# BUSINESS INTELLIGENCE REPORT

Navigating Trends in Cybersecurity, Technology, and Private Investments

As we close the first quarter of 2025, this report provides a data-driven analysis of key developments shaping the cybersecurity, technology, and private investment landscape. We break down the most critical insights impacting businesses, investors, and decision-makers, from evolving threat intelligence and regulatory shifts to emerging innovations and market movements.

www.qwantiv.com

# KEY TAKEAWAYS

- The U.S. imposed significant tariffs on imports from Canada (25%), Mexico (25%), and China (10%), aiming to address economic and security concerns. While expected to generate $100B annually, these tariffs are likely to increase inflation, disrupt supply chains, and trigger retaliatory trade measures from affected countries.
- DeepSeek's AI model launch in China caused a $1 trillion+ sell-off in global markets, showcasing China's rapid advancements in AI and intensifying competition with Western firms. Meanwhile, Baidu acquired JOYY's live-streaming business for $2.1 billion, strengthening its dominance in China's digital sector.
- Cybersecurity threats escalated with state-sponsored cyber espionage from China, Russia, and North Korea. Chinese hackers infiltrated U.S. political and telecom systems, Russian cyber units attacked Ukrainian infrastructure, and North Korea's Lazarus Group stole £5 billion in cryptocurrency to fund its weapons program.
- AI is revolutionizing cybersecurity by enhancing threat detection and automating security responses, but concerns over AI-driven cyberattacks, investment costs, and potential biases in AI models continue to pose challenges.
- In response to increasing cyber threats, the U.S. and EU strengthened cyber defense collaboration, imposed sanctions on Chinese and Russian entities, and launched initiatives to track and seize illicit cryptocurrency flows linked to cybercrime.
- Venture capital funding is heavily concentrated in AI, HealthTech, ClimateTech, FoodTech, and FinTech. Key deals include Bridgetown Research's $19M funding for AI-powered market analysis and Safe Superintelligence Inc.'s $1B investment in AI safety research.
- The quantum computing market is expected to grow from $839M in 2023 to $16.2B by 2034, driven by increased research funding, cybersecurity applications, and pharmaceutical advancements.
- AI-driven medical diagnostics and longevity-focused biotech startups are attracting increased venture capital, with companies like Viz.ai and Everlab leading investments in AI-powered healthcare solutions.
- Sustainability-focused investments are on the rise, with MGA Thermal and Fleet Space Technologies developing innovative solutions in renewable energy and resource exploration.
- As Q2 2025 approaches, rising geopolitical uncertainty, cybersecurity risks, and AI advancements will continue to shape global markets. Businesses must prioritize AI-driven security frameworks, regulatory compliance, and strategic investments in emerging technologies to navigate the evolving landscape.

# THE BUZZ

## DeepSeek rushes to launch new AI model as China goes all in

Last month, the Chinese startup triggered a $1 trillion-plus sell-off in global equities markets with a cut-price AI reasoning model that outperformed many Western competitors. Read more **HERE**


---

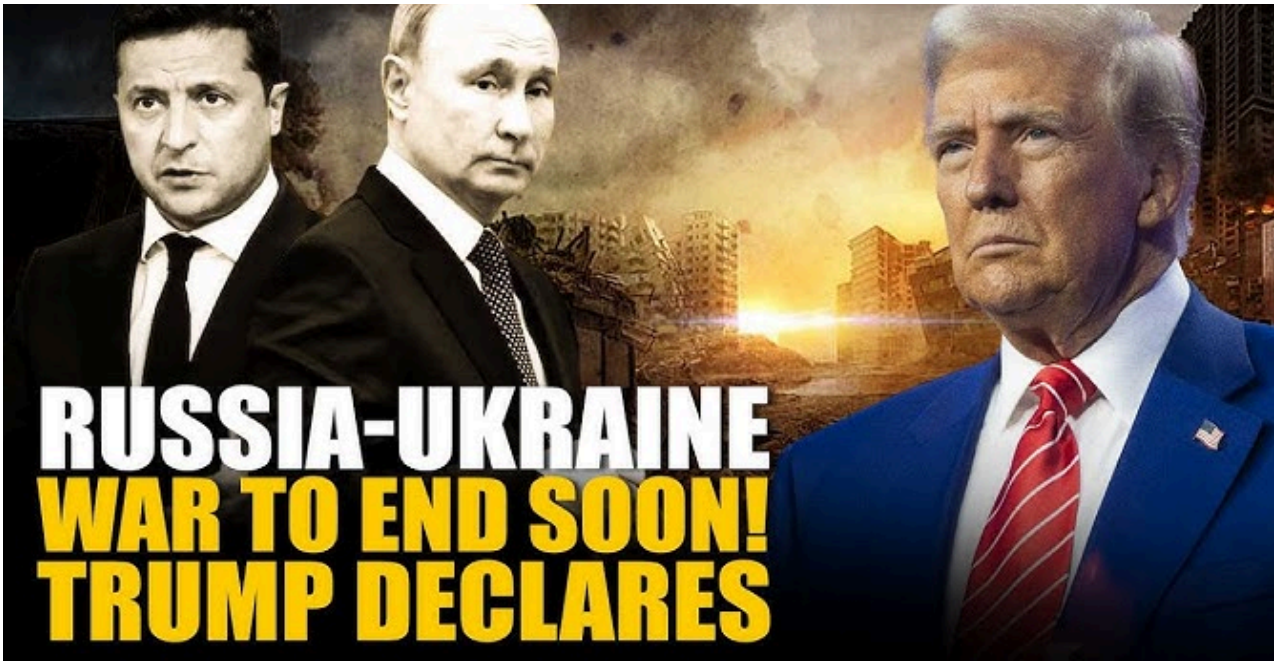
## Baidu acquires JOYY's live-streaming business in China for $2.1 billion

