



BUSINESS INTELLIGENCE REPORT

Explore this month's edition, covering the latest developments in AI, cybersecurity, and global news, as we dive into the rapidly evolving and transformative world of technology and current events.

www.qwantiv.com

KEY TAKEAWAYS

Economic & Market Shifts:

- Wall Street reacts to new policies under Trump's administration.
- Tariffs on China and Europe may keep inflation elevated at 2.5% in 2025.
- CBDCs (Central Bank Digital Currencies) gain traction, reshaping global finance.

Cybersecurity & Tech Disruptions:

- Quantum computing threatens encryption, driving the push for post-quantum cryptographic standards.
- Supply chain cybersecurity risks are growing, with companies reinforcing vendor security.
- WhatsApp spyware attack raises privacy and security concerns.

AI & Innovation Trends:

- AI-driven financial tools personalize banking and investment services.
- China's DeepSeek AI and Big Tech earnings shape market sentiment.
- Apple's Starlink-enabled iOS 18.3 enhances global connectivity.

VC & M&A Highlights:

- AI-powered climate tech sees record funding as sustainability investments rise.
 - DefenseTech investment surges amid geopolitical tensions.
 - Biotech startups face liquidity challenges, leading to distressed M&A deals.
-



THE BUZZ

The US economic, market themes emerging for 2025: YF Chartbook

As Wall Street adjusts to President Trump's return to the Oval Office and the wave of new policies and executive actions he has since signed into law. Read more [HERE](#)



DeepSeek AI, Big Tech earnings, Fed decision

China's introduction of DeepSeek, a Chinese startup that launched a reportedly cost-effective artificial intelligence (AI) chatbot, sent ripples through Wall Street.

Read more [HERE](#)



Meta Confirms Zero-Click WhatsApp Spyware Attack Targeting 90 Journalists, Activists

Meta-owned WhatsApp said on Friday that it disrupted a campaign that involved the use of spyware to target journalists and civil society members.

Read more [HERE](#)



Apple's New 'Game Changer' iPhone Update Brings Starlink Satellite Access

Apple has just released iOS 18.3, its latest iPhone update (full details [here](#)) and the software contained a surprise extra: compatibility with the Starlink satellite network, according to a new report.



FINANCIAL TRENDS

Trends For January 2025

Central Bank Digital Currencies (CBDCs) Rollout:

By early 2025, CBDCs are likely to transition from pilot phases to broader implementation as governments prioritize financial digitization and sovereignty. For example, the European Central Bank's digital euro and China's digital yuan (e-CNY) could dominate cross-border transactions, reducing reliance on SWIFT and private stablecoins. Emerging economies like India and Nigeria may also expand CBDC use to enhance financial inclusion, targeting unbanked populations via offline-enabled digital wallets. However, debates over privacy (e.g., programmable money tracking spending) and cybersecurity risks (e.g., hacking of centralized ledgers) could spark regulatory clashes. Central banks will likely collaborate with fintech firms to design user-friendly interfaces while balancing anti-money laundering (AML) requirements. By Q1 2025, CBDC adoption could reshape remittance markets and challenge cryptocurrencies like USDT in developing nations.



AI-Powered Hyper-Personalization in Finance:

Generative AI tools, such as advanced LLMs (Large Language Models), are expected to revolutionize financial services by 2025. Banks and robo-advisors might deploy AI to create dynamic, individualized portfolios that adjust in real-time based on macroeconomic data, life events (e.g., marriage, retirement), or even social media sentiment. For instance, tools like ChatGPT-5 could act as 24/7 financial coaches, analyzing spending habits and recommending tax-saving strategies. Insurtech firms may leverage AI to offer hyper-customized premiums using IoT data from smart homes or wearables. However, ethical concerns—such as algorithmic bias in loan approvals or over-reliance on opaque AI systems—could prompt stricter regulations, akin to the EU's AI Act. By February 2025, firms failing to transparently audit their AI models may face reputational and legal risks.

