INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

Emerging Technology in the Energy Sector:

Threats, Vulnerabilities, and Recommendations for Industry

By Nick Reese

Thomas Morin

Sam Houston State University

Emerging Technology in the Energy Sector:

Threats, Vulnerabilities, and Recommendations for Industry

By Nick Reese
Thomas Morin

Contents

Abstract

Emerging technologies are reshaping the energy sector, presenting both opportunities and significant security challenges. This paper investigates the transformative potential of quantum computing and artificial intelligence (AI) in areas such as grid management, operational efficiency, and predictive maintenance while highlighting the vulnerabilities they introduce. A key focus is the sector's readiness to address emerging threats so that greater infrastructure security can be achieved, leading to resilience in Texas and the US economy. The findings emphasize the need for a unified approach to security standards and working professionals who can be trained to advance these security standards in the near future. This research will inform not only the energy industry but also the development of a 2025 professional course aimed at equipping energy professionals with the tools to adapt to an evolving technological landscape.

Introduction

The energy sector is no stranger to technological advancements. Throughout history, the pursuit of more and highly efficient energy drove innovations across sectors. The energy sector in 2025 is likewise poised to both motivate and benefit from emerging technology advancements. Technologies such as solar cells and batteries with direct impact on energy generation, distribution, and consumption are already having an impact. Technologies with indirect impacts on the energy sector will be those that will determine the sector's future.

The economic race for dominance in various emerging technologies such as artificial intelligence (AI) and quantum computing is well documented. Less well documented is the geopolitical race for dominance in those technologies. With significant statecraft implications, major powers have well documented ambitions to build and maintain large global leads in emerging technologies, including the US. This is the state of the world in 2025, and it is changing the security landscape.

Also a reality in 2025 is a war in Ukraine that is stretching into its fourth year.[i] Throughout the Russian invasion, targets have been made of critical infrastructure elements, including energy. The Russian invasion of Ukraine is giving the rest of the world a view of the future of warfare and the targets seen as viable by adversaries. The energy sector is a clear target of foreign adversaries, for peacetime and wartime operations, in the cyber and physical domains. While the energy sector is accustomed to the implementation of new technologies, it stands at an inflection point. The combination of a geopolitical race centered on emerging technologies and the integration of internet connected devices in information technology (IT) and operational technology (OT) systems creates this inflection. The continued security of the energy sector depends both on technologies that directly contribute to its core mission and on those enabling technologies that will make or break the overall security posture of the sector.

The energy sector has already been at one such inflection point. The introduction of internet connected technologies created new vulnerabilities where such vulnerabilities had not previously existed. The integration of IT and OT systems created efficiencies and allowed many organizations to scale with rising energy demand. They were also responsible for multiple cyberattacks to include the Colonial Pipeline ransomware attack in May of 2021.[ii] Major outages like these can impact the economic security of the US as well as other dependent sectors such as transportation. These vulnerabilities have been present for decades, but attacks still occur. With the coming introduction of AI and quantum computing, the energy sector must apply the lessons it has learned through the integration of internet connected technologies and prepare itself anew for the next inflection point. The added reality of nation-state adversary targeting of critical infrastructure gives this requirement an extra imperative.

This paper studies specific technologies and discusses their applications to the energy sector to include AI and quantum computing. The study is conducted from a security perspective and leverages decades of direct national and homeland security experience to

include critical infrastructure security work directly with energy companies. It examines geopolitical and domestic conditions around emerging technologies and applies them directly to the energy sector. The study also provides a list of specific recommendations for energy security that are practically applicable today. While larger changes are needed in the sector, the recommendations of this paper will create the initial conditions for emerging technology security improvements. The authors also acknowledge that this topic requires additional research and specific projects that will give the energy sector what it needs to secure itself for years to come. These follow-on recommendations are also provided in the recommendations section.

The energy sector may be accustomed to technology changes, but it is living in a different world today. The conditions are present for a major energy disruption impacting the national, economic, and homeland security of the United States. This topic requires immediate attention from senior executives and government officials to ensure the safety and security of critical infrastructure, and our economy, for years in the future.

Purpose and Scope of Research

This paper explores how emerging technologies, specifically quantum computing and AI, could reshape the energy sector. Specifically, changes made in grid adaptability, energy sourcing and resilience are explored. It examines the current state of security readiness and proposes actionable strategies for improvement.

Importance of Security and Adaptation

As technological advancements accelerate, the energy sector must modernize its security infrastructure to address increasingly sophisticated threats. Without adaptation, vulnerabilities in critical infrastructure could lead to significant risks.

Overview of Key Emerging Technologies in Energy

When considering the application of emerging technologies to the energy sector, two fundamental concepts shape their implementation: what is known and what remains unknown. Artificial Intelligence and Quantum computing technologies hold the potential to improve efficiency, enhance grid resilience, and optimize energy management. However, their integration into existing energy infrastructure requires a balance between leveraging current knowledge and addressing uncertainties. Emerging technologies, by definition, exist at the intersection of practical application and theoretical possibility, necessitating continuous research and adaptation.

Current Status

AI has already demonstrated its capabilities in areas such as predictive maintenance, demand forecasting, and grid management[iii]. By analyzing vast datasets, AI can identify inefficiencies, predict equipment failures, and enable real-time decision-making to optimize energy distribution. Its ability to integrate with renewable energy sources further enhances sustainability efforts, making AI a valuable tool for modernizing the energy sector[iv]. However, AI's effectiveness is dependent on high-quality data, robust infrastructure, and skilled personnel capable of managing its deployment.

Quantum computing remains largely in the research phase concerning its application in energy. Theories suggest that quantum algorithms could revolutionize optimization problems and energy distribution strategies[v]. However, the gap between laboratory research and real-world application remains substantial. Unlike AI, which is already in use across the industry, quantum computing is not yet commercially viable for energy-related tasks. Nevertheless, its potential to disrupt traditional computational methods makes it an important area for continued study and investment.

As AI becomes more integrated into energy systems and quantum computing advances toward practical applications, the industry must address knowledge, security, and workforce challenges to fully harness these technologies' benefits.

