evaluate many possible solutions to a problem simultaneously and exploit quantum mechanical effects to identify the correct ones more efficiently than classical computers. As a result, quantum computers could potentially solve certain computational tasks in a timeframe that jeopardises the security of many current cryptographic systems. Two examples potentially affected are integer factorisation (breaking a large number down into the prime numbers that produce it) and discrete logarithm calculations (determining the exponent required to produce a known result within a mathematical group). Both would take classical computers impractically long periods to complete. Quantum computers move beyond classical computing by using Shor's algorithm, a specialised formula that solves these exact mathematical problems in minutes or hours.[4] This strips away the protection on which digital systems depend, undermining the security assumptions that form the basis of present-day encryption. For instance, researchers estimate that classical computers cannot factor a 2048-bit RSA key at all, but a large-scale, error-corrected quantum computer could in principle achieve this within days.[5] Although large-scale, fault-tolerant quantum computers remain under development, their projected capabilities have prompted growing concern regarding the long-term security of cryptographic systems that underpin modern military, governmental, and commercial communications.[6]



A cryogenic refrigerator at US Air Force Research Labs used to measure superconducting qubits – the first such demonstration at a US military service laboratory.

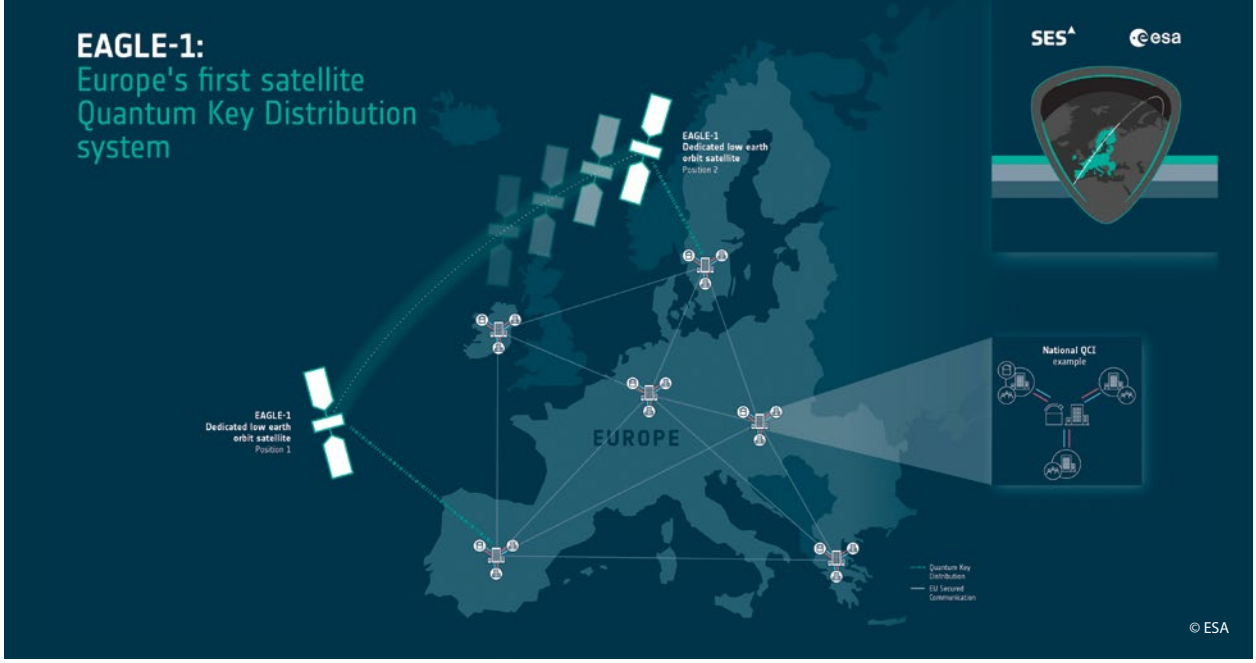
The risk posed by quantum computing to NATO communications does not depend on adversaries possessing a cryptographically relevant quantum computer today. Adversaries with mature signals intelligence programmes are already capable of intercepting and archiving encrypted NATO communications at scale; the barrier is not collection, but decryption. A more immediate concern is the 'store-now, decrypt-later' attack vector, in which they systematically harvest and archive encrypted Alliance communications, with the intention of decrypting them retrospectively once sufficient quantum capability becomes available.[7] For NATO Air C2, such cryptographic compromise could directly affect operations security (OPSEC) and Alliance interoperability. Exposure or manipulation of Air Tasking Order data, Air C2 messaging, or Tactical Data Link traffic could undermine trust in the Recognised Air Picture (RAP). It could also degrade the conditions necessary for centralised command, distributed control, and decentralised execution. In this context, quantum computing represents a systemic risk to Air C2, reinforcing the need for early transition to quantum-resilient cryptographic standards across the Alliance.