U.S.-listed shares of JOYY jumped 6%, while Baidu was up about 1% in premarket trading. Read more **HERE**


---

## Trump teases 'economic development' with Russia as he marks the third year of the war in Ukraine

President Donald Trump added a new wrinkle to ongoing talks that he says may help end the war in Ukraine: new "economic development" with Russia that the president says could come in addition to ongoing discussions between the US and Ukraine.
Read more **HERE**




---

## Crypto's biggest hacks and heists after $1.5 billion theft from Bybit

Cryptocurrency exchange Bybit said last week hackers had stolen digital tokens worth around $1.5 billion, in what researchers called the biggest crypto heist of all time.
Read more **HERE**


---

# FINANCIAL TRENDS

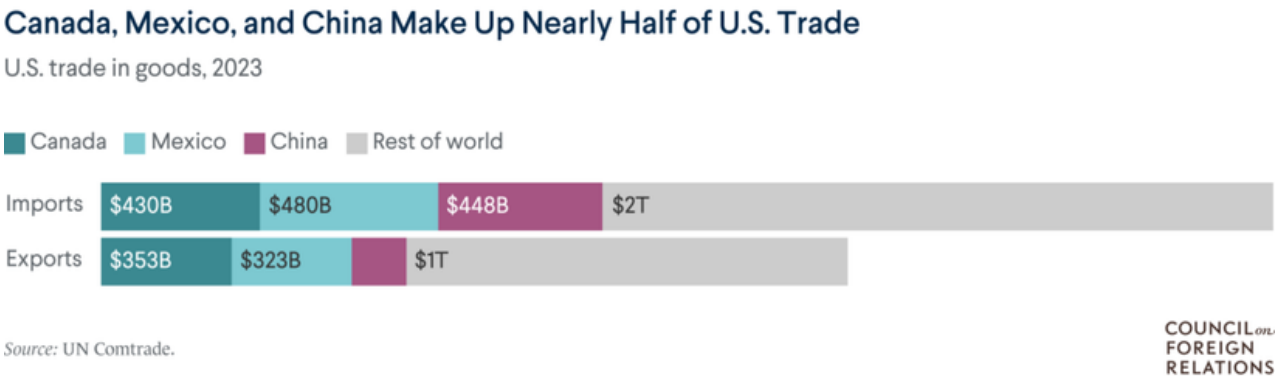
## Trends For Q1 2025

**Implementation of New Tariffs and Trade Policies:**

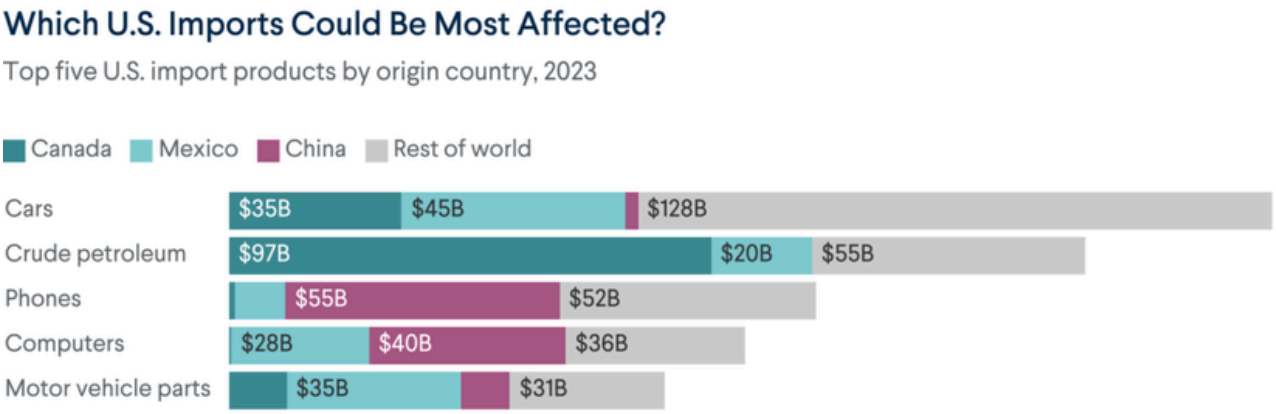
In early February 2025, President Donald Trump introduced significant tariffs on imports from Canada, China, and Mexico, aiming to address issues such as migration, drug trafficking, and the influx of fentanyl precursor chemicals. These tariffs impose a 25% tax on all goods from Canada and Mexico and a 10% tax on imports from China. This move is expected to have profound economic implications for the United States and its trading partners.

**Impact on the United States:**

The tariffs affect nearly half of all U.S. imports, totalling over $1.3 trillion. Analysts predict a potential 15% reduction in overall U.S. imports due to these measures. While the tariffs could generate approximately $100 billion annually in federal tax revenue, they may also disrupt supply chains, increase business costs, lead to job losses, and raise consumer prices.