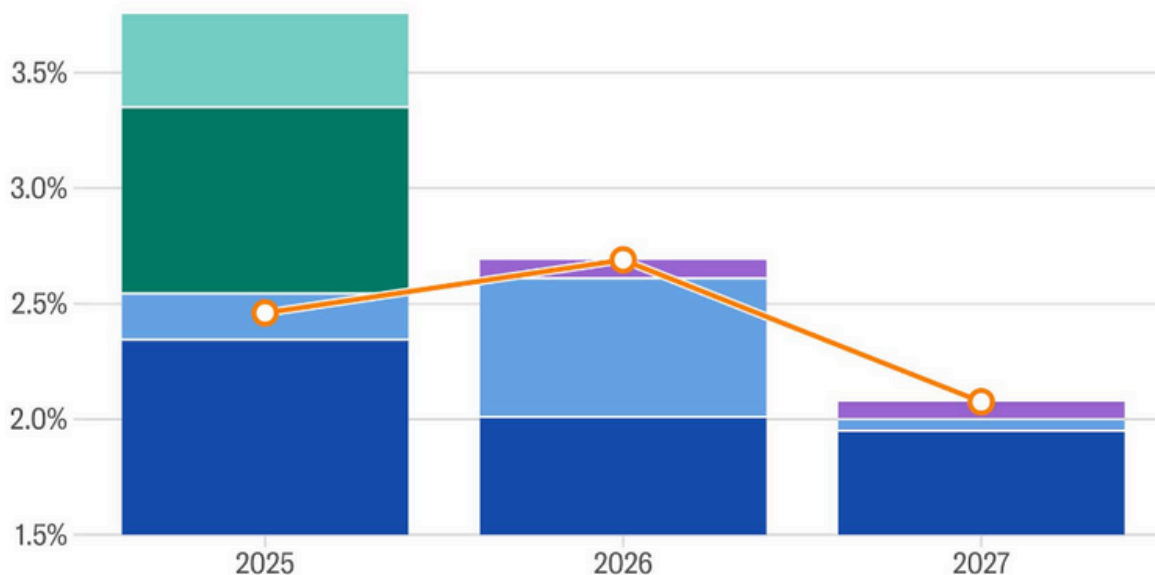
Robust U.S. Labor Market:

The U.S. labour market remains strong, with economists anticipating the addition of 170,000 new jobs in January and an unemployment rate holding steady at 4.1%. Factors such as recent natural disasters and annual data revisions may influence these figures

TARIFFS COULD PUSH UP INFLATION OUTLOOK

● CURRENT DEUTSCHE BANK FORECAST ● PRE-TRUMP FORECAST ● TARIFFS ● ADDITIONAL DEMAND/LAGGED INFLATION
● CANADA/MEXICO 50% PASS-THROUGH ● CANADA/MEXICO 75% PASS-THROUGH

PERCENTAGE POINT CONTRIBUTION TO INFLATION RATE



SOURCE: DEUTSCHE BANK VIA MATTHEW LUZZETTI

yahoo!finance

Trump Tariffs:

Initially, it projected that core Personal Consumption Expenditures (PCE) inflation would decrease to 2.3% this year, assuming no changes in tariff policies. However, considering our current baseline scenario—which includes a 20 percentage point increase in tariffs on Chinese imports, aligning tariff rates on European auto imports, and implementing a 5% universal baseline tariff in 2026—we now anticipate that core PCE inflation will persist at 2.5% in 2025.

THE CYBER PULSE

The Changing Landscape of Cyber

Quantum-Resistant Encryption Efforts

As quantum computing technology advances, it poses a significant threat to current encryption standards. Quantum computers can potentially solve complex mathematical problems, such as factoring large prime numbers, much more efficiently than classical computers. This capability could render widely used encryption methods, like RSA and ECC, vulnerable, as they rely on the difficulty of these mathematical problems for security.