For NATO, this shift has two implications. First, the pace of quantum-enabled encryption and decryption capability development may accelerate, as commercial incentives will likely drive iterative improvements and deployment.[8] Second, access to quantum computing capabilities may progressively extend beyond a small number of state actors through commercial cloud-based services and international research partnerships. Major technology firms already provide limited access to quantum processors through cloud platforms, allowing universities, private companies, and smaller states to experiment with quantum applications without needing to build out their own quantum infrastructure. Adversary states and non-state actors that lack sovereign quantum programmes could nonetheless leverage cloud-based quantum resources to probe or attack cryptographic systems underpinning NATO communications. Continued advances in quantum computing and sustained state investments suggest that NATO defence planning must prepare for their eventual emergence. However, there are additional factors and challenges to take into consideration.

Quantum-Resistant Cryptographic Standards and the Migration Challenge

The most significant practical development in cryptographic resilience in recent years is the publication of finalised PQC standards by the National Institute of Standards and Technology (NIST). They comprise Federal Information Processing Standards 203, 204, and 205.[9] These standards rely on two mathematical safeguards to withstand quantum attacks: complex high-dimensional grids and irreversible one-way functions. Quantum algorithms cannot easily shortcut these mathematical problems, thus the encryption remains secure against both classical and quantum attacks. Consequently, NATO and its member nations now have standardised, implementable solutions available.

However, the challenge is not identifying the solution but executing the transition at Alliance scale. Migrating NATO Air C2 systems to quantum-resilient cryptographic standards is a complex, multi-year undertaking. The Air C2 architecture spans a wide range of national and multinational systems with different procurement timelines, certification requirements, and interoperability dependencies.



Eagle-1 will be the first European space-based quantum key distribution system, designed to launch by early 2027.

Another challenge lies in maintaining cryptographic interoperability across NATO and coalition networks during the transition to PQC. NIST standards provide a common technical foundation, and many NATO Air C2 systems rely on US-developed cryptographic equipment, key management infrastructures, and security architectures. Consequently, the modernisation of US military cryptographic capabilities and the availability of approved quantum-resistant solutions will shape NATO's migration timeline. During the transition period, legacy, hybrid, and PQC implementations will likely coexist across Allied networks, creating potential interoperability challenges that NCIA and national authorities must manage carefully. Ensuring smooth information exchange between NATO and national Air C2 systems will therefore be as important as the technical adoption of PQC itself. Additionally, a coordinated, NATO-wide migration plan is essential to avoid a fragmented transition in which some Allied systems achieve quantum resilience while others remain vulnerable, creating exploitable seams in the collective defence architecture.[10]

Overcoming these challenges to achieving successful migration of NATO Air C2 systems to PQC will require close coordination among three NATO bodies. These are the NATO Communications and Information Agency (NCIA), the NATO Consultation, Command, and Control Board (C3 Board), and Allied Command Transformation (ACT).[11] The C3 Board will play a central governance role by establishing Alliance-wide policy, interoperability requirements, and implementation priorities for quantum-resilient communications. ACT will incorporate PQC into future capability development, experimentation, and digital transformation initiatives, ensuring that emerging Air C2 concepts are designed with quantum resilience from the outset. Meanwhile, NCIA will serve as the principal technical implementation authority, translating policy and capability requirements into deployable solutions through system engineering, testing, certification, and integration across NATO networks and C2 systems. Together, these organisations will provide the governance, innovation, and technical expertise necessary to coordinate a coherent Alliance-wide transition while maintaining operational effectiveness and interoperability throughout the migration process.

Quantum Key Distribution: A Complementary, Not Alternative, Approach

Aside from quantum-proofing encryption algorithms by implementing PQC standards, another complementary approach to securing communications is through a technology called Quantum Key Distribution (QKD).[12] QKD offers a niche defensive option for securing especially sensitive Air C2 links. It enables the detection of interception attempts and provides security assurances that are independent of computational assumptions by exploiting the physical properties of quantum measurement. These characteristics fundamentally distinguish QKD from the PQC standards. Demonstrations of QKD over operational

NIST is an agency leading the charge on post-quantum cryptography for the government sphere.

fibre networks have shown increasing technical maturity over the past two years.[13] However, consistent with prior JAPCC analysis of quantum-enhanced technologies for the air and space domains, QKD should be considered as a complementary capability rather than a scalable solution for tactical airborne communications.[14] It is best suited to protecting high-value command links or critical nodes in both the air and space domains.

QKD payloads can operate within the size, weight, and power limits of small platforms, a key determinant of whether the technology scales. In 2019, the 2.6 kg satellite SpooQy-1 generated and detected entangled photon pairs in low Earth orbit, demonstrating that the entanglement sources underpinning QKD can operate on power- and compute-constrained platforms.[15] Moreover, the Eagle-1 satellite represents a major milestone in Europe's efforts to develop sovereign quantum-secure communications capabilities.[16] Developed through a partnership between the European Space Agency, the European Commission, and European space industry partners, Eagle-1 will demonstrate the feasibility of space-based QKD within the EU. It is due to launch in late 2026 or early 2027, followed by a three-year validation phase.[17] China, however, reached this milestone first. Its Micius satellite performed satellite-to-ground QKD over distances of up to 1,200 km and supported the first intercontinental quantum-secured video conference between Beijing and Vienna in 2017.[18] For now, the Alliance is not setting the pace with quantum for air and space power, but reacting to it.