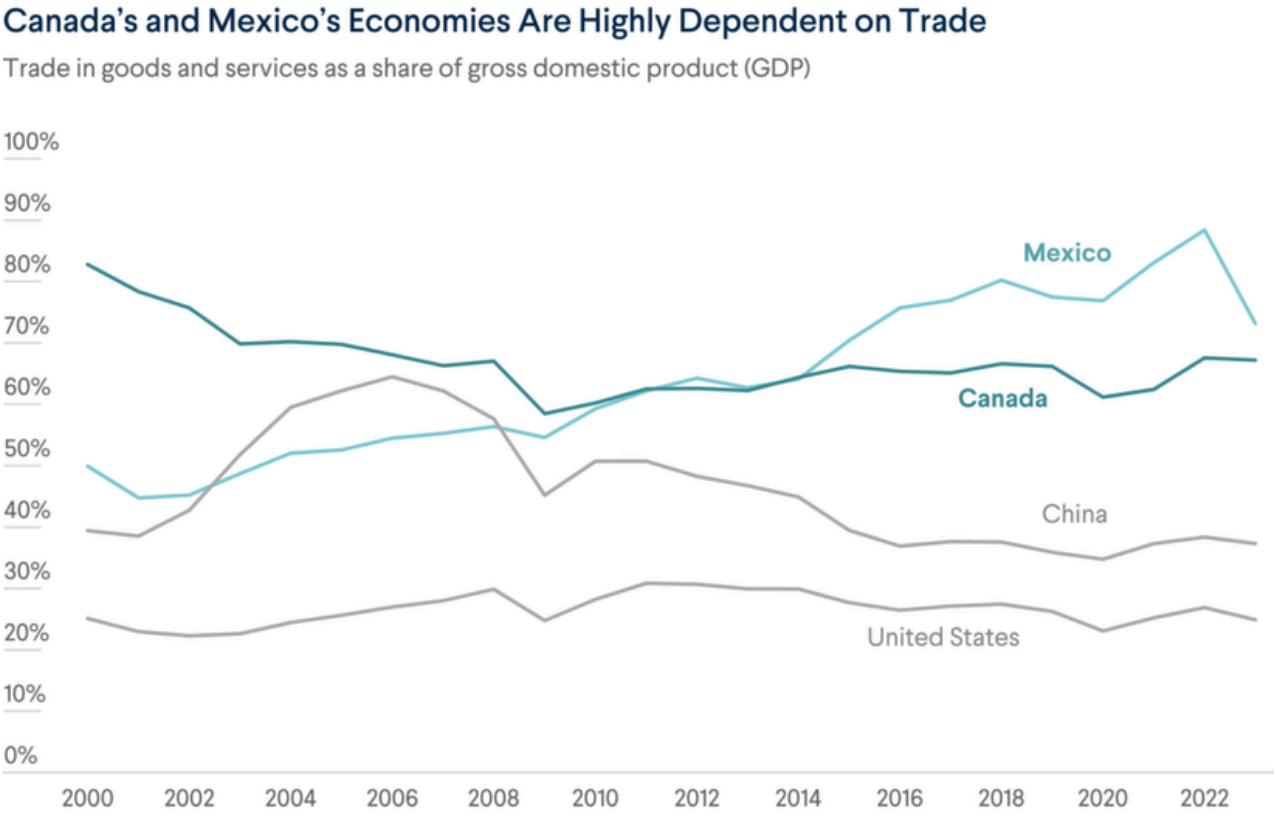

Sectors such as automotive, energy, and agriculture are particularly vulnerable. Gasoline prices in the Midwest could rise by up to 50 cents per gallon, given that Canada and Mexico supply more than 70% of U.S. crude oil imports. The automotive industry might see production costs increase, potentially adding up to $3,000 to the price of some vehicles. Additionally, grocery prices could climb, as Mexico provides over 60% of U.S. vegetable imports and nearly half of all fruit and nut imports.