While AI has gained traction in the energy sector, significant gaps remain in how effectively it can be integrated into existing infrastructure. One of the most pressing concerns is data quality and accessibility. AI-driven solutions rely on vast amounts of historical and real-time data to make accurate predictions and automate processes. However, many energy companies struggle with fragmented, inconsistent, or incomplete data sources[vi]. Without standardized data management practices, AI models may produce unreliable results, limiting their effectiveness in optimizing energy systems.

Security

Another major concern is cybersecurity. AI-enhanced energy systems introduce new vulnerabilities, as they rely on interconnected networks and real-time data processing[vii]. Cyber threats such as data breaches, adversarial AI attacks, and infrastructure hacking pose serious risks to grid stability and energy security[viii]. Without robust cybersecurity measures, AI's potential benefits could be outweighed by the risks associated with system disruptions and malicious attacks.

Quantum computing presents an even more complex security challenge. While still in the early stages of development, quantum technology has the potential to break existing encryption methods, posing a significant threat to energy infrastructure security[ix]. Many energy systems (like most online systems) rely on cryptographic protocols to protect sensitive data and ensure secure communication[x]. The eventual commercialization of quantum computing will necessitate the development of quantum-resistant security measures to safeguard critical infrastructure.

Bridging these knowledge and security gaps requires proactive measures, including investments in research, improved data management strategies, and the implementation of advanced cybersecurity frameworks. Without these efforts, the energy sector may struggle to fully integrate AI and prepare for the risks of quantum computing while maintaining system security and reliability.

Workforce skills

The challenges associated with knowledge limitations and security vulnerabilities are closely tied to the broader issue of workforce readiness. As AI and quantum computing continue to evolve, the demand for skilled professionals capable of implementing, securing, and managing these technologies is growing. However, the current workforce in the energy sector often lacks the necessary expertise to keep pace with these advancements, creating a significant skills gap.

AI adoption requires professionals trained in data science, machine learning, and cybersecurity. However, many workers (including those within the energy sector) are trained in more traditional settings with limited exposure to AI-driven methodologies given it's rapid, recent emergence[xi]. As a result, AI solutions may not be effectively implemented, leading to inefficiencies and missed opportunities[xii]. To address this gap, the industry must invest in training programs that equip energy professionals with the skills needed to work alongside AI systems and optimize their capabilities.

Quantum computing presents an even more pronounced skill gap. Since its practical applications in energy are still largely theoretical, there is a shortage of professionals with expertise in quantum algorithms, cryptography, and advanced computational models[xiii]. As quantum technology progresses toward commercialization,

the demand for specialists in this field will increase. Without adequate preparation, the energy sector risks falling behind in adopting quantum-driven solutions.

The growing market demand for AI and quantum computing expertise highlights the need for industry-academia collaboration. Universities, technical training programs, and industry leaders must work together to develop interdisciplinary curricula that combine energy sector knowledge with emerging technology skills. Additionally, organizations should invest in professional development initiatives to upskill existing employees, ensuring that the workforce remains adaptable to technological advancements.

Addressing these skill gaps is crucial to the successful integration of AI and quantum computing in the energy sector. Without a well-trained workforce, even the most advanced technologies will fail to deliver their full potential, leaving the industry vulnerable to inefficiencies, security risks, and missed innovation opportunities.

AI and quantum computing represent transformative forces in the energy sector, offering opportunities to enhance efficiency, security, and sustainability. However, their successful implementation depends on addressing key knowledge limitations, security vulnerabilities, and workforce challenges. AI is already being used in grid management, predictive maintenance, and renewable energy forecasting[xiv], yet its effectiveness is constrained by data quality issues and cybersecurity risks. Quantum computing, while still in its early stages, presents long-term security concerns that must be proactively managed.

Equally important is the need to bridge skill gaps in the workforce. The demand for professionals with expertise in AI, data science, and quantum computing far exceeds the current supply, creating a critical challenge for the energy industry. Investing in targeted education and training programs will be essential to ensuring a workforce capable of leveraging these technologies effectively.

By addressing these challenges, the energy sector can position itself at the forefront of technological innovation, ensuring a resilient and efficient energy future.

Case Studies of Key Technologies

Quantum Computing

Of the litany of emerging technologies on the horizon, quantum computing is perhaps the one with the most potential to cause an extreme shift in our security landscape, and the one

with the most mystery surrounding it. Quantum computing is a different type of computation altogether that brings with it new opportunities and risks. The current risk to the energy sector is a knowledge gap. Leaders and executives from across sectors have other, more present risks to worry about such as ransomware or other cyberattacks. However, quantum computing offers a new type of risk, with uncertainty about when it will fully arrive at sufficient capacity to directly threaten cybersecurity. This section will provide an overview of quantum computing as a technology and discuss its opportunities and risks specific to the energy sector. It is important to note that the gap in general understanding of quantum computing concepts among the general energy workforce and its leadership presents the most significant vulnerability today. A lack of understanding of quantum computing at a fundamental level risks a slow response to its arrival and a misunderstanding of its developments. This paper addresses some basic Quantum computing concepts and recommends a broader, near-term effort to educate energy professionals about quantum computing.

Quantum computing represents a paradigm shift in computational science, moving beyond the classical bit's binary logic to harness the quirky principles of quantum mechanics.[xv] Unlike classical computers, which manipulate bits representing either 0 or 1, quantum computers utilize qubits, which can exist in a superposition of both states simultaneously.[xvi] A bit is the fundamental unit of information inside a classical computer, represented physically by an electrical pulse (or the absence of a pulse) inside tiny transistors on chips. These pulses create binary code in the form of a 1 or 0, which classical computers then use to conduct operations. Classical computers use these bits to execute Boolean Logic operations such as AND, OR, NOT, and XOR (exclusive or). The fundamental unit of quantum computing is the qubit, represented by a physical subatomic particle. Behaviors such as superposition provide new computational possibilities not available to the binary code and Boolean Logic of classical computers. This fundamental difference unlocks computational possibilities previously deemed unattainable.[xvii]

At the heart of quantum computing is the concept of superposition.[xviii] Superposition is a characteristic of quantum particles where these physical particles can be in multiple places at once. Quantum particles exhibit wave-particle duality - the ability to sometimes behave as a wave and sometimes behave as a particle. This means that a particle is in more than one “state” at the same moment. Being in multiple states at the same time gives the particle infinite potential locations at any moment before measurement or the moment when outside forces act on the system. Existing in superposition gives a qubit inside a quantum computer (represented physically by a quantum particle) important capabilities to represent information that are not possible with classical, binary computers.