Conclusion

The potential disruption of public-key cryptography by future adversary quantum computing presents a significant threat to NATO Air C2. NIST's PQC standards provide the technical blueprint, yet adversaries may already be harvesting encrypted communications against a decryption capability that does not yet exist. QKD complements that blueprint, offering assurance independent of computational assumptions for high-value command links and critical nodes in both the air and space domains. However, a quantum-resilient migration across NATO's federated Air C2 architecture is a complex undertaking, requiring close synchronisation with US cryptographic modernisation timelines.

As an Alliance structurally dependent on digital networks, shared situational awareness, and seamless multinational interoperability, NATO cannot afford a passive approach to quantum computing. By driving collaborative, Alliance-wide migration standards today, NATO will outpace adversary capabilities and safeguard its decisive operational edge for tomorrow. ●

1. Mosca, M., Piani, M., & Van Assche, G. (2023). Cybersecurity implications of quantum computing. Nature Reviews Physics, 5(5), pp. 249–262.
2. Superposition is the quantum property that allows a qubit to exist in multiple states simultaneously.
3. Entanglement is the quantum property that links qubits so that their states remain correlated even when separated by large distances.
4. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), pp. 1484–1509. https://doi.org/10.1137/S0097539795293172.
5. Gidney, C. (2025). How to factor 2048 bit RSA integers with less than a million noisy qubits. arXiv. https://arxiv.org/abs/2505.15917.
6. Bindel, N., Brendel, J., & Wolf, R. (2023). The long-term security of cryptographic systems in the quantum era. IEEE Security & Privacy, 21(4), pp. 42–50.
7. Alagic, G., et al. (2024). Status report on the first round of the NIST post-quantum cryptography standardization process. ACM Transactions on Privacy and Security, 27(1).
8. Zwerger, M., et al. (2024). Long-distance quantum key distribution in real-world networks. Physical Review Applied, 21(2).
9. National Institute of Standards and Technology. (14 August 2024). Announcing issuance of Federal Information Processing Standards (FIPS) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard. Federal Register. https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based.
10. North Atlantic Treaty Organization. (2024). Emerging and disruptive technologies: Strategic assessment update. NATO.
11. NATO Science and Technology Organization. (n.d.). Science & technology trends 2020–2040.
12. Zhang, H., et al. (2025). Towards global quantum key distribution. Nature Reviews Electrical Engineering, 2, pp. 806–818. https://doi.org/10.1038/s44287-025-00238-7.
13. Kumar, P., & Thomas, J. M. (June 2026). Building quantum networks on classical fiber infrastructure. Optics & Photonics News, 37(6), pp. 26–33. https://www.optica-opn.org/home/articles/volume_37/june_2026/features/building_quantum_networks_on_classical_fiber_infrastructure/.
14. Krelina, M., & Dúbravčík, D. (February 2023). Quantum technology for defence: What to expect for the air and space domains. JAPCC Journal, 35, 39–46. https://www.japcc.org/articles/quantum-technology-for-defence/.
15. Villar, A., et al. (2020). Entanglement demonstration on board a nano-satellite. Optica, 7(7), pp. 734–737.
16. European Space Agency. (n.d.). Eagle-1. ESA Connectivity and Secure Communications. Retrieved 13 August 2026, from https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1.
17. Ibid.
18. Liao, S.-K., et al. (2017). Satellite-to-ground quantum key distribution. Nature, 549(7670), pp. 43–47. https://doi.org/10.1038/nature23655.

ABOUT THE AUTHORS

Lieutenant Colonel Nakul Nayyar,
CAN AF, JAPCC

Lieutenant Colonel Nakul Nayyar is a Communications and Electrical Engineering (CELE) Officer in the Canadian Armed Forces and currently serves as the Cyber Subject Matter Expert at the Joint Air Power Competence Centre (JAPCC), a NATO Centre of Excellence in Kalkar, Germany. His work focuses on the operational implications of emerging technologies – particularly cyber capabilities, artificial intelligence, and autonomy – for NATO air power and multi-domain operations. Prior to his current role, he served in Washington, D.C., as the Canadian Communications and Electronics Defence Attaché to the United States. Lt Col Nayyar co-authored the white paper *AI Handbook: Practical Considerations for the Warfighter* and is currently contributing to a white paper on Military AI Governance, examining policy, accountability, and validation frameworks required for the responsible operational use of AI in defence.

1st Lieutenant Dr. Matthias Rößler,
DEU AF, JAPCC

1st Lieutenant Dr. Matthias Rößler is a Quantum Subject Matter Expert (SME) in the German Air Force and served as a Resident Fellow at the Joint Air Power Competence Centre (JAPCC) until July 2026. His work focuses on the impact and adoption of emerging disruptive technologies, combining his experience as a researcher, analyst, and strategist with political and defence perspectives. He currently serves as a research scientist and technology advisor for the European Commission's Quantum Flagship Initiative, and as a quantum SME to the German Armed Forces and NATO. 1st Lt Rößler holds master's degrees in physics and materials science, and a PhD in experimental condensed matter physics from RWTH Aachen University and the University of Cologne.