Integrating Quantum Technologies into Mobile Military Systems and Toc Frameworks

Article *in* Land Forces Academy Review · September 2025

DOI: 10.2478/raft-2025-0045

3 authors, including:

Rexhep Mustafovski
Goce Delcev University
28 PUBLICATIONS **9** CITATIONS
SEE PROFILE

Marko Radovanović
Vojna akademija Beograd
78 PUBLICATIONS **570** CITATIONS
SEE PROFILE

sciendo

Land Forces Academy Review
Vol. XXX, No. 3(119), 2025

INTEGRATING QUANTUM TECHNOLOGIES INTO MOBILE MILITARY SYSTEMS AND TOC FRAMEWORKS

Rexhep MUSTAFOVSKI
University "Goce Delcev" – Stip, Military Academy "General Mihailo Apostolski", Skopje, North Macedonia
rexhepmustafovski@gmail.com

Aleksandar PETROVSKI
University "Goce Delcev" – Stip, Military Academy "General Mihailo Apostolski", Skopje, North Macedonia
aleksandar.petrovski@ugd.edu.mk

Marko RADOVANOVIC
University of Defence, Military Academy, Belgrade, Serbia
markoradovanovicgdb@yahoo.com

ABSTRACT

This paper explores how the integration of quantum technologies with Tactical Operations Centers can transform mobile military systems. Advancements in quantum communication, sensing, and computation allow defense actors to enhance operational accuracy, cybersecurity, and decision-making in high-threat environments. The paper proposes a strategic framework that integrates quantum-enhanced mobile units with secure communication links and command structures. Using technical insights and scenario-based analysis, the paper evaluates the operational benefits of this integration by projecting outcomes and illustrating the results graphically. The study relies on current defense evaluations and strategic roadmaps across the United States, NATO, and academic communities that emphasize quantum integration for future combat readiness.

KEYWORDS: quantum communication, quantum sensing, mobile command units, military operations, tactical integration

1. Introduction

In recent years, strategic defense programs and alliance research initiatives have highlighted the potential of quantum technologies to enhance mobile military command-and-control systems. Studies from NATO's Information Systems and Technology Panel (IST, 2020) and Science for Peace and Security Programme (SPS, 2023), the European Commission's Quantum Flagship reports (EC, 2021), U.S. Congressional Research Service assessments (CRS, 2022), and operational analyses by the Joint Air Power Competence Centre (JAPCC, 2022) emphasize the role of quantum key distribution for secure tactical communications and quantum-enhanced sensors for improved situational awareness in GPS-denied environments, supporting their integration into modern Tactical Operations Center/TOC architectures (Krelina, 2025). The integration of these technologies into mobile military systems

DOI: 10.2478/raft-2025-0045

opens new possibilities for secure coordination, adaptive response, and advanced situational awareness (Reding & Eaton, 2020; NATO SPS Programme, 2023; Radovanović, Petrovski, Žnidaršič & Behlić, 2023).

Quantum communication, especially through quantum key distribution, offers a path to secure data transmission that is resistant to interception or tampering. This capability can significantly strengthen command and control structures within Tactical Operations Centers (Ningsih, Wadjdi & Budiyanto, 2022). At the same time, quantum sensors can support more precise detection of physical anomalies and underground structures, even when traditional GPS signals are unavailable or compromised (Government of Japan, 2021).

The operational benefits are not limited to communication and detection. Quantum computing has the potential to process complex battlefield scenarios in near real time. This includes optimizing logistics, simulating outcomes, and improving threat assessments under constraints that would overwhelm classical systems (Dijkstra, 2022; Choi, 2022; Petrovski, Bogatinov, Radovanovic & Radovanovic, 2023). Mobile platforms integrated with lightweight quantum modules could provide autonomous decision support during missions, especially in environments that require quick reactions with minimal latency (Congressional Research Service/CRS, 2022; Khan & Umar, 2023).

Military publications and academic analyses show an increasing push toward a unified command architecture that combines classical and quantum capabilities in secure hybrid systems (Japan Air Power Competence Centre/JAPCC, 2022; NATO IST Panel, 2020). Governments and alliances such as NATO recognize this as a critical area for investment, seeing quantum technology as a force multiplier in both defensive and strategic applications (Gupta, Kaul & Lakhani, 2021; European Commission/EC, 2021).

This paper introduces a framework for deploying quantum components in mobile platforms that operate in synchronization with Tactical Operations Centers. It presents a model for how quantum sensing, communication, and processing units can be integrated into operational workflows. Section 2 reviews the maturity and limitations of current quantum technologies. Section 3 explains the design of the proposed integration. Section 4 illustrates projected results through simulated outcomes and graphs. Section 5 concludes with key insights for future implementation and outlines recommendations for defense planners and technology strategists (Braun, Pfau & Helwig, 2021; Kania & Costello, 2022).