**Impact on Canada and Mexico:**

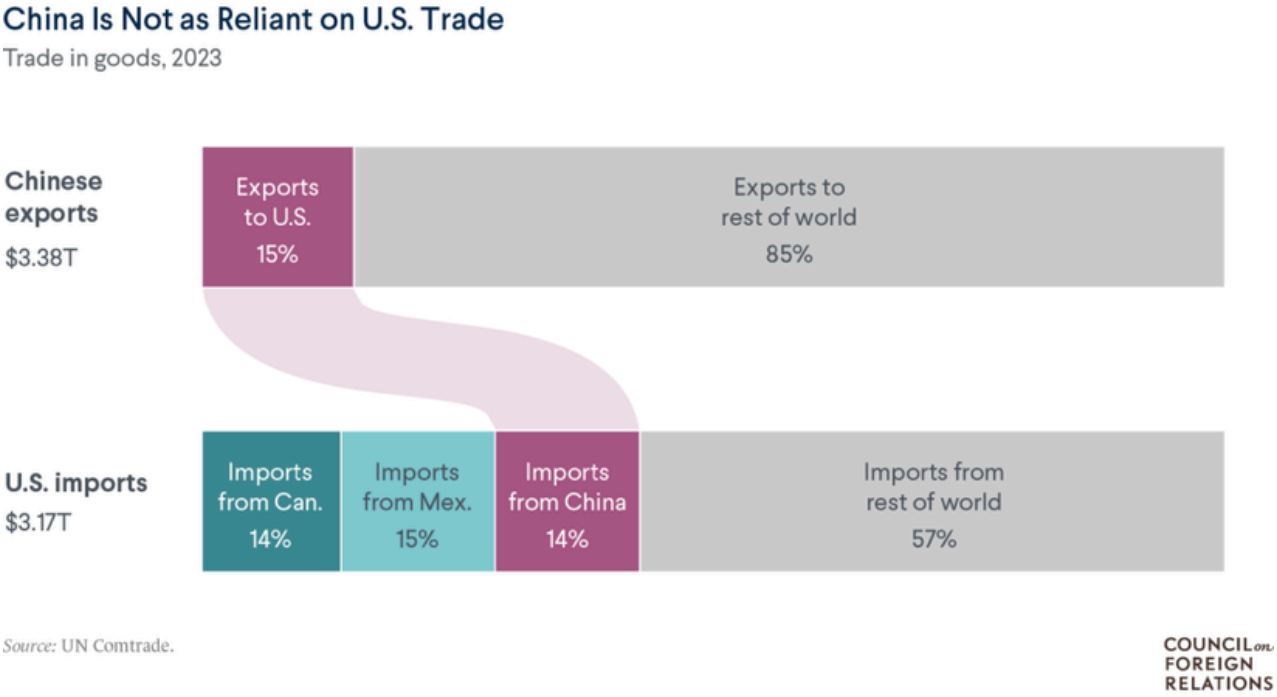
Trade constitutes about 70% of the economies of both Canada and Mexico, with the United States being their primary export market. Over 80% of Mexico's exports, including automobiles, machinery, and agricultural products, are destined for the U.S., accounting for 15% of total U.S. imports. The northern regions of Mexico, which are heavily industrialized, could face significant economic challenges due to these tariffs.

Canada faces similar challenges, as the U.S. purchases more than 70% of its exports. The energy sector is particularly at risk, with 80% of Canadian oil exports directed to the U.S. The imposed tariffs could lead to substantial economic downturns in both countries.




**Impact on China:**

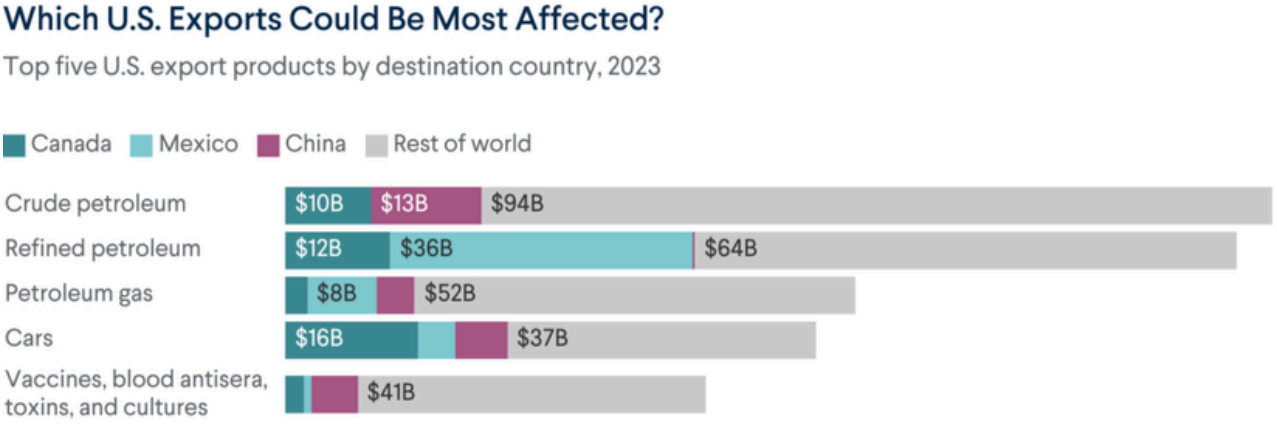
China's economy is less dependent on trade with the U.S., with imports and exports comprising about 37% of its GDP, a decrease from over 60% in the early 2000s. While U.S.-China trade has declined in recent years, China has increased trade with other partners, such as the European Union, Mexico, and Vietnam. This diversification may mitigate the impact of the new 10% tariff on Chinese goods entering the U.S.




**Potential Retaliatory Measures:**

Each country's currency could weaken further, lessening the bite of tariffs on imports and raising the effective price of U.S. exports to other nations.
A weakened yuan has already softened the blow for Chinese producers, helping their exports remain competitive around the world. The roughly 30 percent depreciation of Mexico's peso since April and the Canadian dollar's 8 percent drop since September also lessen the potential impact. Markets could potentially drive the peso, as well as the Canadian dollar, further down not that tariffs are in place.
Additionally, Canada, China, or Mexico could respond in kind, imposing tit-for-tat tariffs on the United States. Mexican President Claudia Sheinbaum has already suggested that Mexico could retaliate with tariffs of its own, and the United States-Mexico-Canada Agreement (USMCA), which underpins North American free trade, would likely allow it.

