World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Quantum Technologies and AI in National Defense: The Strategic Role of Quantum Networks in Contemporary Geopolitics

Martha Monique Nogueira Rodrigues [1, *], Thays Felipe David de Oliveira [1], João Vinícius Jobim Rosa [2] and Fernando Manuel Araújo Moreira [1]

[1] *Military Institute of Engineering (IME), Nuclear Engineering Section, Rio de Janeiro, Brazil.*
[2] *Military Institute of Engineering (IME), Section of Fortification and Construction Engineering, Rio de Janeiro, Brazil.*

World Journal of Advanced Research and Reviews, 2025, 28(03), 551-565

Publication history: Received on 29 October 2025; revised on 03 December 2025; accepted on 06 December 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.3.4086

Abstract

Quantum networks are connections between quantum processors and repeaters that produce, exchange, and process quantum information. They serve to optimize the transmission of data in the form of quantum bits, known as qubits. Quantum networks were developed to complement classical networks in order to solve problems currently considered impossible. Among these applications are quantum key distribution (QKD), clock synchronization, secure remote computing, metrology, and distributed consensus. The objective of this work is to investigate the technological foundations, their strategic applications, and consequences in geopolitics. Specifically, this article addresses applications in energy sectors considered strategic, such as oil and gas and nuclear energy. Combined with Artificial Intelligence (AI), this technology can accelerate the discovery of wells and the processing of company analyses, making carbon capture more efficient. In nuclear reactors, quantum computing represents a significant advance. Its advantage lies in its ability to perform more precise simulations of nuclear reactions, for example, neutron scattering, fission and fusion processes, and the exploration of extreme environments that are difficult or impossible to reproduce in the laboratory. Furthermore, this article also analyzes the geopolitical impact of this scenario, emphasizing the technological race and strategic disputes. Next, the challenges and perspectives regarding technical barriers, regulatory issues, and the future of quantum networks in the energy matrix are discussed. To conclude this work, reflections are made on methods to achieve the safe and ethical integration of these quantum technologies.

Keyword: Network; Quantum; Intelligence; Artificial; Energy; Geopolitics

1. Introduction

According to [1], Quantum Information Science (QIS) has four pillars (quantum sensing and metrology, quantum networks, quantum simulations, and quantum computing), as shown in Figure 1. Each area plays a strategic role in technological and energy evolution. Among these pillars, quantum networks emerge as a promise to make connections faster and more secure.

The geopolitical scenario is characterized by energy transition, the need for decarbonization, expansion of renewable sources, and growing energy demand. In this context, there is a need to reconfigure critical infrastructure and implement more digitized and interconnected systems, such as smart grids and decentralized microgrids [2].

Based on phenomena such as quantum entanglement and quantum key distribution (QKD), quantum networks offer highly secure communication from a theoretical point of view. For the energy sector, especially interconnected electrical grids and hybrid systems such as nuclear, wind, oil, and gas, reliability is essential to prevent cyberattacks [3-4].

* Corresponding author: Martha Monique Nogueira Rodrigues

To improve energy transition management, quantum networks are integrated with artificial intelligence, resulting in secure quantum connections between operations centers, laboratories, and power plants, where it is possible to perform power flow simulations, fault prediction, and efficient responses to critical events [5], which are fundamental capabilities in a complex energy system where any incident can have international impacts.

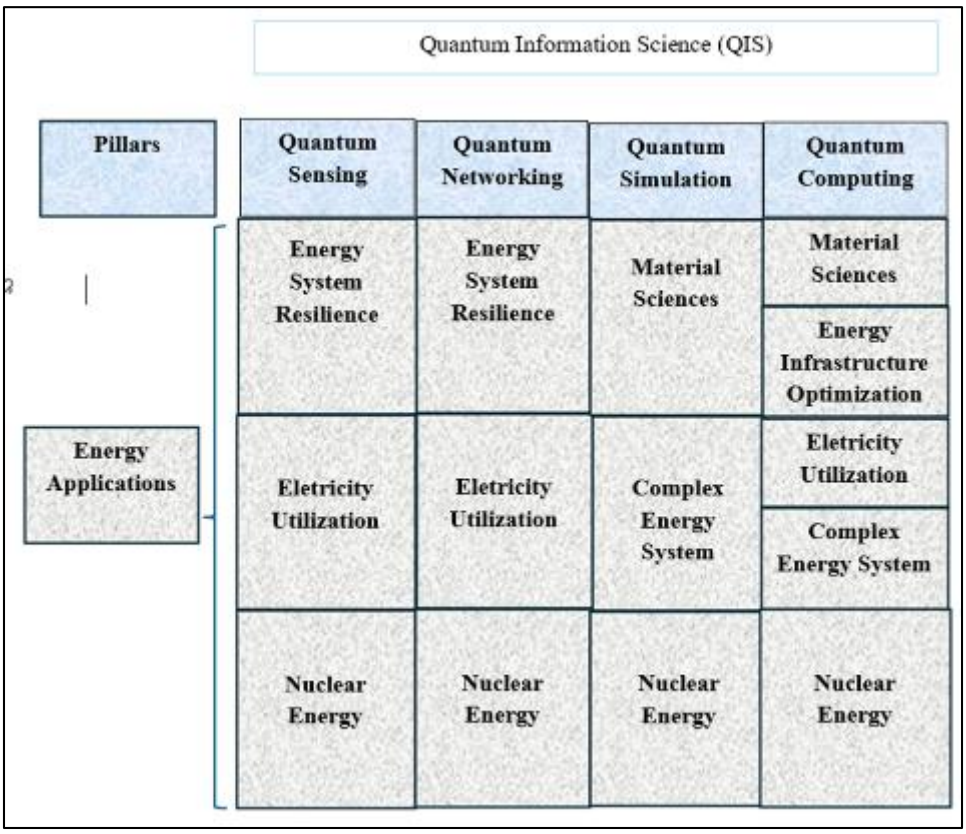

Figure 1 The four pillars of Quantum Information Science and possible applications in different areas of energy research and engineering [1]

In the geopolitical and technological context, the nation that has the knowledge and mastery of the quantum network will be at the forefront of cyber resilience and industrial innovation. China, the United States, and the European Union lead the race for quantum supremacy and influence defense policies and international agreements [6].

The scale of the impact of this technological integration makes it necessary to understand and map opportunities, risks, and practical applications with a view to security, sustainability, and innovation in strategic sectors.

This raises the question: how can quantum networks, combined with artificial intelligence, protect strategic energy sectors from cyberattacks?

The objective of this study is to analyze the potential of quantum networks, integrated with Artificial Intelligence, and their application in energy sectors, such as nuclear, oil, and gas, in the context of energy transition and decarbonization, to strengthen reliability and optimize operational efficiency by increasing technological competitiveness [1].

This paper takes an integrated temporal approach, addressing the current state of cybersecurity in strategic sectors, emerging quantum technologies in the experimental phase and their future prospects, and discussing their impacts on the energy transition and geopolitical competition.