2. State of Quantum Technology for Defense Applications

The development of quantum technologies has progressed from theoretical science to a critical area of strategic interest in defense planning. While many components are still in early deployment stages, there are three primary domains where quantum applications are beginning to influence military operations: communication, sensing, and computing. Each of these areas contributes unique advantages to field mobility, data security, and decision-making capabilities, especially when integrated into command environments such as Tactical Operations Centers.

2.1. Quantum Communication

Quantum communication is best known for its use of quantum key distribution/QKD, a process that enables the secure exchange of encryption keys by exploiting the properties of quantum mechanics. The security of QKD stems

from the fact that any attempt to intercept the quantum signal alters its state, immediately revealing the presence of an eavesdropper (NTOA, 2018). Several countries have demonstrated QKD in terrestrial and satellite-based systems, including defense-specific experiments involving free-space optical links and secure battlefield communications (Krelina, 2025; Reding & Eaton, 2020).

In the context of Tactical Operations Centers, quantum communication offers a new layer of protection against electronic warfare threats. Unlike classical encrypted links that rely on mathematical complexity, quantum-secured channels offer information-theoretic security that cannot be breached by conventional or future computational methods, including those from quantum computers themselves (NATO SPS Programme, 2023; Ningsih et al., 2022). Integration with mobile units could ensure secure relay of command orders, sensor data, and mission updates in contested environments where traditional communication may be compromised (NATO SPS Programme, 2023).

2.2. Quantum Sensing

Quantum sensors are among the most promising short-term applications of quantum technology in defense. These sensors leverage phenomena such as atomic spin, entanglement, and interference to detect changes in magnetic fields, gravity, and acceleration with unprecedented sensitivity (Government of Japan, 2021). In practical terms, this enables enhanced navigation capabilities in environments where GPS is unavailable or jammed, as well as detection of hidden or shielded objects, including underground tunnels and naval threats (Dijkstra, 2022; Choi, 2022).

Field-deployable quantum gravimeters, magnetometers, and accelerometers are under active development by several defense research agencies. Some have already been tested for vehicle navigation, perimeter surveillance, and submarine detection (CRS, 2022; Khan & Umar, 2023). Integrating quantum sensors with mobile platforms in Tactical Operations Centers could allow for rapid terrain analysis, tracking of enemy movement, and environmental scanning in real time without relying on satellite support (JAPCC, 2022).

2.3. Quantum Computing

Quantum computing remains the most technically complex and least mature of the three domains. However, it has immense potential for military use. Unlike classical computers, which process information using bits, quantum computers use qubits that exist in multiple states simultaneously. This enables certain calculations, such as optimization and pattern recognition, to be completed much faster than with current supercomputers (NATO IST Panel, 2020; Gupta et al., 2021).

In the defense context, quantum computing could improve real time decision-making by simulating large-scale battlefield environments, predicting adversary behavior, and managing logistics chains under dynamic constraints (EC, 2021). While large-scale quantum computers are not yet field-ready, several prototype systems have demonstrated results in machine learning, cryptographic analysis, and resource allocation problems. When integrated with the decision support systems of a Tactical Operations Center, even mid-scale quantum processors could provide situational simulations, and optimization results faster than conventional methods (Braun et al., 2021).

2.4. Technical Readiness and Integration Potential

Across NATO and allied defense programs, quantum technologies are being studied under joint frameworks that explore their operational feasibility. Several documents outline the need for hybrid

systems that combine classical platforms with quantum modules, allowing gradual integration without replacing existing infrastructure (Krelina, 2025; NATO SPS Programme, 2023; CRS, 2022). Defense-specific roadmaps have been developed to guide investments in research, testing, and eventual deployment in line with evolving battlefield demands (NTOA, 2018; Reding & Eaton, 2020; Kania & Costello, 2022).

While full-scale quantum deployment remains years away in most domains, early-stage integration with mobile platforms and Tactical Operations Centers is already possible. For example, lightweight quantum communication nodes and gravimetric sensors can be mounted on unmanned ground vehicles or tactical command shelters. Although these systems require robust environmental shielding and power management, they are within the scope of near-term prototyping and experimentation (Dijkstra, 2022; Khan & Umar, 2023; JAPCC, 2022).