This wouldn't be the first time countries have reciprocated. In 2018, Mexico and Canada placed retaliatory tariffs on a combined more than $15 billion worth of U.S. goods — including steel, pork, yoghurt, and tablecloths — after Trump imposed tariffs on their steel and aluminium. Likewise, the United States lost $20 billion in annual farm exports when China hit back against a slew of U.S. tariffs from 2018 to 2019.



# THE CYBER PULSE

## The Cyber Landscape For Q1

Artificial Intelligence (AI) is revolutionizing cybersecurity by enhancing threat detection, automating responses, and managing risks more effectively. By integrating AI technologies like machine learning and neural networks into security frameworks, organizations can analyze vast amounts of data, recognize patterns, and adapt to evolving threats with minimal human intervention.

**Enhancing Threat Detection and Response**

Traditional cybersecurity measures often struggle to keep up with the sophistication and volume of modern cyberattacks. AI addresses these challenges by rapidly analyzing extensive datasets to identify anomalies and potential threats. This capability enables quicker and more accurate threat detection, allowing security teams to respond promptly and effectively.

**Automating Routine Security Tasks**

AI streamlines cybersecurity operations by automating repetitive and time-consuming tasks such as monitoring network traffic and analyzing security logs. This automation not only reduces the workload for security professionals but also minimizes the risk of human error, leading to more reliable security outcomes.

### Proactive Risk Management

By continuously learning from new data, AI systems can anticipate potential vulnerabilities and attack vectors. This proactive approach allows organizations to implement preventive measures before threats materialize, thereby strengthening their overall security posture.

### Challenges and Considerations

Despite its advantages, the adoption of AI in cybersecurity presents certain challenges. Ensuring the security of AI systems themselves is crucial, as they can be targeted by adversaries. Additionally, the integration of AI requires significant investments in technology and expertise. Organizations must also be mindful of potential biases in AI algorithms, which could lead to inaccurate threat assessments.

### The Future of AI in Cybersecurity

As AI technology continues to evolve, its role in cybersecurity is expected to expand. Innovations such as advanced language models and quantum AI hold the potential to further enhance threat detection and response capabilities. However, as cybercriminals also leverage AI for more sophisticated attacks, organizations must remain vigilant and continuously update their defences to stay ahead in this dynamic landscape.

In summary, AI offers transformative potential for cybersecurity by improving efficiency and effectiveness in threat management. While challenges exist, strategic implementation of AI can significantly bolster an organization’s defence against cyber threats.

## State-Sponsored Cyber Espionage: An In-Depth Analysis

In 2024, state-sponsored cyber espionage escalated, with nations such as China, Russia, and North Korea intensifying their cyber operations to achieve geopolitical, economic, and military objectives. This document provides a comprehensive analysis of the key actors, their recent activities, and the international responses to these cyber threats.

### China’s Cyber Espionage Activities

China’s cyber espionage efforts have been primarily attributed to advanced persistent threat (APT) groups like APT41, also known as the Winnti Group. This group operates under a dual model, engaging in both state-sponsored espionage and financially motivated cybercrimes.

**Recent Incidents:**

- Infiltration of U.S. Political Systems: In the summer of 2024, Chinese hackers infiltrated the Republican National Committee's (RNC) email system, maintaining access for several months. The breach, discovered by Microsoft and detailed in Alex Isenstadt's book "Revenge: The Inside Story of Trump's Return to Power," revealed that the hackers were interested in the GOP's stance on Taiwan, as the 2024 platform did not mention the island. RNC officials chose not to inform the FBI, fearing media leaks. The U.S. government was aware of the breach, which follows a history of Chinese cyber espionage targeting U.S. political campaigns.
- Telecommunications Breach: On August 27, 2024, it was reported that Chinese hackers compromised at least nine telecommunications firms in the U.S., including major providers like AT&T, Verizon, Lumen Technologies, and T-Mobile. The hackers accessed metadata of users' calls and text messages, including date and time stamps, source and destination IP addresses, and phone numbers from over a million users. Notably, the breach affected staff of the Kamala Harris 2024 presidential campaign, as well as phones belonging to Donald Trump and JD Vance. The attack was attributed to the Salt Typhoon APT group linked to China's Ministry of State Security (MSS).

**Motivations:**

China's cyber activities are driven by a desire to advance its technological capabilities and achieve geopolitical objectives. By infiltrating political systems and critical infrastructure, China aims to gather intelligence that supports its strategic interests, including its stance on Taiwan and efforts to counter Western influence.

**Russia's Cyber Operations**

Russian cyber espionage is predominantly conducted by groups affiliated with the Main Intelligence Directorate (GRU), such as Fancy Bear (APT28) and Cozy Bear (APT29). These groups focus on disruption, disinformation, and destabilization efforts.

Recent Incidents:

- Disruption of Ukrainian Infrastructure: In April 2024, the GRU-linked group Sandworm disrupted a Ukrainian nuclear power plant's safety systems, raising fears of a Chernobyl-style disaster. This attack exemplifies Russia's strategy to undermine Ukrainian stability and deter NATO support.
- Espionage on Western Political Entities: Fancy Bear has been implicated in various cyber attacks on Western political entities, including the Democratic National Committee and the campaign of French presidential candidate Emmanuel Macron. These operations aim to influence political outcomes and sow discord among NATO allies.

**Motivations:**

Russia's cyber operations are designed to project power, gather intelligence, and destabilize adversaries. By targeting political entities and critical infrastructure, Russia seeks to undermine democratic processes and weaken the cohesion of Western alliances.