In response, the cybersecurity community is actively developing and standardizing quantum-resistant, or post-quantum, cryptographic algorithms designed to withstand attacks from quantum computers. The U.S. National Institute of Standards and Technology (NIST) has been at the forefront of this initiative, evaluating various algorithms to establish new cryptographic standards. After extensive research, NIST has approved three algorithms for post-quantum cryptography, which will be integrated into hardware and software systems to enhance security against future quantum threats.

One notable example of a quantum-resistant algorithm is NTRU (Nth-degree Truncated Polynomial Ring Units), a public-key cryptosystem that utilizes lattice-based cryptography. Unlike traditional systems, NTRU is resistant to attacks using Shor's algorithm, making it a promising candidate for post-quantum encryption.

The urgency of adopting quantum-resistant encryption is underscored by the “harvest now, decrypt later” threat model. In this scenario, adversaries collect and store encrypted data today, anticipating that future quantum computers will be able to decrypt it. To mitigate this risk, organizations are encouraged to transition to quantum-resistant algorithms promptly, ensuring the long-term confidentiality and integrity of sensitive information.



Increased Focus on Supply Chain Security

The complexity and globalization of modern supply chains have introduced significant cybersecurity challenges. Organizations often rely on a network of third-party vendors and suppliers, each potentially introducing vulnerabilities into the system. Recent cyberattacks have exploited these supply chain weaknesses, leading to data breaches and operational disruptions.

For instance, North Korean cyber actors have been known to compromise supply chains by utilizing social engineering tactics and Trojan software, aiming to infiltrate organizations indirectly through their suppliers.

In response to these threats, organizations are implementing more stringent security measures across their supply chains. Key strategies include:

- **Vendor Risk Assessments:** Conducting thorough evaluations of suppliers' security practices to identify and mitigate potential risks before establishing partnerships.
- **Continuous Monitoring:** Implementing systems to monitor third-party activities in real-time, allowing for the rapid detection and response to suspicious behaviours.
- **Contractual Security Requirements:** Establishing clear security expectations and requirements within contracts to ensure suppliers adhere to the organization's cybersecurity standards.
- **Incident Response Collaboration:** Develop joint incident response plans with suppliers to ensure coordinated and effective actions in the event of a security breach.

By adopting these measures, organizations aim to enhance the resilience of their supply chains against cyber threats, thereby safeguarding their operations and data from potential compromises.

In summary, the evolving landscape of cybersecurity in 2025 highlights the critical importance of advancing encryption methods to counteract emerging threats from quantum computing and strengthening supply chain security to protect against increasingly sophisticated cyberattacks.



VENTURE CAPITAL SPOTLIGHT

Key VC Trends for Early 2025

AI-Infused Climate Tech Dominates VC Funding:

Climate tech startups integrating generative AI for carbon accounting, grid optimisation, and ESG reporting attract record-breaking rounds.

- PitchBook Data Angle:
 - Median deal size for AI-climate startups hits \$50M+ in Series B (up 30% YoY).
 - Corporate VCs like Shell Ventures and Microsoft Climate Innovation Fund lead deals.
 - Example: A startup using AI to predict wildfire risks (e.g., Overstory AI) raises 200Mata200Mata1.5B valuation.

DefenseTech Surges Amid Geopolitical Tensions

Rising global conflicts drive VC interest in dual-use technologies (e.g., autonomous drones, cyber-physical systems).

- PitchBook Data Angle:
 - DefenseTech deal count grows by 40% YoY in Q1 2025.
 - Sequoia and a16z double down on startups like Anduril or Shield AI.
 - Sovereign wealth funds (e.g., Saudi Arabia's PIF) co-invest in "national security AI" ventures.

Liquidity Crunch for Late-Stage Biotech Startups

High interest rates and FDA approval bottlenecks force down rounds and fire sales.

- PitchBook Data Angle:
 - The biotech IPO window remains shut; 75% of Series D+ rounds are flat or down.
 - Distressed M&A accelerates as Big Pharma (e.g., Pfizer, Roche) acquire gene-editing startups at discounts.