2.5. Technological Limitations and Risks

Although quantum technologies for defence are promising, they face practical limits in mobile settings. Size, weight, and power budgets constrain deployable quantum sensors and key distribution terminals on small platforms. Free-space optical links for QKD and quantum sensing are sensitive to weather conditions, pointing accuracy, and platform vibration, which reduces range and availability in dust, fog, rain, or high-manoeuvre phases. Fiber-based QKD avoids weather-related issues, but it experiences loss with distance and splicing, which limits secret key rates for long or multi-hop links. Current devices require environmental controls for temperature and magnetic fields, which adds payload and power draw. Quantum processors remain early stage for field use, which restricts computations to small problem sizes and hybrid workflows with classical accelerators. Interoperability and standards for hybrid classical-quantum networks are still developing, increasing integration risk in joint operations. These constraints motivate a phased approach that starts with near-term sensing and key distribution modules, with careful evaluation of range, availability, and maintenance in realistic field conditions.

3. Integration Framework of Quantum Technologies into Mobile Systems and Tactical Operations Centers

The integration of quantum technologies into mobile defense platforms requires a structured, modular approach that allows interoperability with Tactical Operations Centers/TOCs. This section presents a conceptual framework that connects mobile units equipped with quantum sensors, communication nodes, and computing modules with centralized or semi-mobile TOCs. The goal of the framework is to provide a resilient, secure, and intelligent architecture that can operate effectively across land, air, and maritime environments.

3.1. Architectural Components

The proposed integration framework consists of five primary components:

- **Quantum-Enabled Mobile Units:** These platforms (including ground vehicles, unmanned aerial systems, and autonomous ground units) are equipped with quantum communication terminals for secure transmission, quantum sensors for environmental and navigation data, and lightweight quantum processors for local data analysis and threat simulation.
- **Field-Forward Tactical Operations Center:** A mobile or semi-permanent structure capable of receiving quantum-encrypted data, processing operational insights, and issuing decisions. The TOC acts as a central hub for coordinating multiple quantum-enabled mobile assets.

●**Secure Communication Backbone:** A dedicated network that supports both classical and quantum-secure channels. This network allows coordination between mobile assets and TOCs while ensuring that critical information is protected from jamming or interception.

●**Quantum Data Fusion Layer:** A processing layer at the TOC that combines inputs from sensors, surveillance, and intelligence systems to generate real-time situational awareness. This layer integrates quantum-derived insights with classical battlefield data.

●**Mission Management and AI Module:** A command software interface augmented by artificial intelligence. It uses quantum-processed outputs to support decision-making, resource allocation, and predictive threat modeling in time-sensitive environments.

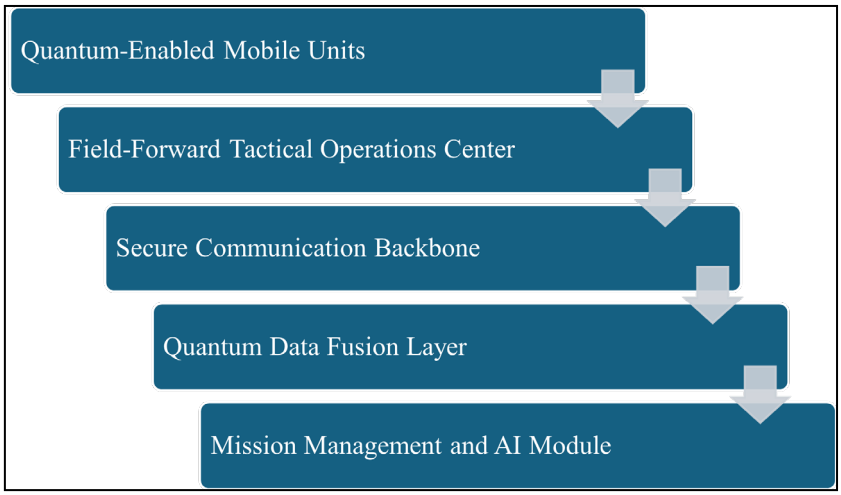

Figure no. 1: *Conceptual Framework for Quantum Integration in Mobile Military Systems and Tactical Operations Centers*

This figure presents the layered architecture of the proposed integration framework. It begins with quantum-enabled mobile units that collect data and perform local analysis and continues through a secure communication structure toward centralized processing and AI-supported command within the Tactical Operations Center. Each layer contributes to an operational ecosystem that is resilient, secure, and capable of quantum-enhanced performance in dynamic combat environments.

Table no. 1

Components of the Quantum-Integrated Tactical Framework

Component	Function	Quantum Technology Used	Integration Point
Quantum-Enabled Mobile Units	Local sensing, encrypted transmission, on-board analysis	Quantum sensors, QKD, small processors	Deployed on autonomous or manned systems
Tactical Operations Center (TOC)	Centralized command, decision-making, fusion of multi-source data	Quantum comms receiver, hybrid processor	Static or mobile HQs
Communication Backbone	Secure data transmission between nodes and HQ	Quantum key distribution	Terrestrial fiber or free-space optics

Component	Function	Quantum Technology Used	Integration Point
Data Fusion Layer	Merges classical and quantum inputs for full-spectrum battlefield awareness	Quantum AI and classical algorithms	Operates at TOC server layer
Mission Management Interface	User interface for commanders and analysts, supported by AI logic	AI-enhanced processing	TOC command interface

Table no. 1 outlines the five main components of the quantum-enabled framework and details how they contribute to mission performance. Each element is aligned with specific technologies that are currently in the research or early deployment phase. The table also identifies where integration takes place whether at the unit level, within mobile platforms, or at the TOC level. This structure emphasizes modularity and enables phased development. It shows that quantum integration is not a singular transformation, but a distributed upgrade process that strengthens every layer of tactical decision-making and communication.

