Keynote Speech

by

Khun David (Dej) Titivanich

Assistant Governor, Information Technology Group, Bank of Thailand

TB-Cert Cybersecurity Annual Conference 2025

The Quantum-AI Shift: Cybersecurity and Fraud in the Next Era

09.00 am – 09.10 am August 21, 2025

Ballroom, Intercontinental Hotel

---

1. Opening

Good morning, distinguished guests and members of the banking sector's CERT community.

It is an honor to speak at this pivotal moment when the convergence of quantum computing and artificial intelligence is redefining the cybersecurity landscape.

The financial sector has always been at the forefront of technological adoption. From real-time payment systems to digital financial platforms, technology has enabled us to deliver efficient, innovative, and more inclusive financial services.

Today, two transformative technologies, AI and Quantum Computing, are reshaping the financial landscape. We are not merely witnessing a technological revolution, but are entering a new paradigm of threats and defenses.

2. The Dual Nature of Emerging Technologies

Artificial Intelligence has transformed security operations. It enables predictive analytics, detects anomalies in real time, and automates responses with remarkable speed. But it is a double-edged sword: the same technology that strengthens our defenses also empowers adversaries.

Today, Generative AI can craft realistic phishing emails, produce convincing deepfakes, and fabricate synthetic identities. Even more concerning, AI-enabled malware can adapt and evolve to bypass traditional security measures.

And the threat doesn't stop there. According to Gartner, quantum computing is expected to reach commercial maturity within this decade. When that happens, it will accelerate AI-driven threats, amplifying their speed, scale and complexity beyond what traditional defenses can manage.

Quantum computing isn't just a technological milestone — it's a cryptographic tipping point. With Shor's Algorithm, quantum computers are expected to break asymmetric encryption algorithms like RSA in hours, whereas classical computers would take millions of years.

Moreover, a key concern now is the threat of "harvest now, decrypt later" attacks. Adversaries can collect encrypted communications today and decrypt them in the future once quantum computing becomes functional and accessible.

Thus, the Quantum-AI shift accelerates the threat surface to become more non-linear and adaptive, which is a challenge that we must all prepare for.

3. Implications for the Banking Sector

For banks, the implications are profound. Banks must help safeguard customers and ensure the security and reliability of financial services. Technology should be leveraged not only for business growth but also to strengthen defenses and enhance operational resilience.

One critical area is the integration of AI into Security Operations Centers (SOCs). This can dramatically improve real-time monitoring, accelerate anomaly detection, and automate incident response, which reduces both reaction time and human error to ensure timely preventive measures.

Another key area is the enhancement of fraud detection and prevention. AI can enable timely alerts to customers and help prevent suspicious transactions. Although we have come a long way, our Central Fraud Registry (CFR) still relies on static rule-based mechanisms with limited customer profile data, which may not be conducive to rapid mule account traceability, especially when transfers to higher-tiered mule accounts can occur within minutes. AI might play a role in unlocking such limitations and empowering the CFR to become an effective infrastructure for fraud detection and prevention, reinforcing trust in the financial system.

Finally, transitioning to quantum-safe algorithms is no longer optional. NIST has already proposed post-quantum cryptographic standards. It is inevitable for financial institutions to start their journey in adopting quantum-proof encryption technologies to uplift their existing security infrastructure.

Additionally, migration to post-quantum cryptography, or PQC, requires substantial time and effort, so planning early would be beneficial. In parallel, banks should also consider cryptographic agility for adapting to new cryptographic standards, as they emerge, to ensure long-term security and integrity of sensitive financial data.

4. What should we do next to catch up with the Quantum-AI trend?

As for the Bank of Thailand, we have already started the journey for BAHTNET, our Realtime Gross Settlement and High Value Payment system, by inventorizing cryptographic algorithms used, and planning a migration strategy to incorporate quantum-safe algorithms as part of the BAHTNET Modernization project.

As a regulator, we plan to publish the AI Risk Management Guideline, a principle-based policy framework for banks, within this year. It promotes the safe and secure use of AI while effectively managing associated risks, aligned with responsible AI principles (ETDA, MAS, HKMA) and international standards (NIST, ISO).

The guideline emphasizes that banks remain accountable for AI-driven decisions, have governance and comprehensive risk management framework for AI, and ensure customer protection for AI services.

As we move toward the quantum era, we also support the banking industry's transition to quantum-safe infrastructure. We plan to raise quantum risk awareness, targeting banks' board-level and senior management. Additionally, we will collaborate with TBCERT to set up a task force to lead the industry's transition to the post-quantum era.

5. The Role of TB-CERT and Industry Collaboration

TB-CERT has always been the main driving force behind the implementation of secure practices and standards within the banking community. Since its inception, TB-CERT has played a vital role in fostering collaboration and enhancing cybersecurity readiness across the sector.

In this digital payment era, threat actors are adapting rapidly and focusing directly on customers. Over the past two years, TB-CERT has helped the industry eliminate unauthorized fraud and overcome many forms of malware on mobile banking apps. Today, thanks to TB-CERT's contributions, there have been zero cases of unauthorized fraud.

The next challenge is navigating the transition to the Quantum-AI era. Looking forward, the Bank of Thailand expects TB-CERT to continue playing as a strategic leadership role in capability development and proactively guide the financial sector through this transformation.

6. Closing

In closing, the Quantum-AI shift is not a distant future; it's unfolding now. Let us not be passive observers, but active architects of secure, resilient financial systems.

Together, we can shape a future where innovation and security coexist.

Thank you.