2. Technical Fundamentals (Quantum Networks / Artificial Intelligence (AI)) applied to quantum networks

The evolution of quantum communications has been driven by advances in quantum entanglement networks, distributed quantum computing, and quantum sensor networks [7].

This progress was possible because quantum networks use fundamental properties of quantum mechanics, mainly entanglement and superposition, which offer advantages in security and efficiency [8]. They are composed of quantum nodes interconnected through communication channels, allowing the transmission of qubits and the creation of quantum entanglement between different parts of the network [9], in addition to the use of quantum channels and repeaters.

The purpose of these networks is to enable applications such as quantum state teleportation, quantum key distribution, and distributed quantum computing—processes that become even more optimized when integrated with Artificial Intelligence (AI). Among these innovations, Quantum Key Distribution (QKD) networks stand out, which are already in operation, with successful implementations in several regions [10-11].

The application of AI to QKD helps improve the predictability of attacks and failures, highlighting anomalies known as black hole repeaters, which compromise the integrity of repeaters in complex networks [12]. AI also uses machine learning to optimize routes, adjust switching protocols in real time, and automatically classify suspicious events.

AI is capable of performing real-time analysis, identifying complex patterns in large volumes of data, and detecting subtle events through neural networks and probabilistic models [13-14]. In addition, it enables self-calibration and self-adjustment of sensors—essential functions in thermally and electromagnetically unstable environments—and generates maps that predict variations in magnetic fields, gravitational acceleration, and radiation [15].

AI, in conjunction with quantum networks, ushers in a new era of independent, secure, and responsive systems, representing a fundamental advance toward the quantum internet and the strategic use of emerging technologies for geopolitical purposes.

To better understand how this integration manifests itself in practice, we will address three fundamental applications of artificial intelligence in the context of quantum communications: network routing, error correction and mitigation, and monitoring with optimization.

To better understand how this integration manifests itself in practice, we will address three fundamental applications of artificial intelligence in the context of quantum communications: network routing, error correction and mitigation, and monitoring with optimization.

In the first case, the main challenge is to select the ideal “path” for transmitting qubits between nodes—a complex task, subject to critical errors such as decay, decoherence, and entanglement loss. In this context, Reinforcement Learning (RL) algorithms, such as Proximal Policy Optimization (PPO), stand out for their simplicity of implementation and robust performance in various types of problems [16].

For more demanding applications, such as in Quantum Key Distribution (QKD) optical networks, Deep Reinforcement Learning (DRL) algorithms are used, capable of simultaneously solving routing and resource allocation problems [17].

In the second domain, quantum communications are highly sensitive to noise and multiple forms of interference. Deep Learning (DL) models can correct error patterns more quickly and efficiently than classical methods, such as CRC, Hamming, Reed–Solomon, or LDPC codes, which introduce redundancy into the transmitted data, allowing for the detection and correction of transmitted bits.

In conventional systems, an erroneous message can simply be retransmitted using an ARQ (Automatic Repeat Request) protocol. However, this model does not apply to quantum networks: measurement destroys the quantum state, and the no-cloning theorem prohibits the replication of quantum information.

Deep learning models — especially transformer-based neural networks (such as current large language models, LLMs)—surpass traditional decoders in surface code implementations, resulting in significant advances in Quantum Error Correction (QEC) [18].

In addition, it is worth highlighting the ability to self-calibrate: neural networks can automatically calibrate quantum photonic sensors using only training data, without the need for detailed device modeling. This approach treats the sensor as a “black box,” dramatically reducing the resources and time required for calibration compared to manual procedures [19].

Finally, in the third area, AI enables real-time analysis of physical parameters (such as optical losses, temperature, and synchronization), automatically adjusting the emission and reception systems to ensure stability and efficiency in key transmission or entanglement. In practice, optimizing these parameters is essential to maximize the secret key generation rate. However, classic Local Search Algorithms (LSA) are often slow and limited by the computational capabilities of devices [20].

Artificial intelligence and machine learning have significantly improved both the efficiency and security of quantum communications. These methods enable ultra-secure, reliable, large-scale communication, contributing to the development of a future quantum internet capable of analyzing protocols and mitigating noise-induced errors caused by noise during quantum data transmission [21].

3. Applications in Nuclear Energy and Oil & Gas

The nuclear energy, oil, and gas sectors require constant attention to safety, communication, and the most accurate measurements. The integration of quantum networks, Artificial Intelligence (AI), and quantum sensors represents a strategic advantage for sectors such as nuclear and oil and gas, where the accuracy, safety, and reliability of monitoring systems are essential.

The role of these integrations in these sectors will be discussed below, highlighting how the characteristics of each sector influence the applications, challenges, and opportunities of these emerging technologies.

3.1. Nuclear Energy

New reactor designs feature advanced technologies such as remote monitoring and semi-autonomous operation, with the aim of reducing economic costs, leveraging passive safety systems, and enabling support for different types of energy production [22].

Nuclear security consists of prevention, detection, and response measures to prevent theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving nuclear material and other radioactive substances and their associated facilities. Responsibility for nuclear security lies with national governments [23].

Attackers almost always begin by gathering information about the target system to identify the network topology, software versions, authorization or authentication mechanisms, and critical targets. Therefore, the first critical layer of defense against attacks is to ensure the confidentiality and authentication of any communication [24]. One of the most well-known cyber-attacks on a nuclear power plant was the Stuxnet virus attack in 2008, developed by the US in partnership with Israel, whose goal was to paralyze Iran's nuclear power plants [23].

However, the first attack on an operating civilian nuclear power plant was carried out by an armed group during Russia's military action in Ukraine in early 2022.

Incidents such as these show that, despite all the technology in the nuclear field, there are critical vulnerabilities. To reduce them, cryptographic implementation was proposed by the US Nuclear Regulatory Commission (US NRC) in 2010 through Regulatory Guide 5.71 [25], but there is no public document confirming that any plant has implemented all the requirements, even though nuclear plants used in licensing or modernization processes often include security plans proposed by the US NRC [26].

However, in 2024, the National Institute of Standards and Technology (NIST) published the first official post-quantum cryptography standards, which should gradually complement existing guidelines, such as RG 5.71, against cyber-attacks from a quantum computer [27].

Current cryptographic schemes are based on the computational complexity of public-key cryptography. Unfortunately, however, public-key cryptography has been shown to be vulnerable to the advent of quantum computers and Shor's algorithm [28-30]. In [31], predictions about the evolution and scalability of quantum computers are cited as an example, indicating that they could compromise public key cryptography (RSA) in a matter of hours if sufficiently large and stable machines were built.

Theoretical information security — that is, unconditional security—can be achieved by implementing the One-Time Pad (OTP) symmetric encryption algorithm, which requires that the communicating parties have access to truly random and continuously updated keys that are equal in size to the encrypted data [32]. Despite its perfect theoretical security, its

application is difficult, because the parties share and store many secret keys that are the same size as the transmitted data, which makes synchronization and distribution of large-scale systems unfeasible [33].