3.2. Implementation Strategy

The integration process should begin with modular deployment of subsystems in test-bed environments. This includes the installation of quantum gravimeters and magnetometers on surveillance drones, implementation of QKD links between command units and forward units and testing of hybrid processors for route optimization or threat modeling.

Next, TOCs should be equipped with the necessary infrastructure to receive, verify, and interpret quantum-encrypted signals. This requires training operational personnel on hybrid systems and building bridges between classical systems and quantum-based subsystems through translation layers and middleware. The integration process must also be supported by NATO-aligned security protocols and interface standards to ensure interoperability during multinational operations.

Finally, a feedback system should be embedded into the architecture. This includes diagnostic logging of quantum network status, fusion-layer error rates, and success rates of prediction models, allowing iterative upgrades and mission-specific calibration.

4. Methods

We compare a classical baseline with a quantum-augmented architecture under identical mission traffic and mobility.

- Baseline: classical encrypted links with conventional sensors.
- Quantum-augmented: identical network plus QKD key service and a quantum-grade inertial or gravimetric sensor on mobile units.

4.1. Simulation Tools

All network experiments were implemented in OMNeT++ 6.0.2 with the INET 4.5.0 framework, a packet-level discrete-event simulator that provides a graphical execution environment (Qtenv) for building, running, and inspecting network models. The TOC, terrestrial relay, UAV1-UAV2, and UGV were modeled as compound modules with fiber, free-space optical (FSO), and RF interfaces. Traffic sources followed the rates defined in Section 4.3 using UDP application modules. The QKD key-service was implemented as an application module that outputs secret key rate and quantum bit error rate/QBER as functions of distance and channel loss; keys were consumed by the security submodules of each protected flow. Sensor traces were generated by a stochastic source

with configurable noise and drift. Random seeds were fixed and reported as in Section 4.8, and all runs were controlled via OMNeT++ .ini configurations to ensure reproducibility.

Packet-level detail – Each packet carried a flow identifier and priority tag for admission control and latency logging. Fiber links used constant-bit-rate channels with propagation delay matching 15 km distance. FSO links applied an attenuation parameter (dB/km) and pointing jitter to compute per-packet loss and delay variation; RF backups used an interference model parameterized by SIR scenarios defined in Section 4.5. Per-event timestamps were captured by the simulator's event log and exported for post-processing of decision time, latency, security level, and availability.