As Nielsen and Chuang explain, a qubit's state can be described as a linear combination of $|0\rangle$ and $|1\rangle$, expressed as $\alpha|0\rangle + \beta|1\rangle$, where α and β are complex probability amplitudes.[xix] This superposition allows a quantum computer to explore multiple computational paths in parallel, offering the potential for exponential speedups in certain tasks.[xx] Whereas a classical computer reads binary code in a linear fashion, quantum computers can represent and read information in multiple states at once owing to the properties of superposition. This means that instead of checking answer possibilities one by one, quantum computers can check all possible answers simultaneously using superposition. This provides a new computational capability not

available in classical computers. The ability to solve specialized problems using their higher data capacity and computational power will be transformative when quantum computers are built to a sufficient capacity.

Furthermore, quantum computers leverage entanglement, a phenomenon where two or more qubits become correlated, such that their states are inextricably linked.[xxi] "Entanglement is a physical resource, like energy."[xxii] This correlation allows for the execution of complex operations that are impossible in classical systems. For example, manipulating one entangled qubit instantaneously affects the state of its entangled partner, regardless of the distance separating them.[xxiii] Entanglement has important implications for cryptography in the area of key distribution. Quantum key distribution has been demonstrated but its complexity and requirement for specialized equipment make it difficult to implement in practice. While it is important to be aware of entanglement as a property of quantum mechanics, superposition is significantly more important for the applications discussed here.

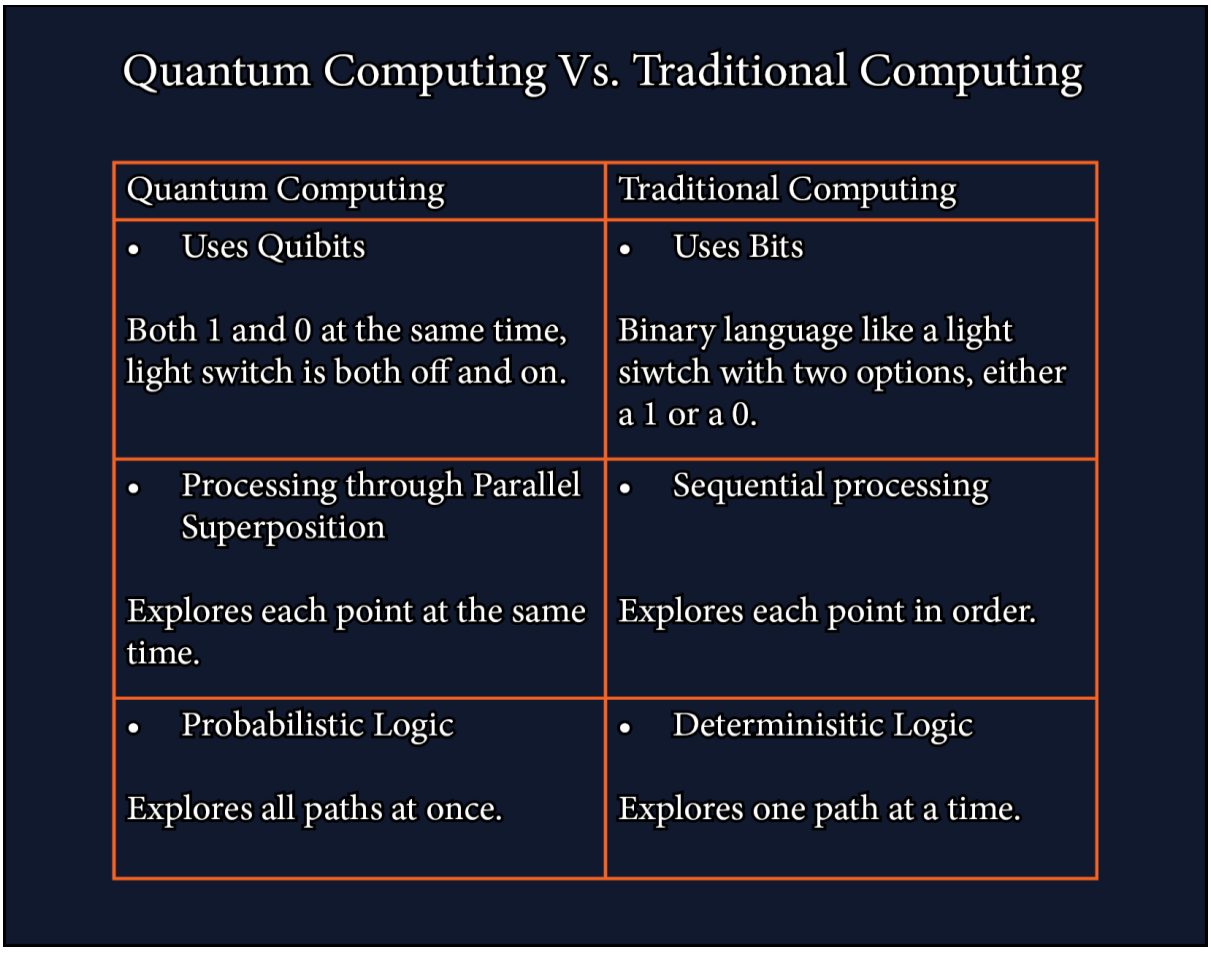

Figure 1: Chart (designed by Thomas Morin) detailing the differences between quantum and traditional computing.