There are already initiatives to implement large-scale quantum computers in the next decade. Among them are the US National Quantum Initiative Act [34], Google's Quantum Artificial Intelligence Lab, which plans to commercialize quantum computers [12-13, 35], IBM Q [14-15], among others.

With the advancement of quantum computers and, consequently, the weakening of classical systems, there is a need to develop security mechanisms based on quantum mechanics. One notable example is Quantum Key Distribution (QKD), which allows two parties, connected by optical interfaces, to generate secure random keys through a quantum channel that is immune to espionage threats [36].

Research indicates that integrating this technology into next-generation nuclear systems could provide significant benefits, enabling safe, autonomous, and unsupervised operation in remote areas, such as in micro reactors and fission batteries. A recent study successfully demonstrated the implementation of Quantum Key Distribution (QKD) in a fully digital nuclear reactor (PUR-1). Achieving high-performance real-time encrypted communication—including secure transmission of encrypted data via optical fibers for up to 140 km, with low latency and high stability, increasing resilience against future cyber threats [24].

It is also possible to further improve the monitoring of nuclear activity with the implementation of artificial intelligence algorithms to calibrate quantum sensors and the improvement of sensing technologies, as in the case of neutrino detectors being developed for non-invasive surveillance of nuclear reactors, allowing the identification of their activity level or possible operational deviations, with major implications for non-proliferation [37].

At the same time, it is possible to use radiation sensor networks in urban environments that enable the continuous and intelligent detection, location, and tracking of radiological materials, significantly improving nuclear security [38].

The successful integration of Quantum Key Distribution (QKD) in nuclear reactors, as demonstrated at the PUR-1 facility, lays the foundation for secure quantum communications. However, quantum cryptography alone addresses only one dimension of nuclear cybersecurity. To achieve truly resilient and autonomous nuclear systems, quantum security must be augmented with artificial intelligence capabilities that enable real-time anomaly detection, predictive maintenance, and adaptive system optimization. This convergence of AI and quantum technologies transforms nuclear facilities from passively secure infrastructures to actively intelligent infrastructures.

The integration of Artificial Intelligence (AI) with quantum technologies, such as QKD, establishes a new paradigm of operational and cyber security for nuclear systems. While QKD ensures the confidentiality and authenticity of communications [11], AI acts as a cognitive analytical layer, capable of detecting and mitigating failures in real time. This convergence reinforces both the physical and informational resilience of nuclear power plants, enabling autonomous operation and intelligent monitoring of critical infrastructure.

In the context of operational safety, AI optimizes risk management through predictive models that detect anomalies and probabilistically assess critical failures before they occur [39]. Unlike traditional approaches based on thresholds or fixed rules, machine learning algorithms recognize complex, nonlinear patterns in data from thermal, radiation, and flow sensors, reducing false alarms and increasing the reliability of safety decisions.

A recent advance is presented by Chaudhary et al. (2024) [40], who developed a Bi-LSTM neural network model applied to the simulated Asherah NPP nuclear plant. The system achieved 100% accuracy and recall, with a false positive rate of zero, in detecting anomalies induced by cyberattacks. The statistical detection threshold was set to MSE ≈ 0.007, allowing anomalies to be identified up to 54 seconds before the Reactor Protection System (RPS) was activated, thus enabling preventive and preemptive actions. In addition, the model employs Explainable AI (XAI) techniques, such as the SHAP method, to identify the most influential variables — average reactor temperature, pressure, and flow — ensuring transparency and auditability in the decision-making process. These results reinforce the role of AI as an element of trust and interpretability in critical nuclear infrastructures.

In addition, AI is widely used for noise filtering and adaptive calibration of measuring instruments. Neural models distinguish operational noise from fault signals, automatically adjusting sensor parameters according to environmental variations. This self-correcting capability eliminates much of the need for manual intervention, reducing maintenance time and improving the accuracy of continuously operating solid-state radiation detectors and high-sensitivity neutron flux sensors [41]. In more advanced applications, neuromorphic sensors integrate learning circuits directly into the

hardware, enabling autonomous response and dynamic reconfiguration under thermal or electromagnetic fluctuations—an essential feature for small modular reactors (SMRs) and next-generation microreactors [41].

At the same time, AI is widely incorporated into the design and simulation of nuclear systems, replacing empirical correlations and deterministic models with hybrid machine learning approaches. These methods enable dimensionality reduction, reduced-order modeling, and highly efficient thermohydraulic and neutron analyses, maintaining computational accuracy at a lower cost. Recent studies conducted in Spain demonstrate the successful use of deep neural networks (DNNs), convolutional neural networks (CNNs), and Bayesian networks in safety analyses, fuel cycle optimization, and uncertainty quantification in nuclear reactor design—consolidating AI as an indispensable tool throughout the life cycle of a nuclear project [42].

Together, these applications demonstrate that Artificial Intelligence not only complements the security provided by quantum networks, but also enhances the autonomy, efficiency, and adaptability of modern nuclear systems. The result is an infrastructure capable of operating under the principles of predictive and informational security, combining quantum cryptography with adaptive intelligence—a decisive step toward the next generation of autonomous digital reactors and intelligent energy systems.

The same principles of integration between AI and quantum technologies are becoming increasingly relevant in other energy-intensive sectors, notably oil and gas, where process safety and predictive analytics play equally critical roles.

3.2. Oil and Gas

With the evolution of quantum networks, ways have been developed to monitor, control, and distribute energy more safely and reliably compared to existing networks. These methods include analyzing global CO_2 emissions, using automation technology in fossil fuel infrastructure to make it safer and more efficient, and modernizing the energy network using quantum technologies. In the long term, quantum networks are expected to be used to distribute cryptographic keys to protect energy data and make energy supply more reliable [1].

Also, according to Crawford et al. [1], quantum networks can be used in CO_2 emission sources, such as coal plants, industries, ships, and vehicles equipped with quantum technologies. Measurement units, such as quantum sensors, can connect to an advanced communication network to assess emissions with greater accuracy and sensitivity.

In 2014, NASA launched its carbon observatory in orbit—OCO-2—to monitor CO_2 emissions in the Earth's atmosphere with a resolution of 1 to 3 km [43]. This was considered a computationally complex problem, as it required accurate and detailed models of landscapes and areas of high CO_2 emissions on the Earth's surface.

Only with the advent of quantum computing was it possible to improve the accuracy of the sensors that collect data in the cells, and each of them can be equipped with quantum CO_2 monitoring technology. Quantum sensor networks require distributed nodes with multiparty entangled states, discrete and continuous variables, and complex sensing protocols [1].

The use of entangled quantum sensor networks can make measurements and the accuracy of multiple distributed parameters more sensitive, such as temperature, pressure, pipe corrosion, and gas concentrations. Although natural gas pipelines use classic fiber optic detection technologies, research indicates that, in the future, quantum sensors could contribute to improving monitoring accuracy and infrastructure [44].