**North Korea's Cyber Activities**

North Korea's cyber operations are primarily conducted by the Lazarus Group, also known as Guardians of Peace or Whois Team. This group engages in cyber espionage and financially motivated attacks to fund the regime's initiatives.

Recent Incidents:

- Cryptocurrency Thefts: The Lazarus Group has reportedly stolen £5 billion in cryptocurrency from Western countries, with the funds allegedly supporting Pyongyang's nuclear program. In their largest heist, they stole £1.2 billion worth of digital assets from the Dubai-based Bybit exchange, causing a significant drop in Ethereum's value.
- Infiltration of Defense Contractors: In February 2024, the Lazarus Group infiltrated a South Korean defence contractor, stealing missile schematics. This operation highlights North Korea's efforts to acquire advanced military technology through cyber espionage.

**Motivations:**

North Korea's cyber activities are driven by the need to circumvent international sanctions and generate revenue for its weapons programs. Additionally, by infiltrating defence contractors, North Korea aims to enhance its military capabilities.


**International Responses**

In light of escalating state-sponsored cyber threats, international responses have intensified, focusing on collaboration, sanctions, and defensive measures.

**Collaborative Measures:**

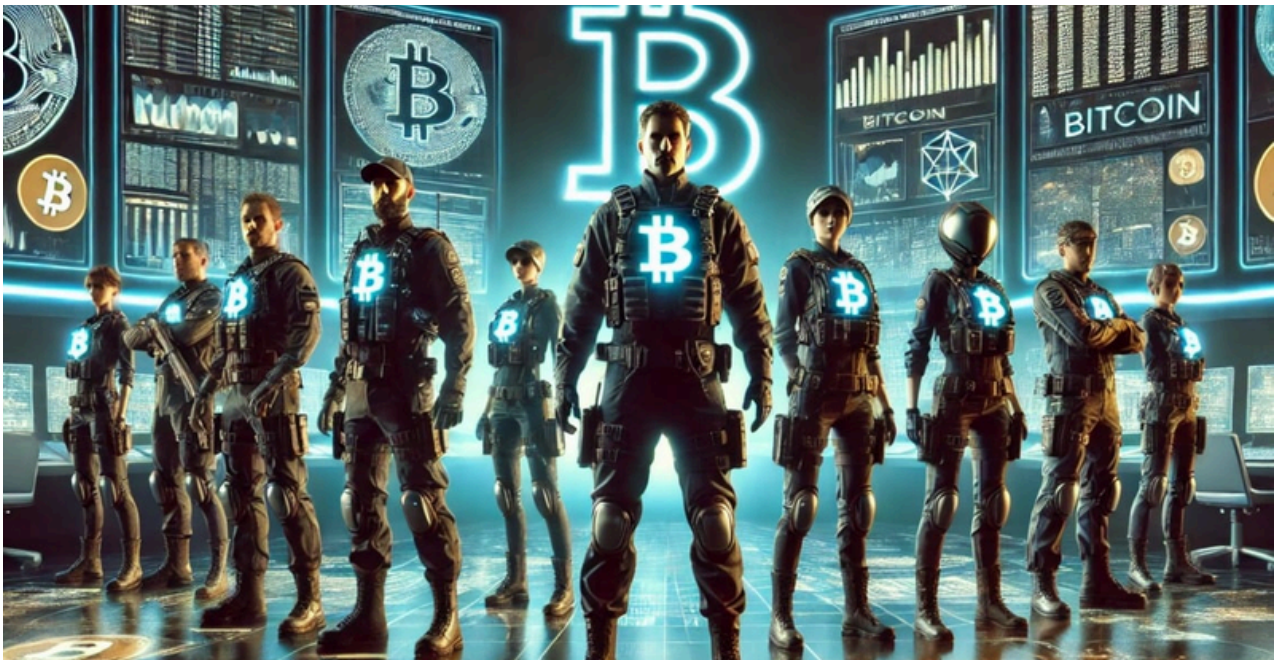
- U.S.-EU Cyber Dialogue: The United States and the European Union have enhanced threat intelligence sharing through platforms like the EU's Cyber Crisis Liaison Organisation Network (CyCLONe) and the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative (JCDC). These collaborations facilitate real-time data exchange on APT tactics, enabling coordinated responses to cyber threats.

**Sanctions and Indictments:**

- Targeting Cyber Actors: The U.S. Treasury has sanctioned entities supporting state-sponsored cyber activities, such as Chinese cloud providers hosting malicious infrastructure. Similarly, the EU has frozen the assets of individuals linked to Russian cyber operations and banned Russian IT firms from EU markets.

**Counter-Ransomware Initiatives:**

- Cryptocurrency Tracking: The U.S.-EU Task Force on Cryptocurrency Abuse has been established to track and seize illicit funds obtained through cyber heists. In 2024, this task force recovered significant amounts of cryptocurrency linked to North Korean cyber activities.



# VENTURE CAPITAL SPOTLIGHT

## VCs Bet Big: The 5 Industries Shaping Tomorrow's Economy

In the first quarter of 2025, venture capital firms have concentrated their investments in several key industries, each witnessing significant deals that underscore the sectors' growth and innovation potential.