Just like classical computers, quantum computers must include multiple qubits in the quantum processor, all of which must behave according to our requirements and must work

together. Qubits, with their quirky quantum behavior, are difficult to control and require extraordinary lengths to manipulate. During operation, the processor of a quantum computer must be kept at just a fraction of a degree above absolute zero. The cryogenics alone required to create this temperature, literally one of the coldest places in the universe, is complex and demands significant energy. Further, quantum computers require the use of logic gates the same way classical computers do. However, quantum computers require different gates to conduct different operations such as the Hadamard gate, which changes the basis state of a qubit. Between the difficulty in controlling a single qubit, let alone multiple qubits, the requirements for advanced cryogenics, and the need to engineer new logic gates, the challenges facing practical quantum computing are significant. However, these are engineering problems, not limitations of physics. Advancements are being made every day, and most experts believe that quantum computing is a reality in the future, though how far into the future remains a question. Even though the challenges are significant, it is important to understand the scope of the power of quantum computing and what can be accomplished when the engineering challenges are overcome. Running certain algorithms on a quantum computer present computational challenges, opportunities, and threats that are not present with classical computers.

The power of quantum computing stems from its ability to exploit these quantum phenomena through quantum algorithms. For example, Shor's algorithm demonstrates the potential to factor large numbers quickly, a task that is computationally intractable for classical computers.[xxiv] This capability has profound implications for cryptography, as it threatens the security of widely used public-key encryption schemes.[xxv] The threat to asymmetric cryptography from a quantum computer of sufficient capacity, called a cryptoanalytically relevant quantum computer or CRQC, is one of the most significant cybersecurity threats the energy sector will face. The next section will discuss this threat in depth followed by a discussion of quantum error correction, one of the most significant milestones in the development of quantum computers.

Cryptography

Currently, asymmetric encryption schemes provide the basis for the security of our data online from internet traffic to email. Asymmetric encryption, also called public key encryption, refers to those schemes that use a public key and a private key to encrypt messages. The recipient must have both keys to unlock the message. This scheme proves extremely valuable in preventing vulnerabilities in key exchange. The asymmetric encryption schemes currently in use are based on factorization problems. Factoring large numbers is a difficult operation for classical computers to solve due to the deterministic and binary nature of classical computer operations. For quantum computers with the help of Shor’s Algorithm, factorization problems can be solved quickly. This represents a significant threat to cybersecurity and the security of sensitive data that will impact all industries and sectors. The estimates on how long it would take a classical computer to break factorization-based encryption are in the billions of years making it practically unbreakable. Quantum computers with Shor’s Algorithm take that time to decryption down to minutes. There is significant practical and geopolitical application for such a device.

Encryption schemes provide the basis for the security of our data from internet traffic to communications. Most encryption refers to mathematical schemes using “keys” to encrypt messages. The asymmetric encryption schemes currently in use are based on factorization math problems. Factoring large numbers is a difficult operation for classical computers to solve due to their deterministic and binary nature. For quantum computers with the help of Shor’s Algorithm, factorization problems can be solved quickly. The estimates on how long it would take a classical computer to break factorization-based encryption are in the billions of years making it practically unbreakable. Quantum computers of sufficient capacity to run Shor’s Algorithm take that time to decryption down to minutes. This represents a significant threat to cybersecurity and the security of sensitive data and will impact all industries and sectors. There is significant practical and geopolitical application for such a device.

The energy sector will be impacted by the threat of quantum computing to asymmetric encryption, and its data is too sensitive and vital to leave to chance. The energy sector must prioritize the transition to post-quantum cryptography and to cryptographic agility into the future. Full recommendations will be provided in the recommendations section. What follows is an explanation of the threat to asymmetric cryptography and what post-quantum cryptography is.

Asymmetric encryption protocols such as Rivest, Shamir, Adleman (RSA) are factorization-based.[xxvi] In any exchange of information using RSA, there is a public key and a private key. The public key is transmitted in the open with the message. That key is a very long number, hundreds of digits. The private key is a prime number the public key number factors into. If those numbers match, the message is decrypted. If someone intercepted the message, they would have access to the public key number. To decrypt the message, they simply must factor the public key into the private key number, but this operation is extremely difficult to do on a binary system. As a result, even the most advanced classical computers would take billions of years to decrypt such a message.

Recognizing this vulnerability, the National Institute of Standards and Technology (NIST) within the US Department of Commerce launched a call for submissions for a new encryption protocol that would replace the factorization based encryption with different math,[xxvii] math that not even quantum computers are good at. This new encryption protocol will still have a public key and a private key, but the math that enables the keys will be based on the closest vector problem rather than factorization. The results will replace our current public key encryption protocols to make our encryption systems resilient to quantum attacks.

The charts below will list some opportunities and risks of introducing quantum computing in critical energy infrastructure.

Opportunities:

Opportunities in Using Quantum Computing in Critical Energy Infrastructure

Opportunity	Potential	Reccomendations
Grid Optimization	• Real-time optimization of energy distribution. • Predictive maintenance to prevent outages. • Optimization of energy storage deployment.	• Invest in research and development of quantum algorithms for grid management and explore partnerships with quantum computing companies.
Renewable Energy Management	• Quantum computing can improve forecasting of renewable energy generation (solar, wind), leading to better integration into the grid. • Optimize the placement and operation of renewable energy facilities.	• Utilize quantum simulations to model and predict renewable energy output and optimize resource allocation.
Materials Science and Energy storage	• More efficient solar cells. • Advanced batteries with higher energy density. Improved catalysts for cleaner fuel production.	• Fund research into quantum materials science and collaborate with research institutions.
Energy Trading and Risk Management	• Quantum algorithms can enhance risk assessment and optimization in energy trading, leading to more accurate predictions and better decision-making.	• Explore the use of quantum computing for financial modeling and risk analysis in energy markets.
Carbon Capture and Sequestration	• Quantum simulations can aid in the development of more effective carbon capture and sequestration technologies.	• Invest in research that applies quantum computing to molecular modelling of carbon capture materials.

Figure 2: Chart (designed by Thomas Morin) detailing opportunities and recommendations for quantum computing in critical energy infrastructure.