Building on these developments, Artificial Intelligence (AI) plays a crucial complementary role—transforming the vast data sets generated by quantum sensor networks into actionable insights and predictive intelligence for the oil and gas industry [45-46].

Building on these quantum advances, the fusion of Artificial Intelligence (AI) with quantum sensing networks and advanced instrumentation has decisively enhanced monitoring, analysis, and forecasting capabilities in the oil and gas sector.

While the first part of this section emphasized the role of Quantum Information Science (QIS) and entangled quantum sensors in the accurate detection of physical and environmental parameters, AI emerges as a natural extension of these innovations—responsible for interpreting, correlating, and predicting complex patterns in the resulting data. This synergy between AI and quantum technologies forms the link between intelligent physical monitoring and cognitive seismic interpretation, revolutionizing exploration and operational management in highly complex environments.

While quantum sensors revolutionize the detection of physical phenomena with remarkable accuracy, it is AI that enables the interpretation and operationalization of this data on a large scale in industrial contexts. This combination is particularly relevant in three critical areas of the energy industry: seismic interpretation for exploration, predictive monitoring of structural integrity, and early detection of operational failures. The following sections examine specific applications of AI in these contexts, illustrating how deep learning approaches have transformed established industry practices.

Accurate identification and characterization of geological faults remain a fundamental challenge in hydrocarbon exploration, especially in complex geological formations. Conventional seismic interpretation methods rely heavily on manual analysis by specialized geoscientists—a time-consuming process subject to interpretive variability.

A recent study conducted in the Tarim Basin in northwestern China demonstrates how AI-based models overcome these limitations. In this region, characterized by karstified carbonates at depths exceeding 6,000 meters, interpreting strike-slip faults is essential for optimizing drilling trajectories and development planning. Traditional seismic methods face great difficulties in obtaining clear images of these structures due to lithological complexity and dispersion effects caused by karstification [47].

To address these challenges, Wang et al. (2025) [47] developed a methodology based on U-Net networks with transfer learning, achieving results superior to conventional methods. The model effectively suppressed features unrelated to faults—such as karstified cavities and fractures—while producing clear images of fault geometry. This approach automates processes that traditionally required months of manual interpretation, significantly reducing analysis time and improving the consistency of results [47].

In addition to structural interpretation, AI demonstrates remarkable ability to predict seismic behavior and assess risks. Laurenti et al. (2024) [48] analyzed seismic waves recorded during the Norcia earthquake (M 6.5; 2016), using seven-layer convolutional neural networks to classify seismograms into three categories: foreshocks, aftershocks, and time-to-failure (TTF). The model achieved over 90% accuracy in distinguishing these classes, using raw seismic data as input, without the need for manual feature extraction [48].

The results indicate that deep learning models can detect subtle changes in the attenuation properties of elastic waves, capturing information about the evolution of fault zone characteristics throughout the seismic cycle, with direct implications for safety monitoring in exploration and production operations, especially in regions affected by seismicity induced by fluid injection or hydraulic fracturing [48].

The integration of quantum sensors and AI algorithms creates synergistic opportunities for leak detection and structural integrity monitoring. A collaborative project involving Louisiana State University, the University of Oklahoma, and Oak Ridge National Laboratory (ORNL) has developed a quantum entanglement-based fiber optic sensing system for detecting underground leaks in oil and gas pipelines. The approach replaces classical light sources with entangled quantum light, which generates much less background noise and has greater sensitivity to low-amplitude signals [49].

Validated with operational data from production wells in the Shengli Field (China), the combined model demonstrated superior robustness compared to individual models, especially when applied to datasets of varying quality—a common scenario in real industrial environments [50].

This transition to AI-enhanced predictive approaches, driven by data science, has resulted in significant reductions in unplanned downtime, increased service life of critical equipment, and optimized maintenance intervals. However, Johnson et al. (2023) [51] highlight persistent challenges related to the quality and availability of real-time data, the complexity of managing large volumes of heterogeneous information, and the operational costs associated with implementing these technologies [51].

Overall, the integration of AI, deep learning, and quantum sensing has produced substantial gains in operational efficiency, safety, and sustainability across the energy industry. As emphasized by Hassan et al. (2025) [52], the continuous evolution of these tools is consolidating a paradigm of autonomous and intelligent operations, in which automated seismic interpretation and quantum monitoring of infrastructure become the pillars of a safer, more productive, and environmentally responsible industry — directly contributing to the global energy transition and reinforcing the role of research and innovation in shaping the next generation of smart energy systems [52].

4. Geopolitics of Quantum Technologies and AI

The geopolitical landscape surrounding quantum technologies and artificial intelligence has fundamentally shifted from an academic pursuit to a critical domain of strategic competition that shapes contemporary international relations. China views quantum technology as a central element in global competition in science and technology, increasing government investments to around $15 billion [53], while the United States maintains its technological leadership through coordinated federal initiatives and partnerships with the private sector. This technological rivalry goes beyond traditional metrics of national power, setting new parameters in which quantum supremacy and AI capabilities determine geopolitical hierarchies.

Strategic competition between major powers manifests itself in distinct approaches to quantum development. China's technological development is largely government-led, with Beijing fully aware that whoever develops quantum technologies first will have tangible military advantages in cryptology, communication, and information processing [53].

In contrast, the US leads investment in the quantum private sector (44% of global funding), followed by the UK, Canada, and Australia (collectively around 20%) and China (17%) [54], demonstrating a market-driven approach that leverages private capital and entrepreneurial ecosystems. The European Union, as a whole, lags behind, with just over 12% of investment in the sector [54], highlighting the challenges faced by fragmented European innovation systems despite substantial public commitments.

European efforts to address this competitive disadvantage reveal the complexities of coordinating quantum strategies across multiple national jurisdictions. With nearly €7 billion in public investment in quantum, the EU trails only China [55], but faces structural limitations. Since 2018, Europe has committed more than €11 billion, but attracts only 5% of global private investment in quantum, compared to the US, which has 50% [56]. The proposed European Quantum Act represents an attempt to overcome these coordination challenges by seeking to unite fragmented national efforts into a more cohesive European strategy [57].

The implications for national security of quantum technologies focus primarily on cryptographic vulnerabilities that threaten existing security infrastructures. As Michele Mosca, a founding member of the Institute for Quantum Computing, demonstrated with his influential “Mosca Theorem,” the convergence of quantum technology with the global economy presents vast opportunities, but also immense risks [58]. Large-scale quantum computers could break current encryption standards, jeopardizing the security of communications and data around the world [57].

This threat has led to coordinated responses across multiple domains. NIST has published a final set of cryptographic tools designed to resist attacks from quantum computers, with post-quantum cryptographic standards protecting everything from confidential email messages to e-commerce transactions [59]. The urgency of this transition is reinforced by regulatory mandates, such as FIPS 203, FIPS 204, and FIPS 205, which specify algorithms derived from CRYSTALS-Dilithium, CRYSTALS-KYBER, and SPHINCS+, published in August 2024 [60].

