Chapter 15
Quantum AI and Cybersecurity:
The Next Frontier in Industrial Security

Varsha Tyagi
https://orcid.org/0009-0004-9223-3174
Raj Kumar Goel Institute of Technology, Ghaziabad, India

Pallavi Tyagi
Raj Kumar Goel Institute of Technology, Ghaziabad, India

Gauravkant Tyagi
Equinor ASA, Norway

Pawan Kumar Goel
https://orcid.org/0000-0003-3601-102X
Raj Kumar Goel Institute of Technology, Ghaziabad, India

ABSTRACT

Quantum AI is emerging as a groundbreaking solution in the field of cybersecurity, particularly for industrial automation. With the increasing sophistication of cyber threats, traditional security measures are becoming inadequate to protect critical infrastructure. This chapter explores the integration of quantum computing and artificial intelligence (AI) to fortify industrial security. It discusses key concepts such as quantum cryptography, AI-driven threat detection, and real-time anomaly monitoring. The chapter also highlights the challenges associated with implementing quantum AI in industrial settings and outlines future research directions. By utilizing quantum AI, industries can achieve unprecedented levels of security, ensuring robust protection against evolving cyber threats.

DOI: 10.4018/979-8-3373-3241-3.ch015

1. INTRODUCTION

Imagine a world where computers can solve the hardest problems in just seconds. A world where even the strongest data protections can be broken easily, and where artificial intelligence (AI) becomes smarter than anything we've seen before. This isn't science fiction — it's the new reality that quantum computing is bringing, and it's coming soon in our daily life.

Right now, we are at a turning point where quantum computing, AI, and cybersecurity are coming together. This powerful combination will change the way we think about technology and security in ways we are just starting to understand. It's like we've been playing a simple game of chess, and suddenly, the game has changed into something much bigger and more complex, where the rules keep changing with every move.

In the past, we explored how AI affects security and human rights. Now, we are stepping into a new and even more mysterious area: the world of quantum technology — a field that could change everything.

For decades, cybersecurity has been like building bigger and stronger walls to keep intruders out (Smith, 2022). But with quantum computing, the very idea of walls might become useless. Quantum machines won't just be faster — they'll be able to solve problems that traditional computers would take millions of years to crack (Shor, 1994). This means today's encryption methods, which protect everything from bank accounts to national secrets, could become powerless almost overnight (Mosca, 2018).

At the same time, quantum technology offers new ways to defend ourselves. Quantum encryption — using the strange properties of particles — can create communication lines that are impossible to hack without being noticed (Bennett & Brassard, 1984). It's like setting a trap where the intruder trips an alarm just by trying to open the door.

Artificial intelligence, already a key player in cybersecurity, will also get a quantum upgrade. Quantum AI could detect cyber threats in real time, even before attacks happen, by analyzing massive amounts of data at speeds never seen before (Huang et al., 2022). This would allow security systems not just to react to attacks, but to predict and prevent them.

However, this new world comes with its own challenges. Quantum computers will first be in the hands of governments and big corporations, leading to a "quantum divide" between the powerful and the vulnerable (Preskill, 2018). Smaller businesses, and everyday users, might find themselves at a disadvantage, facing risks they are not prepared for.

We are not just preparing for faster computers — we are preparing for a complete change in the rules of cybersecurity. In this new era, survival won't depend on stronger walls, but on smarter, quantum-powered strategies (Bindel et al., 2019).

Cybersecurity encompasses a range of technologies, processes, and practices designed to safeguard networks, devices, software, and data from attacks, damage, or unauthorized access. The complexity of cybersecurity is increasing due to the rapid expansion of interconnected devices, systems, and networks. This challenge is further intensified by advancements in the digital economy and infrastructure, which have contributed to a significant rise in cyberattacks with severe consequences.

Additionally, research highlights the continuous evolution of cyber threats, including those posed by nation-state-affiliated groups and criminal adversaries, who employ increasingly sophisticated tactics to infiltrate even the most secure systems. As cyber threats become more advanced, the frequency, scale, and impact of cyberattacks are also rising, making it essential to adopt intelligence-driven cybersecurity measures. This approach enables dynamic defense mechanisms against evolving cyber threats and helps manage large volumes of security data effectively. Organizations such as the National Institute