Risks:

Risks in Using Quantum Computing in Critical Energy Infrastructure

Risks	Potential	Recommendations
Cryptographic Vulnerabilities	• Quantum computers pose a threat to existing cryptographic systems used to secure energy infrastructure.	• Begin transitioning to post-quantum cryptography to safeguard sensitive data and control systems. • Conduct thorough risk assessments of cryptographic vulnerabilities.
Disruption of Existing Business Models	• Quantum-driven optimization could disrupt traditional energy market dynamics.	• Monitor the development of quantum computing and its potential impact on the energy sector. • Develop flexible business strategies to adapt to changing market conditions.
Talent Acquisition and Skill Gaps	• A shortage of skilled professionals in quantum computing could hinder adoption.	• Invest in training and education programs to develop quantum computing expertise. • Establish partnerships with universities and research institutions.
Computational overhead	• While quantum computers hold great promise, the current state of technology still comes with overhead, and error correction challenges.	• Carefully assess the viability of quantum solutions for specific problems. • Stay up to date with the improvements in quantum hardware and software.

Figure 3: Chart (designed by Thomas Morin) detailing risks and recommendations for quantum computing in critical energy infrastructure.

Artificial Intelligence in the Energy Sector

AI is rapidly transforming industries worldwide, and the energy sector is no exception. By leveraging advanced algorithms and computational power, AI enhances operational efficiency, optimizes grid management, and improves energy forecasting[xxviii]. Unlike traditional computing, which follows predefined rules, AI adapts and learns from data patterns, allowing for more sophisticated decision-making and automation. AI applications in energy range from predictive maintenance to real-time energy demand management, providing a level of precision and responsiveness that was previously unattainable.

One of the most promising aspects of AI in energy is its ability to analyze vast datasets to identify inefficiencies and predict system failures before they occur. Machine learning models can process information from sensors, smart meters, and historical data to optimize energy distribution[xxix]. AI-driven automation also enables demand response programs, where energy providers can adjust electricity supply in real time based on consumption patterns, reducing waste and enhancing grid stability[xxx]. Additionally, AI can improve renewable energy integration by forecasting solar and wind power generation more accurately, allowing grid operators to balance supply and demand effectively[xxxi].

Despite its immense potential, AI adoption in the energy sector is not without challenges. Legacy systems created before the recent rise of AI have many structural challenges in implementing AI. Moreover, the deployment of AI demands specialized expertise in both energy systems and data science, creating a significant skill gap that must be addressed to fully realize the benefits of AI in energy[xxxii].

The introduction of AI presents transformative opportunities for the energy sector, particularly in enhancing grid resiliency, optimizing energy consumption, and improving predictive maintenance. AI-driven grid management enables real-time monitoring and response, reducing the risk of outages and improving overall system stability. By analyzing data from sensors and smart meters, AI can detect anomalies and predict potential failures, allowing for proactive maintenance and reducing costly downtime[xxxiii].

Additionally, AI plays a critical role in energy efficiency and sustainability. Smart energy management systems powered by AI can optimize heating, cooling, and lighting in buildings based on occupancy patterns, leading to significant cost and energy savings[xxxiv]. AI-driven automation also enhances energy trading by analyzing market trends and optimizing pricing strategies. This allows energy providers to better manage supply and demand fluctuations, leading to more stable energy markets[xxxv].

Renewable energy integration is another area where AI excels. Wind and solar power generation are inherently variable (as the sun doesn't always shine, etc.), making it challenging to balance supply and demand. AI-powered forecasting models improve the accuracy of renewable energy predictions, enabling grid operators to adjust power distribution dynamically[xxxvi]. This reduces reliance on fossil fuels as backup energy sources and supports a smoother transition to renewable energy systems.

Despite its advantages, AI adoption in the energy sector presents several risks and challenges. One major concern is the lack of adequately trained energy professionals capable of implementing and managing AI-driven systems. Many energy workers lack experience with AI technologies. This could potentially lead to errors, inefficiencies, and underutilization of AI capabilities[xxxvii]. Without sufficient investment in workforce training, the industry may struggle to fully leverage AI's potential.

Another critical risk is cybersecurity. As AI becomes more embedded in energy infrastructure, it increases the sector's vulnerability to cyber threats[xxxviii]. AI-driven systems rely on vast amounts of data, which, if compromised, could disrupt energy operations. Many energy networks still rely on outdated cyber infrastructure that was not designed to withstand modern cyber threats. If AI systems are not properly secured, they could become targets for cyberattacks, leading to grid disruptions or data breaches.

Additionally, AI-driven decision-making introduces concerns regarding transparency and accountability. Machine learning models can be highly complex, making it difficult for energy professionals to understand how certain decisions are made[xxxix]. This lack of interpretability can create challenges in regulatory compliance and risk management. Ensuring that AI operates within ethical and legal guidelines requires ongoing oversight and the development of clear accountability frameworks.

AI has the potential to revolutionize the energy sector by improving efficiency, enhancing grid stability, and optimizing renewable energy integration. However, its successful implementation requires addressing key challenges, including workforce skill gaps, outdated infrastructure, and cybersecurity vulnerabilities. To fully harness AI's benefits, the energy industry must invest in training programs, modernize its cyber infrastructure, and develop regulatory frameworks that ensure AI-driven systems are secure and accountable. With the right strategies in place, AI can play a crucial role in shaping a more resilient and sustainable energy future.

Analysis of Security and Knowledge Gaps

Assessment of Current Security Capabilities

The energy sector is rapidly adopting emerging technologies like artificial intelligence (AI) to enhance operational efficiency, grid reliability, and sustainability. However, this growing reliance on advanced systems brings complex security challenges that the current energy workforce is largely underprepared to address. AI introduces vulnerabilities through its dependence on large-scale data, automated decision-making, and interconnected digital infrastructure.

Quantum technology, while still largely in the research and development stage, represents a potential future disruptor. Although not yet ready for real-world deployment in the

energy sector, its potential capabilities—particularly in breaking classical encryption—pose significant long-term security concerns[xl]. This looming threat, though not yet immediate, underscores the importance of quantum-aware training and planning across the industry.

Despite these risks, energy sector training programs have not kept pace with the interdisciplinary demands of emerging technologies. Worse still, many cybersecurity incidents go unnoticed due to underreporting and lack of detection[xli]. There is a critical need for targeted education and cross-sector training initiatives that prepare workers to anticipate, understand, and respond to these evolving challenges.