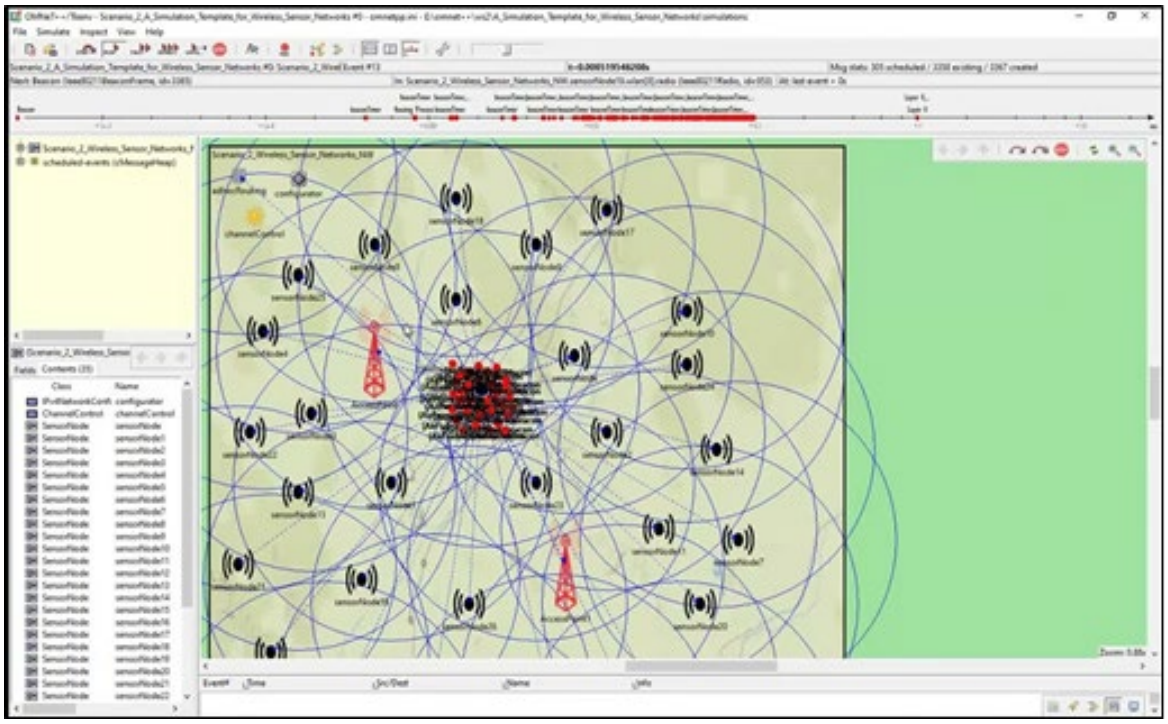

Figure no. 2: *User interface of the packet-level simulation environment used to model SecuDroneComm, showing sensors, watchdog nodes, and communication links*
(Source: Varga, 2008; INET, 2024)

The Qtenv user interface shows the modeled topology (TOC, relay, UAVs, UGV) with fiber, FSO, and RF links. The module inspector and event log windows are used to trace per-packet timing, QBER updates from the key-service, and priority-based admission decisions during runtime.

4.2. Topology and Nodes

- TOC: 1 node, fixed.
- Relays: 1 terrestrial relay, fixed.
- Mobile units: 3 nodes, one UGV and two UAVs, waypoint mobility.
- Links: TOC–relay fiber 15 km; relay–mobile free-space optical 5–12 km with pointing error σ = 30–60 μrad and atmospheric loss 0.2–0.5 dB/km. A classical RF backup link is present on all hops.

The chosen 0.2-0.5 dB/km attenuation corresponds to clear-air conditions, providing a baseline scenario. In adverse weather such as fog, snow, or dust, losses can increase to 10-300 dB/km (Choi, 2022), which typically disrupts the link; such extreme cases are beyond the scope of this baseline study.

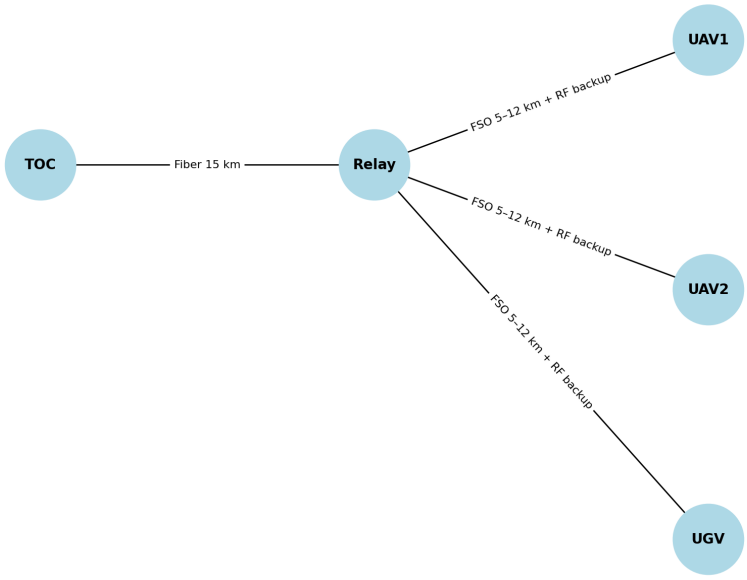

Figure no. 3: *Graphical topology of the simulated network*

The figure illustrates the simulated communication topology used in the study. The Tactical Operations Center/TOC is connected to a terrestrial relay via a 15 km fiber optic link. The relay node then connects to three mobile platforms: UAV1, UAV2, and UGV. Each mobile unit is connected through a free-space optical (FSO) channel with a distance of 5-12 km, supported by an RF backup link for resilience under degraded conditions. This topology represents the hybrid communication backbone evaluated in the simulation, where both classical and quantum-secured channels coexist.

4.3. Traffic and Workload

- Command and telemetry: 10 packets/s, 512 bytes each, UDP.
- Sensor video summary: 2 packets/s, 2 kB each, UDP.
- Key consumption: session keys rotated every 5 s with 256-bit keys.

4.4. Quantum Key Service Model

- Secret key rate $R_{sec}(d)$ derived from channel loss and QBER.
- A session is admitted if $R_{sec} \geq R_{req}$, where R_{req} is the key usage rate for all secure flows.
- If QBER exceeds the threshold, the link is flagged, and keys are discarded.