**Artificial Intelligence (AI) and Machine Learning:**

The AI sector continues to attract substantial venture capital funding, driven by advancements in generative AI and machine learning applications. Notable investments include:


***Bridgetown Research***, a Seattle-based artificial intelligence startup, has successfully secured $19 million in a Series A funding round. The investment was led by prominent venture capital firms Lightspeed Venture Partners and Accel, with additional participation from a leading research university—this infusion of capital values the company at $250 million.

Bridgetown Research takes a distinctive approach, unlike many AI solutions that rely on large language models (LLMs) to search and summarize existing information. The company develops AI agents designed to collect proprietary data directly from experts and through customer surveys. These agents meticulously analyze the gathered information to detect patterns and generate actionable insights, thereby assisting executives and investors in making informed strategic decisions.

The newly acquired funds are earmarked for enhancing the capabilities of these AI agents, enabling them to perform a broader spectrum of analyses. Additionally, Bridgetown aims to expand its access to sector-specific intelligence by forging strategic partnerships. Initially, the company's focus was on private equity deal screening; however, it has since broadened its services to offer comprehensive market research solutions.

Founded by Harsh Sahai, Bridgetown Research benefits from his extensive experience in the tech and consulting sectors. Sahai previously led machine learning teams at Amazon and served as an engagement manager at McKinsey & Co. His vision for the company is to revolutionize the due diligence process by leveraging AI to expedite research and reduce costs. By automating data collection and analysis, Bridgetown aims to provide clients with rapid, reliable insights, thereby streamlining decision-making processes in various industries.

In summary, Bridgetown Research is poised to transform the landscape of market research and strategic decision-making. With its innovative use of AI to gather and analyze proprietary data, coupled with substantial financial backing, the company is well-positioned to offer efficient, cost-effective solutions to its growing clientele.


***Safe Superintelligence Inc. (SSI)*** is an AI startup co-founded by Ilya Sutskever, Daniel Gross, and Daniel Levy. It focuses on developing safe superintelligent systems. In September 2024, SSI raised over $1 billion in funding from prominent venture capital firms, including Andreessen Horowitz, Sequoia Capital, DST Global, and SV Angel, elevating its valuation to $5 billion.

Despite not yet offering commercial products, SSI's mission is to create AI systems that surpass human intelligence while ensuring safety and ethical considerations remain paramount. The company plans to use the funds to acquire computing power and hire top talent, with teams based in Palo Alto, California, and Tel Aviv, Israel.

SSI's singular focus on developing safe superintelligence allows it to operate without the distractions of management overhead or product cycles, insulating its safety, security, and progress from short-term commercial pressures.

The substantial investment in SSI underscores the confidence investors have in the company's leadership and its potential to make significant advancements in AI safety and capabilities. SSI aims to contribute meaningfully to the ongoing discourse on AI's role in society by prioritising safety and ethical considerations.

Venture capital (VC) plays a pivotal role in transforming groundbreaking scientific research into practical applications, particularly in emerging fields like quantum technology. Quantum science, after decades of foundational research, is now beginning to influence areas such as computing, sensing, and networking. During this transitional phase—where quantum technologies are moving from laboratory settings to real-world applications—VC is essential in supporting startups that emerge from academic environments. This support not only provides necessary funding but also helps shape the ecosystem's priorities, steering it toward innovations with significant societal impact.

The inception of dedicated quantum funds, exemplified by Quantonation I, highlights the influence of targeted VC investments. Quantonation I's approach has led to notable outcomes, including the generation of new scientific knowledge, the creation of jobs, and the infusion of capital into the quantum industry. These achievements underscore the importance of specialized investment strategies in nurturing nascent technologies.