To support this transition, a coordinated push toward industry-wide standardization is essential. Establishing common guidelines for AI and quantum readiness—including training protocols, security benchmarks, and integration frameworks—would help ensure consistent, secure adoption across the sector and reduce systemic vulnerabilities.

General Recommendations

To prepare for the transformative impacts of both quantum computing and artificial intelligence (AI), the energy sector must adopt a forward-looking, integrated strategy. These technologies—though at different stages of maturity—promise to reshape how energy is generated, distributed, secured, and optimized. By taking early, strategic action, energy companies can position themselves to lead rather than lag in the coming technological shifts.

Strategic partnerships are essential. Energy companies should actively collaborate with the AI industry, quantum computing firms, academic institutions, and national laboratories. These partnerships provide access to cutting-edge research, facilitate co-designed solutions tailored to sector-specific needs, and foster innovation that might otherwise remain siloed. For AI, such partnerships can accelerate the deployment of predictive analytics for grid maintenance or demand forecasting. For quantum computing, they can lay the groundwork for future breakthroughs in energy storage modeling or cryptographic resilience.

Continuous monitoring is critical. Advancements in AI—including new machine learning models and regulatory standards—are rapidly evolving, as are developments in quantum hardware and error correction. Energy leaders must stay informed about these changes to make agile decisions on integration, investment, and risk management.

Workforce education remains a central pillar. Offering upskilling programs in AI and quantum computing will ensure that the energy workforce is not only aware of these technologies but prepared to implement them responsibly. Training should cover applied AI tools, quantum principles, and the cybersecurity implications of both, ideally linked to certification programs like the proposed Certified Energy Technology Security Officer (CETSO).

Pilot projects serve as low-risk environments for experimentation. Companies can trial AI for automating routine operations, optimizing energy consumption, or improving customer

demand forecasting. Quantum pilot efforts might focus on post-quantum encryption testing or simulating grid optimization problems at scale.

By investing in these areas, the energy sector can develop a robust technological foundation that supports secure innovation, builds internal expertise, and ensures long-term resilience in an increasingly digital and decentralized energy ecosystem.

Proposal for Industry Standardization

To address the widening gap between emerging technology adoption and workforce readiness in the energy sector, an industry-wide certification program is urgently needed. A proposed solution is the creation of a Certified Energy Technology Security Officer (CETSO) credential—a specialized certification designed to equip energy professionals with the interdisciplinary expertise necessary to navigate AI and future quantum-related risks.

This certification would serve as a standardized benchmark for evaluating readiness in three critical areas: emerging technology fluency, cybersecurity resilience, and energy system integration. By grounding the CETSO program in real-world use cases and sector-specific scenarios, the certification would ensure that participants are not only technically proficient but also capable of applying their knowledge in dynamic, high-risk environments. For example, candidates would need to demonstrate a working understanding of how adversarial AI threats could affect grid operations or how to begin planning for quantum-resistant encryption before quantum computing becomes a practical threat.

Importantly, the CETSO would also provide a unified response framework—a set of protocols and best practices for identifying, mitigating, and responding to technology-driven vulnerabilities in the energy sector. This would bring greater consistency across organizations and reduce fragmented approaches to security and technology integration.

The program could be developed in partnership with national laboratories, academic institutions, and public utility commissions to ensure it reflects current threats, future trends, and regulatory expectations. By standardizing both baseline knowledge and advanced skill sets, the CETSO would not only close current professional gaps but also support long-term energy resilience by preparing a workforce that can adapt securely as technology evolves.

Evaluate the Need for an Energy Tech Security Officer Role

The rapid integration of emerging technologies like AI and quantum computing into the energy sector has created a significant gap between technical innovation and security infrastructure. The role of a Certified Energy Technology Security Officer (CETSO) would be critical in addressing this gap. Unlike traditional IT or cybersecurity roles, a CETSO would be trained in the specific risks, regulatory demands, and operational dynamics unique to the energy industry. This position would serve as a bridge between engineers, cybersecurity experts, and executive leadership—ensuring that innovation is pursued without compromising reliability or safety. With AI models becoming more embedded in grid operations and quantum computing

threatening conventional encryption protocols, the CETSO would offer strategic oversight, implement risk mitigation measures, and lead the development of proactive response plans. Sector-wide adoption of this role could significantly strengthen national infrastructure resilience and establish a unified security posture across a fragmented industry.

Explore Guidelines for Certification Standards and Training

To effectively prepare energy professionals for the challenges introduced by AI and quantum computing, a standardized, interdisciplinary certification program is essential. Developing the Certified Energy Technology Security Officer (CETSO) designation would require coordinated input from industry experts, academic institutions, and government agencies. Certification guidelines should cover core competencies in AI deployment, cybersecurity fundamentals, quantum risk awareness, and sector-specific regulatory frameworks. Training programs must be scenario-based and emphasize practical, real-world applications to ensure the certification remains relevant and actionable. The inclusion of continuing education requirements will help professionals stay current with evolving threats and technologies. Additionally, certification pathways should be flexible enough to accommodate professionals from various backgrounds—whether in engineering, IT, or operations—while maintaining rigorous quality controls. By establishing clear guidelines and robust training infrastructure, the CETSO program would elevate industry-wide knowledge and foster a culture of technological accountability and security-first thinking across all layers of the energy workforce.

Analyze Collaborative Efforts Across Public, Private, and Academic Sectors

Successfully navigating the complex security landscape introduced by emerging technologies in energy requires robust collaboration across public, private, and academic sectors. Government agencies play a vital role in setting regulatory baselines and offering funding for pilot programs and research. Private companies, meanwhile, often serve as first adopters and are uniquely positioned to identify real-time risks and implementation bottlenecks. Academic institutions contribute through foundational research, curriculum development, and workforce training. Together, these stakeholders can create a feedback loop that accelerates innovation while maintaining security and compliance. Establishing public-private partnerships (PPPs), convening cross-sector working groups, and co-developing pilot programs are effective strategies to align goals and share expertise. For example, universities could partner with utilities to offer AI and quantum training modules, while government incentives could encourage secure deployment of experimental technologies. By fostering these collaborative ecosystems, the energy sector can achieve both resilience and responsible innovation at scale.