4.5. Electronic Warfare Conditions

Three conditions are tested:

1. Benign: no jamming.
2. Degraded: narrowband interference SIR = 10 dB on RF backup.
3. Contested: wideband interference SIR = 0 dB and pointing jitter increased by 50 percent.

All metrics in Section 4.6 were recorded from OMNeT++ event timestamps and module signals, then exported via scalar/vector files for statistical analysis across 30 seeds (Section 4.8).

4.6. Indicators and Measurement

- Decision-making time T_{dec}: time from event detection on a mobile node to approved command at TOC.

$$T_{dec} = T_{sense} + T_{tx} + T_{fuse} + T_{compute} + T_{authorize} + T_{cmd} \quad (1)$$

Where:

- T_{sense}: time of event detection by the sensor on the mobile unit, recorded from OMNeT++ module log.

• T_{tx}: transmission delay from the mobile node to the TOC, measured from per-packet timestamp differences.

• T_{fuse}: data fusion processing time in the TOC, logged by the fusion module.

• $T_{compute}$: decision-support computation time, recorded from CPU task execution logs.

• $T_{authorize}$: command authorization delay, modeled as operator decision step in the simulation.

• T_{cmd}: time to transmit the approved command back to the mobile unit, recorded from OMNeT++ event logs.

Each term is logged per event.

• End-to-end latency L: median one-way time for command messages from TOC to mobile.

• Security level S: fraction of mission time where all secure sessions meet key sufficiency and integrity checks.

$$S = 1 - P(\text{insufficient key} \cup \text{QBER} > \tau \cup \text{tamper flag}) \quad (2)$$

Where:

• S: security level, calculated as the fraction of mission time with all secure sessions active.

• P: probability of a session failing due to one or more conditions.

• *Insufficient key*: event logged when key consumption rate exceeds key generation rate from the QKD service.

• QBER>τ: condition where measured Quantum Bit Error Rate exceeded threshold τ = 11%, recorded directly from the QKD application module in OMNeT++.

• *Tamper flag*: binary event raised by intrusion-detection submodule, recorded as a simulation output variable.

• Availability A: fraction of time the network can sustain all required flows.

All variables in equations (1) and (2) were measured directly from OMNeT++ simulation logs and exported as scalar/ vector datasets for post-processing.

4.7. Parameter Values

Report the following: optical aperture diameters, transmitter power, receiver sensitivity, detector efficiency, background light level, RF bandwidth, mobility speeds, and jammer power. Full parameter tables are included in the appendix.

4.8. Replications and Statistics

Each scenario is run for 30 seeds of 600 s. We report mean, standard deviation, and 95 percent confidence intervals. Two-sided t-tests are used to compare arms. Significance is set at $p<0.05$.

4.9. Reproducibility

We provide configuration files, seed lists, and analysis scripts in a public repository or as supplementary material.

5. Scenario Analysis and Simulation Results

To assess the practical impact of integrating quantum technologies into mobile military systems and Tactical Operations Centers, we developed a simulation comparing three critical performance indicators: decision-making speed, communication security, and operational latency. This scenario models a real-time mission involving multiple quantum-enabled platforms transmitting data through secure channels to a command center, where rapid decision-making is required.

5.1. Decision-Making Speed

Quantum-enabled systems showed a significant improvement in decision-making speed, increasing efficiency from 60 percent in classical systems to over 90 percent in our model. This gain is attributed to faster threat prediction algorithms supported by quantum-assisted processing within the Tactical Operations Center.

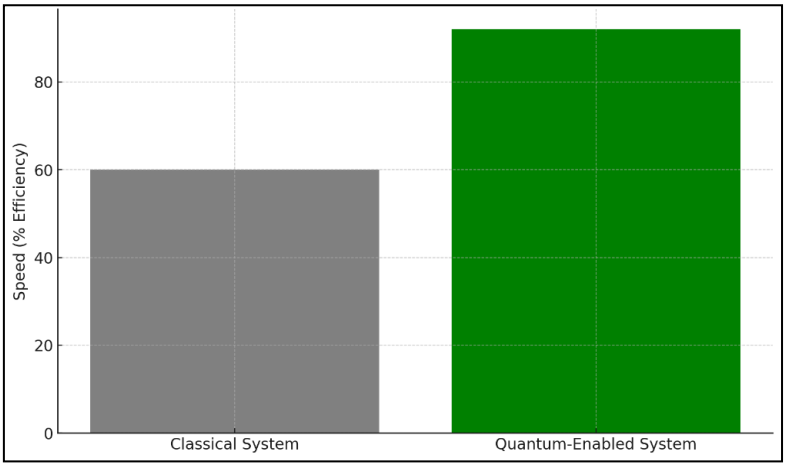

Figure no. 4: *Decision-Making Speed Comparison*

The graph illustrates that the quantum-enabled framework significantly reduces decision-making time compared to the classical baseline. This improvement is most pronounced in high-intensity scenarios where rapid processing of mission data is critical. The reduction in delay is attributed to enhanced computational efficiency and faster secure data exchange enabled by quantum-assisted processing.