The emergence of “quantum inequalities” represents a critical dimension that is often overlooked in geopolitical analyses. In a recent analysis published in Just Security, quantum technology policies may consolidate global inequality by excluding the Global South from access to emerging innovations [61]. The proposed “Qubits for Peace” framework draws a parallel with President Eisenhower’s 1953 “Atoms for Peace” initiative, seeking to enable peaceful applications of quantum computing, sensing, and communication in less developed countries, while protecting military and intelligence uses [61].

Export controls and technology protection measures represent another critical dimension of quantum geopolitics. In September 2024, in conjunction with international partners, the U.S. Department of Commerce published a provisional final rule on export controls for certain quantum technologies [62].

These restrictions extend to research collaboration, as following China's progress in building a 72-qubit superconducting quantum computer in 2024, the US included the creator Origin Quantum and much of the ecosystem on its list of restricted commercial entities due to their support for Chinese military activities [53]. European institutions face particular challenges in this environment, with European researchers working with Chinese partners now blacklisted by Washington [63].

The scope of the technological competition goes beyond quantum computing, encompassing the entire quantum technology ecosystem. China leads the way in quantum communications, possessing the world's largest quantum network, spanning 12,000 km, including two quantum satellites [53]. This infrastructure development demonstrates

how quantum technologies enable new forms of secure communication, fundamentally altering intelligence and security paradigms. As Ciel Qi notes in the Yale Journal of International Affairs, China's multi-decadal focus on quantum communications represents a strategic priority that could significantly influence geopolitics and have substantial impacts on US international strategy [64].

The challenges to international collaboration in quantum research reflect broader geopolitics. Rob Young, director of the Lancaster Quantum Technology Centre, notes that geopolitical barriers compound the inherent challenges of physics research, creating additional obstacles to the international cooperation essential for advancing quantum technology [65]. The broader strategic implications are highlighted in NATO assessments, which classify quantum technologies as "potentially revolutionary and disruptive" and as "an element of strategic competition" with rival states [63].

The intersection of public and private sectors adds complexity to quantum geopolitics. The role of private capital and corporations is much smaller in China than in the US, with major Chinese quantum companies acting as intermediaries between public laboratories and state clients, with limited autonomy [53]. This structural difference influences not only innovation patterns but also the integration of quantum technologies into broader economic and security systems.

Academic research patterns reflect these geopolitical dynamics, with research leadership varying across quantum technology domains. The US leads in research quality in quantum computing (34% of the most cited papers), followed by China (16%) and Germany (4%), while China leads in quantum communications (34%), followed by the US (17%) and Germany (7%) [54]. These patterns suggest that different nations are developing specialized capabilities within the broader quantum technology landscape, just as quantum sensing applications vary by regional focus, as demonstrated in the nuclear monitoring and oil and gas infrastructure protection discussed in the previous sections.

The implications for protecting critical infrastructure are particularly significant in the context of growing technological interdependence. Control over quantum infrastructure means long-term geopolitical influence, as does the digital dominance currently commanded by US and Chinese tech giants [56].

This recognition has led to policy frameworks that emphasize technological sovereignty, with the European Commission identifying quantum technologies as critical to the EU's economic security, recognizing their strategic value and dual-use nature [55]. As Rajesh Uppal notes in his analysis of the applications of the quantum revolution in defense and security, achieving quantum supremacy has become a geopolitical priority, with enormous advantages for the first nation to acquire computers that render all others obsolete [66].

The timeline for quantum technology deployment adds urgency to these competitive dynamics. The growing importance of quantum computers has become so prominent that the UN designated 2025 as the "International Year of Quantum Science and Technology" [67]. Investment patterns reflect this urgency: in the first quarter of 2025 alone, $1.25 billion was invested in quantum companies —70% of the previous year's total in just three months—with projections reaching $173 billion by 2040, making quantum not just a frontier technology but an economic and geopolitical force [56].

The challenges of balancing cooperation and competition in quantum technologies reflect broader tensions in international scientific collaboration. While competition can be healthy and stimulate innovation, it does not mean mobilizing entire populations to adopt a hostile mindset and dangerous attitudes toward competitors [67]. However, security considerations increasingly restrict collaborative possibilities, as Brussels has not yet published a promised risk assessment, but the US blacklist and NATO warnings have made it clear that Europe must exclude Chinese partners from public quantum technology projects [63].

These dynamics establish quantum technologies and AI as fundamental elements of contemporary geopolitical competition, where technological capabilities increasingly determine power and national security in an interconnected global system. The integration of these technologies into critical infrastructure sectors such as nuclear power and oil and gas, discussed in the previous section, represents not only operational enhancement but also strategic positioning within an evolving international order, where quantum capabilities may determine future geopolitical balances.

5. Challenges and Perspectives

Quantum networks, advanced sensors, and artificial intelligence enable advances in the security, efficiency, and reliability of strategic sectors, as already described. Their applicability, however, still faces significant technical challenges, high costs, and geopolitical tensions.

One of the main issues is scalability, as current quantum networks are limited in the number of nodes and qubits. As these infrastructures grow, coherence and fidelity can be compromised, as this difference causes greater noise, decoherence, and signal losses that hinder the maintenance of quantum entanglement, leading to communication instability [68].

Another challenge is integrating quantum networks into the existing classical infrastructure. This requires specific technical solutions, such as advanced optical filtering to minimize noise in quantum signals and nanosecond or picosecond synchronization, which are important for maintaining coherence between network nodes [69-70]. It is worth mentioning the complexity of these solutions due to the extreme precision required and the sensitivity of qubits to small variations. In addition to the technical challenges, the adoption of quantum networks is compromised due to the high costs and complexity of specialized hardware, for example, quantum repeaters, photon detectors and cryogenic systems [71].

Scientific cooperation enables knowledge sharing, cost reduction, and accelerated innovation in quantum-sensitive technologies. However, this collaboration often clashes with competition among global countries, creating tensions and barriers [72]. From this, agreements emerge that could restrict scientific cooperation in strategic areas, such as AI and quantum computing, in addition to impacting the competition for leadership in research, patents, and infrastructure, reflecting a climate of technological rivalry [73-74].

In this scenario, quantum technology finds itself somewhere between scientific cooperation and strategic competition. Its future will depend on technical innovation and also on enabling policies, international governance regimes, and scientific diplomacy sensitive to security implications.

6. Conclusion

This article explored the integration of quantum networks and artificial intelligence to build safer and more efficient communication systems. The use of AI algorithms allows for improved qubit routing, minimized errors, and more accurate network monitoring, paving the way for practical applications in several strategic sectors.

In the energy sector, especially in oil and gas, they are used to process large volumes of data and perform real-time analysis of CO2 emissions, increasing the efficiency and safety of operations. In the nuclear sector, AI-optimized quantum sensors can improve threat detection and prevention, promoting stricter control of radioactive materials and associated facilities.