Conclusion

This paper explored the pressing challenges and transformative potential posed by emerging technologies—specifically AI and quantum computing—within the energy sector. While AI is already being deployed across grid management, forecasting, and efficiency optimization, its widespread adoption often outpaces the sector's readiness in terms of infrastructure, workforce training, and cybersecurity. Quantum computing, though largely theoretical in its current form, introduces long-term threats to encryption and data integrity that demand early strategic planning. Across both technologies, the energy sector remains underprepared, facing clear security vulnerabilities and professional skill gaps that cannot be ignored.

To ensure resilience and responsible innovation, the industry must take immediate action. This includes the development of sector-specific security standards, the creation of a Certified Energy Technology Security Officer role and continued cross-sector research on AI and quantum threats and applications. Partnerships between industry, academia, and government will be essential in driving this forward. The energy sector needs practical outcomes. New educational programs, certifications, and live tabletop exercises should be a priority for energy sector officials and leaders in the next two years. These steps will equip the sector with the professionals and the culture it needs to face these challenges. The best learning is through doing, which is why tabletop exercises to specifically evaluate the risks and gaps are critical. With the right partnerships, the energy sector can continue to innovate and securely deliver reliable energy to consumers around the country.

Looking ahead, the findings and proposals outlined here could serve as the foundation for a professional development course that could launch as early as 2025. This course will be designed to equip energy leaders and decision-makers with the tools and knowledge needed to manage technological change without compromising security or operational integrity. Topics will include emerging tech fundamentals, cybersecurity frameworks, risk assessment, and regulatory considerations—all framed within real-world energy sector use cases. As technology continues to evolve, so too must our leadership and preparedness. This course aims to meet that challenge head-on, building a smarter, safer, and more secure energy future.

About the Authors

	
Nick Reese	**Thomas Morin**
Nick Reese is the founder and CEO of Triantha and a Strategic Advisor to the Space ISAC. He is a former federal government technology policy maker and an adjunct professor at the NYU Center for Global Affairs.	Thomas Morin is an Emerging Technology Consultant and curriculum developer at Triantha. He is a graduate of the NYU Center for Global Affairs and is an expert in the geopolitical implications of emerging technology

Authors' Note

The authors would like to thank Sam Houston State University and the Institute for Homeland Security for their support of this important work and dedication to emerging technology education and research for critical infrastructure.

References

[i] Wallace, Danielle; *Russia Invades Ukraine in Largest European Attack Since WWII*; Fox News; February 24, 2022; https://www.foxnews.com/world/russian-invades-ukraine-largest-europe-attack-wwii

[ii] CISA; *The Attack on Colonial Pipeline: What We've Learned and What We've Done in the Past Two Years;* May 2023; https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[iii] Thompson, Liz. *Revolutionizing Energy Grid Maintenance: How Artificial Intelligence Is Transforming the Future*, 28 May 2024, www.anl.gov/article/revolutionizing-energy-grid-maintenance-how-artificial-intelligence-is-transforming-the-future.

[iv] IBID

[v] Annarita Giani, Zachary Goff-Eldredge. "How Quantum Computing Can Tackle Climate and Energy Challenges." *Eos*, 1 June 2023, eos.org/features/how-quantum-computing-can-tackle-climate-and-energy-challenges.

[vi] Ppdm. "Data Dilemma: Unraveling the Challenges and Downsides of Data in Oil and Gas." *JPT*, Journal of Petroleum Technology , 9 Aug. 2023, jpt.spe.org/data-dilemma-unraveling-the-challenges-and-downsides-of-data-in-oil-and-gas

[vii] Krause T, Ernst R, Klaer B, Hacker I, Henze M. Cybersecurity in Power Grids: Challenges and Opportunities. Sensors (Basel). 2021 Sep 16;21(18):6225. doi: 10.3390/s21186225. PMID: 34577432; PMCID: PMC8473297.

[viii] Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, Materne S. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. 2022;47(3):698-736. doi: 10.1057/s41288-022-00266-6. Epub 2022 Feb 17. PMID: 35194352; PMCID: PMC8853293.

[ix] Office, U.S. Government Accountability. *Science & Tech Spotlight: Securing Data for a Post-Quantum World | U.S. GAO*, 8 Mar. 2023, www.gao.gov/products/gao-23-106559

[x] Shepard, K. (2018, November 5). *Cryptography and communication security in a Digital Age - USC Viterbi School of Engineering*. USC Viterbi School of Engineering. https://illumin.usc.edu/cryptography-and-communication-security-in-a-digital-age-2/

[xi] Duke, S. (2025, April 4). *Why workers must UPSKILL as AI accelerates workplace changes*. World Economic Forum. https://www.weforum.org/stories/2025/04/linkedin-strategic-upskilling-ai-workplace-changes/

[xii] Zwetsloot, Remco. "Strengthening the U.S. AI Workforce." *Center for Security and Emerging Technology*, 30 Aug. 2023, cset.georgetown.edu/publication/strengthening-the-u-s-ai-workforce/.

[xiii] Leddy , C. (2019, January 23). *Q&A: The talent shortage in quantum computing*. MIT News | Massachusetts Institute of Technology. https://news.mit.edu/2019/mit-william-oliver-qanda-talent-shortage-quantum-computing-0123

[xiv] J.P. Pressley. "AI Is Revolutionizing Grid Planning in the Energy and Utilities Sector." *Technology Solutions That Drive Business*, 18 Dec. 2024, biztechmagazine.com/article/2024/10/ai-revolutionizing-grid-planning-energy-and-utilities-sector

[xv] Baker, Philip; *Quantum Paradigm Shift*; University of Chicago; May 29, 2024; https://professional.uchicago.edu/stories/quantum-science-networking-and-communications/quantum-paradigm-shift?language_content_entity=en#:~:text=Based%20on%20the%20foundational%20principles,scales%2C%20quantum%20computing%20represents%20a

[xvi] Schneider, Josh and Smalley, Ian; *What is Quantum Computing?*; IBM; August 5, 2024; https://www.ibm.com/think/topics/quantum-computing#:~:text=While%20classical%20computers%20rely%20on,at%20once%20using%20quantum%20bits

[xvii] Bearne, Adam; *Google unveils a quantum chip. Could it help unlock the universe's deepest secrets?*; NPR; https://www.keranews.org/2024-12-11/google-unveils-a-quantum-chip-could-it-help-unlock-the-universes-deepest-secrets

[xviii] Office of Science; *Creating the Heart of a Quantum Computer: Developing Qubits*; US Department of Energy; https://www.energy.gov/science/articles/creating-heart-quantum-computer-developing-qubits#:~:text=The%20principle%20of%20superposition%20is,two%20options%3A%201%20or%200.