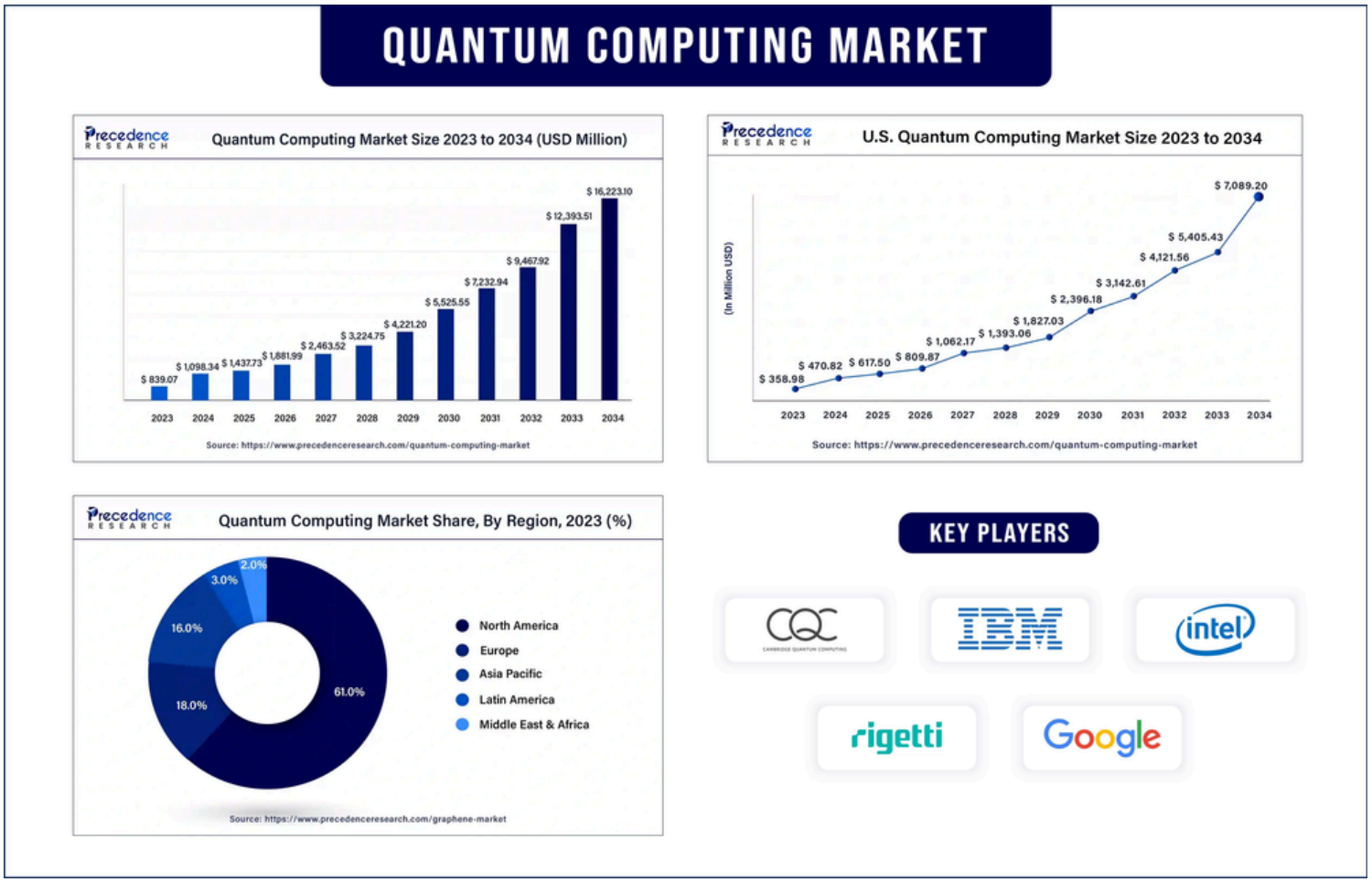
To further accelerate the growth of quantum startups, it's crucial to introduce frameworks that facilitate their emergence and scalability. This involves not only providing financial resources but also fostering collaborations between public institutions and private investors. Such partnerships can create an environment conducive to innovation, ensuring that quantum technologies develop in directions that offer substantial benefits to society.

Moreover, as the quantum industry evolves, there's a pressing need to engage the broader public in its development. This can be achieved through educational initiatives, transparent communication about technological advancements, and inclusive discussions about the societal implications of quantum technologies. By involving society at large, the industry can align its objectives with public interests, promoting responsible innovation.

In conclusion, venture capital is instrumental in bridging the gap between academic research and market-ready quantum technologies. By strategically investing in startups and fostering collaborative ecosystems, VC can drive the advancement of quantum innovations that hold the promise of profound societal impact.

The global quantum computing market is experiencing significant growth, with revenues increasing from approximately $839.07 million in 2023 to a projected $16.22 billion by 2034, reflecting a compound annual growth rate (CAGR) of 30.9% during the forecast period from 2024 to 2034. This expansion is largely driven by the burgeoning startup ecosystem and the transformative computational capabilities of quantum technology.

Quantum computing leverages principles of quantum mechanics to tackle complex problems that traditional computers and even supercomputers struggle to solve efficiently. Startups in this sector are focusing on various aspects, including both hardware and software development, to harness this emerging technology's potential.




One of the most promising applications of quantum computing lies in cryptography. Quantum computers can solve intricate mathematical problems that form the foundation of modern encryption methods, potentially revolutionizing data security.

In the pharmaceutical industry, quantum computing offers substantial benefits by accelerating drug discovery processes. Simulating complex molecular interactions is computationally intensive; quantum computers can expedite these simulations, leading to faster identification of effective drugs and, consequently, significant time and cost savings in drug development.

Additionally, several companies are investing in quantum cloud services, enabling researchers and developers to access quantum computing resources remotely. This accessibility fosters innovation and collaboration, further propelling the market's growth.

Key trends influencing the quantum computing market include:
• Increased Research Funding: Governments and pharmaceutical companies are making substantial investments to develop secure quantum computing platforms, recognizing their potential to solve critical problems more efficiently.
• Advancements in Drug Discovery: Quantum computing facilitates molecular-level research, enhancing the quality and speed of drug development.
• Growth in Machine Learning Applications: The demand for improved accuracy and speed in machine learning applications, such as speech recognition and natural language processing, is driving the adoption of quantum computing solutions.

In summary, the quantum computing market is poised for rapid expansion, driven by technological advancements, increased funding, and its potential to revolutionize various industries, notably cryptography and pharmaceuticals.

## Sectors & Companies Worth Keeping Up to Date On:

**1. Artificial Intelligence (AI) and Machine Learning:**
- OpenAI
- DeepMind:

**2. HealthTech and Biotech:**
- Everlab
- Viz.ai

**3. ClimateTech and Renewable Energy:**
- MGA Thermal
- Fleet Space Technologies

**4. FoodTech and AgriTech:**
- Fresho
- Earthodic

**5. FinTech:**
- JustFund
- Bridgit