Regarding geopolitical implications, countries leading in quantum computing and communication have strategic advantages in security, energy, and technology, placing these nations in a position of global influence, highlighting the importance of international cooperation and regulation.

It was also discussed that despite advances, significant technical challenges remain, such as preserving entanglement over long distances, the complexity of distributed processing, and the need for robust error correction algorithms.

In short, the convergence between quantum technologies and artificial intelligence expands the boundaries of information science and offers solutions to complex challenges, consolidating its position as a strategic field for research.

Compliance with ethical standards

Acknowledgments

I acknowledge the support of the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), the Ministry of Defense of Brazil, and the Financier of Studies and Projects (FINEP) for their contributions to research development and scientific advancement in defense-related technological innovation. Their support has been essential to the broader research initiatives associated with this work.

Disclosure of conflict of interest

The authors declare that they have no competing interests, financial or personal, that could have influenced the results presented in this study.

Statement of ethical approval

This article does not contain any studies with human participants or animals performed by the authors; therefore, ethical approval was not required.

Statement of informed consent

No informed consent was required, as this study involved no human participants.

Funding

This work was supported by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) through a Postdoctoral Fellowship under the PRO-DEFESA Program – Support for Education and Technology in National Defense, within the project "Quantum Technologies and AI in National Defense: The Strategic Role of Quantum Networks in Contemporary Geopolitics"

The funding agencies had no role in the study design, data collection, analysis, decision to publish, or preparation of the manuscript.

Availability of data and materials

All data used in this study are derived from publicly available sources, institutional reports, and scientific literature properly cited throughout the manuscript. No proprietary, confidential, or restricted data were used.

References

[1] Crawford, S. E.; Shugayev, R. A.; Paudel, H. P.; Lu, P.; Syamlal, M.; Ohodnicki, P. R.; Chorpening, B.; Gentry, R.; Duan, Y. Quantum sensing for energy applications: review and perspective. *Advanced Quantum Technologies*, v. 4, 2021. Art. 2100049. Available at: https://doi.org/10.1002/qute.202100049. Accessed on: Aug. 2025.

[2] Rosa, C.; Coimbra, M.; Barbosa, P.; Chantre, C.; Rosental, R., *Microrredes: benefícios e desafios para o setor elétrico brasileiro*. Rio de Janeiro: GESEL – Grupo de Estudos do Setor Elétrico, UFRJ, 2022. Available at: https://gesel.ie.ufrj.br/app/webroot/files/publications/10_Rosa_2022_02_02.pdf. Accessed on: Aug. 2025.

[3] Gkouliaras, K.; Theos, V.; Miller, T.; Jowers, B.; Kennedy, G.; Grant, A.; Cronin, T.; Evans, P. G.; Chatzidakis, S. Demonstration of quantum-secure communications in a nuclear reactor. *arXiv preprint*, arXiv:2505.17502, 2025. Available at: https://arxiv.org/abs/2505.17502. Accessed on: Aug. 2025.

[4] Startups. IoT, IA e energia nuclear são tendências para a transição energética. Startups.com.br, 2025. Available at: https://startups.com.br/negocios/inovacao/iot-ia-e-energia-nuclear-sao-tendencias-para-transicao-energetica/. Accessed on: Oct. 2025.

[5] Ernst & Young. O setor de petróleo e gás enfrenta um novo panorama: uma perspectiva da engenharia de processos. EY Insights, 2025. Available at: https://www.ey.com/pt_br/insights/oil-gas/o-setor-de-petroleo-e-gas-enfrenta-um-novo-panorama-uma-perspectiva-da-engenharia-de-processos. Accessed on: Oct. 2025.

[6] GroeneWegen-Lau, J. China's long view on quantum tech has the US and EU playing catch-up. Merics Report, 2024. Available at: https://merics.org/en/report/chinas-long-view-quantum-tech-has-us-and-eu-playing-catch. Accessed on: Oct. 2025.

[7] Abreu, D.; Pimentel, A.; Abelém, A. Reqroute: Reinforcement learning routing protocol for quantum entanglement networks. Brazilian Symposium on Computer Networks and Distributed Systems (SBRC), p. 630–643, 2024. SBC.

[8] Smith, A.; Abreu, D.; Pimentel, A.; Abelém, A. Redes quânticas sob ataque: Black Hole Repeaters. In: Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), 43., 2025, Natal, RN. *Anais do XLIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Porto Alegre: Sociedade Brasileira de Computação, 2025. p. 266-279. ISSN 2177-9384. DOI: https://doi.org/10.5753/sbrc.2025.5902 Accessed on: Oct. 2025.

[9] Jiang, J.-L.; Luo, M.-X.; Ma, S.-Y. Quantum network capacity of entangled quantum internet. IEEE Journal on Selected Areas in Communications, 2024.

[10] Ribezzo, D. et al. Deploying an inter-European quantum network. Advanced Quantum Technologies, v. 6, n. 2, p. 2200061, 2023.

[11] Xu, F; Ma, X.; Zhang, Q.; Lo, Hoi-Kwong; Pan, Jian-Wei. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, v. 92, n. 2, 025002, 2020. DOI: 10.1103/RevModPhys.92.025002.

[12] Porter, J. Google wants to build a useful quantum computer by 2029. *The Verge*, May 19, 2021. Available at: https://www.theverge.com/2021/5/19/22443453/. Accessed on: Oct. 2025.

[13] Roth, E. *Google reveals quantum computing chip with 'breakthrough' achievements*. The Verge, Dec. 9, 2024. Available at: https://www.theverge.com/2024/12/9/24317382/. Accessed on: Oct. 2025.

[14] Murphy, M. *AI and quantum computing: How IBM showed up at SXSW 2025*. IBM Research Blog, Mar. 2025. Available at: https://research.ibm.com/blog/ibm-research-sxsw-quantum-ai. Accessed on: Oct. 2025.

[15] Abughanem, M. *IBM quantum computers: Evolution, performance, and future directions*. The Journal of Supercomputing, v. 81, n. 5, p. 687, Apr. 2025. DOI: 10.1007/s11227-025-07047-7.

[16] Roik, J.; Bartkiewicz, K.; Černoch, A.; Lemr, K. Routing in quantum communication networks using reinforcement machine learning. *Quantum Information Processing*, v. 23, art. 89, 2024. DOI: 10.1007/s11128-024-04287-z. Available at: https://research.ibm.com/blog/ibm-research-sxsw-quantum-ai. Accessed on: Oct. 2025.

[17] Sharma, P.; Gupta, S.; Bhatia, V.; Prakash, S. Deep reinforcement learning-based routing and resource assignment in quantum key distribution-secured optical networks. *IET Quantum Communication*, 2023. DOI: 10.1049/qtc2.12063. Available at: https://research.ibm.com/blog/ibm-research-sxsw-quantum-ai. Accessed on: Oct. 2025.

[18] Bausch, J. et al. Learning high-accuracy error decoding for quantum processors. Nature, v. 635, p. 834–840, 2024. DOI: 10.1038/s41586-024-08148-8.