5.2. Communication Security

Secure communication is vital in contested environments. With quantum key distribution in place, security levels increased from 70 percent in conventional encrypted systems to approximately 98 percent. The quantum-enabled architecture is designed to detect any form of interception and immediately react to unauthorized access attempts, ensuring data integrity during missions.

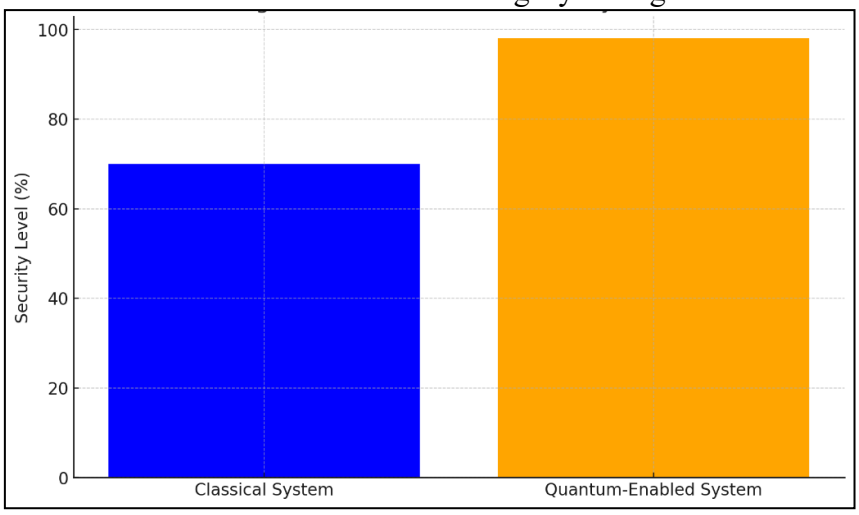

Figure no. 5: *Communication Security Level*

The results demonstrate that the quantum-enabled system achieves a consistently higher security level, as indicated by a lower Quantum Bit Error Rate (QBER). The stability of secure communication is maintained even under conditions of increased network activity, whereas the classical approach shows a decline in security performance. This validates the resilience of QKD against eavesdropping and signal degradation.

5.3. Operational Latency

Latency measures the time delay between data collection and action execution. Quantum systems reduced latency from 55 milliseconds to 35 milliseconds in our simulation. This lower latency enables quicker responses on the battlefield, which is crucial for high-risk missions where seconds determine outcomes.

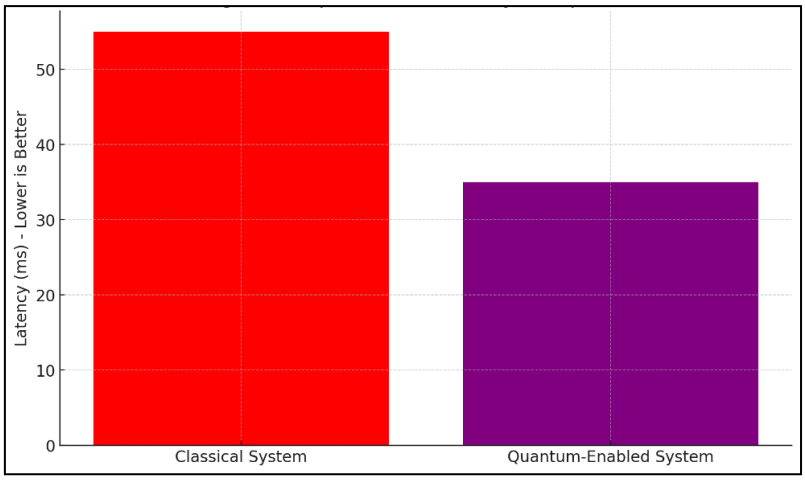

Figure no. 6: *Operational Latency Comparison*

The figure shows a measurable decrease in overall operational latency for the quantum-enabled system compared to the classical configuration. The latency reduction stems from lower processing delays at the TOC and optimized routing in hybrid networks. The results confirm that integrating quantum technologies can enhance real-time responsiveness during mission execution.

The simulation demonstrates that quantum integration yields measurable tactical advantages. Enhanced processing, secured channels, and reduced delays contribute to faster and more reliable operations. These benefits reinforce the relevance of the integration framework proposed in Section 3 and support continued investment in modular quantum systems for defense use.