[xix] Neilsen and Chuang; *Quantum Computing and Quantum Information*; Cambridge University Press; 2010; https://almuhammadi.com/sultan/books_2020/Nielsen_Chuang.pdf

[xx] Schneider, Josh and Smalley, Ian; *What is Quantum Computing?*; IBM; August 5, 2024; https://www.ibm.com/think/topics/quantum-computing#:~:text=While%20classical%20computers%20rely%20on,at%20once%20using%20quantum%20bits

[xxi] Gamble, Sara; *Quantum Computing: What It Is, Why We Want It, and How We're Trying to Get It*; National Academy of Sciences; 2019; https://www.ncbi.nlm.nih.gov/books/NBK538701/#:~:text=In%20reality%20a%20quantum%20computer,a%20series%20of%20operations%20

[xxii] Wootters, William; *Quantum Entanglement as a Quantifiable Resource*; Phil. Trans. R. Soc. A.3561717–1731; http://doi.org/10.1098/rsta.1998.0244

[xxiii] Feldman, Andy; *Entangling particles helps improve the accuracy of quantum measurements*; Advanced Science News; January 26, 2023; https://www.advancedsciencenews.com/entangling-particles-helps-improve-the-accuracy-of-quantum-measurements/

[xxiv] Ultimaco; *What is Shor's Algorithm?*; https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-shors-algorithm#:~:text=Shor's%20algorithm%20is%20a%20quantum,an%20integer%20in%20polynomial%20time.

[xxv] Edwards, Jason; *Quantum Computing and the Future of Cybersecurity*; The National CIO Review; https://nationalcioreview.com/articles-insights/information-security/quantum-computing-and-the-future-of-cybersecurity/#:~:text=However%2C%20quantum%20computers%20equipped%20with,potentially%20rendering%20RSA%20encryption%20ineffective.

[xxvi] Geeks for Geeks; *RSA Algorithm in Cryptography*; January 6, 2025; https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

[xxvii] NIST; *NIST Releases First 3 Finalized Post Quantum Encryption Standards*; August 13, 2024; https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[xxviii] J.P. Pressley. “AI Is Revolutionizing Grid Planning in the Energy and Utilities Sector.” *Technology Solutions That Drive Business*, 18 Dec. 2024, biztechmagazine.com/article/2024/10/ai-revolutionizing-grid-planning-energy-and-utilities-sector.

[xxix] Thompson, Liz. “Revolutionizing Energy Grid Maintenance: How Artificial Intelligence Is Transforming the Future | Argonne National Laboratory.” *Revolutionizing Energy Grid Maintenance: How Artificial Intelligence Is Transforming the Future*, 28 May 2024, www.anl.gov/article/revolutionizing-energy-grid-maintenance-how-artificial-intelligence-is-transforming-the-future.

[xxx] IBID

[xxxi] Rozite, Vida, et al. “Why AI and Energy Are the New Power Couple – Analysis.” *Why AI and Energy Are the New Power Couple*, IEA, 2 Nov. 2023, www.iea.org/commentaries/why-ai-and-energy-are-the-new-power-couple.

[xxxii] Zwetsloot, Remco. “Strengthening the U.S. AI Workforce.” *Center for Security and Emerging Technology*, 30 Aug. 2023, cset.georgetown.edu/publication/strengthening-the-u-s-ai-workforce/.

[xxxiii] Rozite, Vida, et al. “Why AI and Energy Are the New Power Couple – Analysis.” *Why AI and Energy Are the New Power Couple*, IEA, 2 Nov. 2023, www.iea.org/commentaries/why-ai-and-energy-are-the-new-power-couple.

[xxxiv] IBID

[xxxv] IBID

[xxxvi] IBID

[xxxvii] Zwetsloot, Remco. “Strengthening the U.S. AI Workforce.” *Center for Security and Emerging Technology*, 30 Aug. 2023, cset.georgetown.edu/publication/strengthening-the-u-s-ai-workforce/.

[xxxviii] Krause T, Ernst R, Klaer B, Hacker I, Henze M. Cybersecurity in Power Grids: Challenges and Opportunities. Sensors (Basel). 2021 Sep 16;21(18):6225. doi: 10.3390/s21186225. PMID: 34577432; PMCID: PMC8473297.

[xxxix] Dittmar, Lee. *What Does Transparency Really Mean in the Context of AI Governance?*, OCEG, 8 Nov. 2024, www.oceg.org/what-does-transparency-really-mean-in-the-context-of-ai-governance/.

[xl] Edwards, Jason; *Quantum Computing and the Future of Cybersecurity*; The National CIO Review; https://nationalcioreview.com/articles-insights/information-security/quantum-computing-and-the-future-of-cybersecurity/#:~:text=However%2C%20quantum%20computers%20equipped%20with,potentially%20rendering%20RSA%20encryption%20ineffective.

[xli] Casanovas, M. C., & Nghiem, A. *Cybersecurity – is the power system lagging behind?*. IEA. 3 Aug 2023, https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind

INSTITUTE FOR HOMELAND SECURITY

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water / Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Reese, N., & Morin, T. (2025). Emerging Technology in the Energy Sector: Threats, Vulnerabilities, and Recommendations for Industry (Institute for Homeland Security Report No. 2025-1017). Institute for Homeland Security.

https://doi.org/10.17605/OSF.IO/A638Q