[19] Calibration of quantum sensors by neural networks. Physical Review Letters, v. 123, p. 230502, 2019. DOI: 10.1103/PhysRevLett.123.230502.

[20] Kang, Jia-Le; Zhang, Ming-Hui; Liu, Xiao-Peng; Xie, J. Machine learning with neural networks for parameter optimization in twin-field quantum key distribution. *Quantum Information Processing*, v. 22, art. 309, 2023. DOI: 10.1007/s11128-023-04063-5.

[21] Ramya, R.; Kumar, P.; Dhanasekaran, D.; Kumar, R. Satheesh; Sharavan, S. Amithesh. A review of quantum communication and information networks with advanced cryptographic applications using machine learning, deep learning techniques. *Franklin Open*, v. 10, 1 Mar. 2025, p. 100223. DOI: 10.1016/j.fraope.2025.100223.

[22] Fasano, Raymond; Hahn, Andrew; Haddad, Alexandria; Lamb, Christopher. *Advance Reactor Operational Technology Architecture Categorization*. Technical Report, 1 Sept. 2021. OSTI.GOV. DOI: https://doi.org/10.2172/1854723.

[23] World Nuclear Association. Security of nuclear facilities and material. Available at: https://world-nuclear.org/information-library/safety-and-security/security/security-of-nuclear-facilities-and-material. Accessed on: Oct. 2025.

[24] Mazurczyk, W.; Caviglione, L**.** *Cyber reconnaissance techniques: the evolution of and countermeasures for cyber reconnaissance*. Communications of the ACM, New York, v. 64, n. 3, p. 86–95, mar. 2021. Available at: https://cacm.acm.org/magazines/2021/3/250712-cyber-reconnaissance-techniques/fulltext. Accessed on: Aug. 2025.

[25] United States Nuclear Regulatory Commission (U. NRC). Regulatory guide 5.71: Cyber security programs for nuclear facilities. Washington, DC, 2010.

[26] Son, J.; Tak, T.; Inhye, H. Modeling cryptographic algorithms validation and developing block ciphers with electronic code book for a control system at nuclear power plants. Nuclear Engineering and Technology, v. 55, n. 1, p. 25–36, Jan. 2023. DOI: 10.1016/j.heliyon.2023.e13883.

[27] National Institute of Standards and Technology (NIST). NIST releases first 3 finalized post-quantum encryption standards. 2024. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards. Accessed on: Oct. 2025.

[28] Mavroeidis, V. et al. The impact of quantum computing on present cryptography. International Journal of Advanced Computer Science and Applications, v. 9, n. 3, 2018. Available at: http://arxiv.org/abs/1804.00200. Accessed on: Oct. 2025.

[29] Gidney, C.; Ekerå, M. How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, v. 5, p. 433, Apr. 2021. DOI: 10.22331/q-2021-04-15-433.

[30] Szikora, P.; Lazányi, K. The end of encryption? – The era of quantum computers. In: Kovács, T. A.; Nyikes, Z.; Fürstner, I. (org.). Security-Related Advanced Technologies in Critical Infrastructure Protection. Dordrecht: Springer, 2022. p. 61–72.

[31] Azhari, R.; Salsabila, A. N. Analyzing the impact of quantum computing on current encryption techniques. IAIC Transactions on Sustainable Digital Innovation (ITSDI), v. 5, n. 2, p. 148–157, Feb. 2024. Available at: https://aptikom-journal.id/itsdi/article/view/662. Accessed on: Aug. 2025.

[32] Katz, J.; Lindell, Y. Introduction to Modern Cryptography. 3. ed. Boca Raton: CRC Press, 2021.

[33] Nagaraj, Karthikeyan. One-time pad encryption: The ultimate guide – Understanding the key features, advantages, and limitations of one-time pad encryption. Medium, Mar. 27, 2023. Available at: https://aptikom-journal.id/itsdi/article/view/662. Accessed on: Oct. 2025.

[34] National Quantum Initiative. Available at: https://www.quantum.gov/. Accessed on: Oct. 2025.

[35] Neven, H. Meet Willow, our state-of-the-art quantum chip. Google Blog, Dec. 2024. Available at: https://blog.google/technology/research/google-willow-quantum-chip/. Accessed on: Oct. 2025.

[36] CSIRO. Quantum communications research. Quantum Battery Team, 2025. Available at: https://research.csiro.au/quantumbattery/research/quantum-communications/. Accessed on: Oct. 2025.

[37] WIRED. Neutrino detectors could be used to spot nuclear rogues. Wired Magazine, 2024. Available at: https://www.wired.com/story/neutrino-detectors-could-be-used-to-spot-nuclear-rogues/. Accessed on: Oct. 2025.

[38] ARXIV. Quantum paper collection 2023. Available at: https://arxiv.org/abs/2307.13811. Accessed on: Oct. 2025.

[39] Huang, Q.; Peng, S.; Deng, J.; Zeng, H.; Zhang, Z.; Liu, Y.; Yuan, P. A review of the application of artificial intelligence to nuclear reactors: Where we are and what's next. Heliyon, v. 9, n. 3, e13883, Mar. 2023. DOI: 10.1016/j.heliyon.2023.e13883.

[40] Chaudhary, A.; Han, J.; Kim, S.; Kim, A.; Choi, S. Anomaly detection and analysis in nuclear power plants. Electronics, v. 13, n. 22, 4428, 2024. DOI: 10.3390/electronics13224428.

[41] Huurman, J.; Mondal, K.; Martinez, O. An overview of emerging nuclear sensor technologies: Challenges, advancements and applications. Applied Sciences, v. 15, n. 5, p. 2338, 2025. DOI: 10.3390/app15052338.

[42] Ramos, A.; Carrasco, A.; Fontanet, J.; Herranz, L. E.; Ramos, D.; Díaz, M.; Zazo, J. M.; Cabellos, O.; Moraleda, J. Artificial intelligence and machine learning applications in the Spanish nuclear field. Nuclear Engineering and Design, v. 417, 112842, Feb. 2024. DOI: 10.1016/j.nucengdes.2023.112842.

[43] NASA. Estimating carbon flux with quantum computing. Technology Stories, Dec. 2019. Available at: https://science.nasa.gov/technology/technology-stories/estimating-carbon-flux-with-quantum-computing. Accessed on: Oct. 2025.

[44] Degen, C. L.; Reinhard, F.; Cappellaro, P. Quantum sensing. *Reviews of Modern Physics*, v. 89, n. 3, 035002, 2017. DOI: https://doi.org/10.1103/RevModPhys.89.035002.

[45] Johnson, A. O.; Smith, B. K.; Williams, C. D**.** Advancements in predictive maintenance in the oil and gas industry: A review of AI and data science applications. *World Journal of Advanced Research and Reviews*, v. 20, n. 3, p. 167–181, 2023. DOI: https://doi.org/10.30574/wjarr.2023.20.3.2432. Accessed on: Oct. 2025.