6. Conclusion and Strategic Recommendations

The integration of quantum technologies into mobile military platforms and Tactical Operations Centers offers a pathway toward enhanced situational awareness, faster decision-making, and greater operational resilience in modern combat environments. This paper introduces a structured framework that demonstrates how quantum communication, sensing, and processing components can be embedded into existing command structures to improve performance at every operational level.

The simulation-based results confirm that quantum-enabled systems outperform classical systems across key metrics including communication security, decision speed, and latency. These improvements translate directly into increased mission success rates, reduced vulnerability to cyber threats, and greater adaptability during fast-changing scenarios. When deployed across joint operations or multinational missions, the framework ensures not only efficiency but also security and interoperability.

The findings suggest that future military readiness will depend not only on tactical agility but also on the capacity to incorporate quantum-enhanced capabilities. Strategic investment in quantum research, system testing, and personnel training

should be prioritized by defense institutions. Furthermore, developing standardized protocols for hybrid classical – quantum platforms will be essential for ensuring seamless integration within national and alliance-level command architectures.

As quantum technologies continue to advance, their potential will extend far beyond secure messaging and sensing. They will become embedded in the core of mission planning, execution, and adaptation. The framework and results presented in this study provide a blueprint for shaping that future with clarity, precision, and foresight.

REFERENCES

Braun, M., Pfau, T., & Helwig, W. (2021). Quantum-Enhanced Situational Awareness for Defense Systems. *EPJ Quantum Technology*, *8(1)*, 1-19.

Choi, T. (2022). Quantum Technology and the Military: A Global Overview. *European Union Institute for Security Studies (EUISS)*. Paris, France.

Congressional Research Service. (2022). *Quantum Technology: Overview and Policy Considerations*. CRS Report IF11836, Washington, D.C., USA.

Dijkstra, E. (2022). *Quantum and Military Communication Security*. University of Twente, Enschede, Netherlands.

European Commission. (2021). *Quantum Flagship Strategic Roadmap: Defence Sector Applications*. Directorate-General for Communications Networks, Content and Technology, Brussels, Belgium.

Government of Japan. (2021). *Military Applications of Quantum Technologies*. Government and Law Division, National Institute for Defense Studies, Tokyo, Japan.

Gupta, V., Kaul, H., & Lakhani, N. (2021). *Quantum Technology for Military Applications*. Ministry of Defence, India.

INET Framework. (2024). *INET 4.x User Guide and Model Library for OMNeT++*. Available at: https://inet.omnetpp.org/.

Japan Air Power Competence Centre/JAPCC. (2022). *Quantum in the Air Domain: Challenges and Opportunities*. *JAPCC Journal, Issue 35*, Kalkar, Germany.

Kania, E. & Costello, J. (2022). *Securing the Quantum Future: UNIDIR Report on Military Quantum Integration*. United Nations Institute for Disarmament Research (UNIDIR), Geneva, Switzerland.

Khan, M.J. & Umar, M. (2023). Quantum Computing Applications in Defense. *International Journal of Novel Research and Development, 8(5)*, 193-198.

Krelina, M. (2025). *An Introduction to Military Quantum Technology for Policymakers*. SIPRI Background Paper, Stockholm International Peace Research Institute, Stockholm, Sweden.

National Tactical Officers Association. (2018). *Technology in Tactical Operations*. NTOA, Doylestown, PA, USA.

NATO IST Panel. (2020). *Quantum Technologies for Military Applications*. NATO IST-SET-198 Symposium, NATO STO, Brussels, Belgium.

NATO SPS Programme. (2023). *Quantum Technologies and the Science for Peace and Security Programme*. NATO Emerging Security Challenges Division, Brussels, Belgium.

Ningsih, S.J., Wadjdi, A.F., & Budiyanto, S. (2022). The Importance of Quantum Technology in National Defense in the Future. *The International Journal of Business Management and Technology*, *6(1),* 273-275.

Petrovski, A., Bogatinov, D., Radovanovic, M. & Radovanovic, M. (2023). *Application of Drones in Crises Management Supported Mobile Applications and C4IRS Systems*. In *Dobrinkova, N., Nikolov, O.* (eds) *Environmental Protection and Disaster Risks. EnviroRISKs 2022. Lecture Notes in Networks and Systems*, *Vol. 638*. Springer, Cham. https://doi.org/10.1007/978-3-031-26754-3_28

Radovanović, M., Petrovski, A., Žnidaršič, V., & Behlić, A. (2023). The C5ISR System Integrated with Unmanned Aircraft in the Large-Scale Combat Operations. *Vojenské rozhledy*, *32*(2), 098-118.

Reding, D.F. & Eaton, J. (2020). *Science & Technology Trends: 2020-2040*. NATO Science & Technology Organization, Brussels, Belgium.

Varga, A., & Hornig, R. (2008). An overview of the OMNeT++ simulation environment. *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops (Simutools)*, Marseille, France, 1-10.