Publications

Updated 12 July 2025

Why?

I believe thought leaders must continue to learn all their lives and share their knowledge and experience with others.

Disclaimer: All views expressed in my papers and articles are entirely my own and may not necessarily be shared by the Bank of England (or my previous employers). All errors are solely mine.

Quantum and Post-Quantum Security

In my view, crypto agility is essential to protect against weaknesses in traditional cryptography as well as the "harvest now, decrypt later" threat from sophisticated actors with access to quantum computers. I humbly disagree with the 2030–35 roadmaps suggested by fellow professionals, as the man-in-the-middle attack threat already exists. From March 2025, I started providing free post-quantum cryptographic key pairs for researchers and technology enthusiasts.

[Please press "Ctrl" when clicking so the document opens in a new window]

- Cryptoagility strategies for quantum-resistant transitions
- Quantum readiness of Linux technology stack
- Shor's pseudocode for RSA4096 quantum factoring
- Quantum computers and cryptography explained
- Debian Trixie wins PQC OS award
- Bash scripts for quantum-safe Linux security
- Browsers' post-quantum cryptography implementation comparison
- Post-Quantum hacking challenge security recommendations
- Launching FrodoKEM quantum-safe cryptography tools

AI and Technology Trends

In my view, artificial intelligence (AI) can help humans improve their efficiency by handling tasks that are repetitive or require sharp memory. Agentic AI projects can succeed through five pillars: clear vision, grounded ambition, leadership, customer focus, and transparency. However, AI hallucinates in expert code reviews and lacks true human reasoning, making it a tool prone to overconfidence. Over-reliance on AI invites risks; I insist on human oversight, targeted prompting, and standards compliance.

- Five pillars ensure agentic AI success (Co-author)
- Testing AI's expert code review abilities
- Debunking AI hype with Apple insights

- AI standards and guidance list
- Warnings on AI over-reliance risks

Cybersecurity Threats and Analysis

Each asset connected to the internet is an invaluable source of cyber threat intelligence (CTI) that has helped me identify a number of threats ahead of actual attacks. Although zero-day attacks are particularly difficult, I prefer not to use them as an excuse. I practice a strong patching discipline (within 24 hours) and worry that prioritization based on CVSS, EPSS, KEV, and LEV may generate unnecessary risks. My latest experiments involve AI-supported white-box purple testing of edge cases in APIs and web applications.

- Bybit hack exposes crypto security flaws
- CTI analysis of continental hacking patterns
- November 2022 cyber-attack trends
- Increased vulnerability scans emphasize firewall necessity
- Explaining CVSS EPSS KEV LEV vulnerabilities

Cryptography and Encryption Strategies

This section covers my miscellaneous work on non-PQC topics and the ICT/cyber components of the EU Digital Operational Resilience Act.

- DORA ICT encryption cryptography strategies
- Transcript of DNSSEC discussion with ChatGPT
- SPF DKIM DMARC email security guide
- Quiz assesses cryptographic security baseline

Security Implementation and Best Practices

This section includes privacy and security.

- Multi-layered secure IPv6 implementation strategies
- Implementing CISA's secure software recommendations
- Amnesic Computing Standards for privacy
- Brave browser privacy setup tutorial
- Software Ecosystem and future software event talk

Technology Risk Management and CEO/CRO Role

- Future CRO skills for risk management success

Book

- *Cyber Landscape in 2035 (Manuscript stage)*