[46] University Of Oklahoma. Researchers aim to improve oil & gas leak detection with quantum-enhanced sensing. OU Research News, 2021. Available at: https://www.ou.edu/research-norman/news-events/2021/researchers-aim-to-improve-oil-gas-leak-detection-with-quantum-enhanced-sensing. Accessed on: Oct. 2025.

[47] Liu, J.; Wu, G.; Chen, L.; Wan, X.; Ma, B.; Zhang, R.; Qiu, C.; Wang, X.. Deep transfer learning for seismic characterization of strike-slip faults in karstified carbonates from the northern Tarim basin. Scientific Reports, v. 15, art. 9242, Mar. 2025. DOI: 10.1038/s41598-025-94134-7.

[48] Laurenti, L.; Paoletti, G.; Tinti, E.; Galasso, F.; Collettini, C.; Marone, C. Probing the evolution of fault properties during the seismic cycle with deep learning. Nature Communications, v. 15, art. 10025, Nov. 2024. DOI: 10.1038/s41467-024-54153-w.

[49] Oak Ridge National Laboratory (ORNL). Quantum sensing for oil leak detection. Available at: https://www.ornl.gov/news/quantum-sensing-oil-leaks. Accessed on: Oct. 2025.

[50] Wang, M.; Su, X.; Song, H.; Wang, Y.; Yang, X. Enhancing predictive maintenance strategies for oil and gas equipment through ensemble learning modeling. Journal of Petroleum Exploration and Production Technology, v. 15, art. 46, Feb. 2025. DOI: 10.1007/s13202-025-01931-x.

[51] Johnson, A. O.; Smith, B. K.; Williams, C. D. Advancements in predictive maintenance in the oil and gas industry: A review of AI and data science applications. World Journal of Advanced Research and Reviews, v. 20, n. 3, p. 167–181, Dec. 2023. DOI: 10.30574/wjarr.2023.20.3.2432.

[52] Hassan, M.; Kumar, R.; Singh, P.; Patel, A. Artificial intelligence in the oil and gas industry: Applications, challenges, and future directions. Applied Sciences, v. 15, n. 14, art. 7918, Jul. 2025. DOI: 10.3390/app15147918.

[53] Groenewegen-Lau, J. China's long view on quantum tech has the US and EU playing catch-up. MERICS, 2024. Available at: https://merics.org/en/report/chinas-long-view-quantum-tech-has-us-and-eu-playing-catch. Accessed on: Oct. 2025.

[54] ERIXON, Fredrik; DUGO, Andrea; PANDYA, Dyuti; DU ROY, Oscar. *Benchmarking Quantum Technology Performance: Governments, Industry, Academia and their Role in Shaping our Technological Future*. ECIPE Policy Briefs, Mar. 2025. Available at: https://ecipe.org/publications/benchmarking-quantum-technology-performance/. Accessed on: Oct. 2025.

[55] De Luca, S. Quantum: What is it and where does the EU stand? European Parliament – Think Tank, 10 Apr. 2024. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2024)760413. Accessed on: Oct. 2025.

[56] Nolan, P. Europe's quantum leap challenges US dominance: The US, China, and Europe are engaged in a high-stakes sprint to dominate the next frontier of computing. Bandwidth, July 15, 2025. Available at: https://cepa.org/article/europes-quantum-leap-challenges-us-dominance/. Accessed on: Oct. 2025.

[57] Quantum Geopolitics: The Global Race for Quantum Computing. PostQuantum – Industry News: Quantum Computing, Quantum Security, PQC, Mar. 2025. Available at: https://postquantum.com/quantum-computing/quantum-geopolitics/. Accessed on: Oct. 2025.

[58] Mosca, M. Cyber resilience in the era of quantum computing. NATO Review, 2024.

[59] National Institute of Standards and Technology – NIST. *Post-Quantum Cryptography (PQC).* Gaithersburg, MD, 2025. Available at: <https://csrc.nist.gov/projects/post-quantum-cryptography>. Accessed on: Oct. 2025.

[60] National Institute of Standards and Technology (NIST). Post-quantum cryptography standardization. NIST Publications, 2024. Available at: https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization. Accessed on: Oct. 2025.

[61] The European Defense Fund. Quantum and AI for Defense (QUAID). Bruxelas: European Commission, 2025.

[62] National Quantum Initiative. Technology security. National Quantum Initiative Office, Jan. 2025. Available at: https://www.quantum.gov/. Accessed on: Oct. 2025.

[63] Groenewegen-Lau, J. Europe must end its quantum technology research with China. MERICS, 2024. Available at: https://merics.org/en/comment/europe-must-end-its-quantum-technology-research-china. Accessed on: Oct. 2025.

[64] Jensen, A. Quantum technologies in Defense: Opportunities and challenges. RAND Europe, 2025.

[65] Defense Research and Development Canada (DRDC). Quantum Science and Technology Strategy. Ottawa: DRDC, 2023. Available at: https://www.canada.ca/en/defence-research-development.html. Accessed on: Oct. 2025.

[66] Uk Ministry of Defense. Defense Quantum Strategy 2024–2029. Londres, 2024. Available at: https://www.gov.uk/government/organisations/ministry-of-defence. Accessed on: Oct. 2025.

[67] MOSCIONI, Brian. Another Technology Race: US–China Quantum Computing Landscape. Harvard Kennedy School – Belfer Center for Science and International Affairs, U.S.–China Relations Blog Post. Available at: https://www.belfercenter.org/research-analysis/another-technology-race-us-china-quantum-computing-landscape. Accessed on: Oct. 2025.

[68] Australian Department of Defense. National Quantum Strategy Implementation Report. Canberra, 2025. Available at: https://www.defence.gov.au/. Accessed on: Oct. 2025.

[69] Brazilian Ministry of Science, Technology and Innovation (MCTI). Estratégia Nacional de Computação Quântica. Brasília, 2023. Available at: https://www.gov.br/pt-br. Accessed on: Oct. 2025.

[70] Ministério Da Defesa (BRASIL). Livro Branco de Defesa Nacional 2024. Brasília, 2024. Available at: https://www.gov.br/pt-br. Accessed on: Oct. 2025.

[71] Petrobras. Relatório de Inovação e Tecnologia 2025. Rio de Janeiro, 2025. Available at: https://petrobras.com.br/. Accessed on: Oct. 2025.

[72] Electric Power Research Institute (EPRI). Quantum Technologies for Power Systems. Palo Alto, 2025. Available at: https://www.epri.com/. Accessed on: Oct. 2025.

[73] International Atomic Energy Agency (IAEA). Artificial Intelligence for Nuclear Applications. Viena, 2025. Available at: https://www.iaea.org/. Accessed on: Oct. 2025.

[74] OECD Nuclear Energy Agency (NEA). Nuclear Innovation 2050 – Quantum and AI Perspectives. Paris, 2025. Available at: https://www.oecd-nea.org/ Accessed on: Oct. 2025.