

ATHARVA ROBOTICS CENTER

Daily News on Innovation & Technology

1st August, 2025

AI-driven breakthrough uncovers ‘next-gen’ materials that top lithium-ion performance

By Neetika Walter, July 31, 2025

NJIT researchers used AI to discover new battery materials that could power safer, cheaper, and more sustainable multivalent-ion alternatives to lithium



Hindustan Times AI & Cyber Security Summit 2025 Punjab Ignites North India’s Digital Future

By Genesis, July 31, 2025

Bringing together visionary leaders, tech pioneers, and institutional powerhouses, the Hindustan Times AI & Cyber Security Summit – Punjab 2025 unfolded as a landmark initiative in Ludhiana.



ChatGPT, Gemini, GenAI Tools Vulnerable to Man-in-the-Prompt Attacks

By Florence Nightingale, July 31, 2025

A critical vulnerability affecting popular AI tools, including ChatGPT, Google Gemini, and other generative AI platforms, exposes them to a novel attack vector dubbed “Man-in-the-Prompt.”



[Supersonic parachutes get upgrade, NASA conducts flight tests to support Mars deliveries](#)

By Prabhat Ranjan Mishra, July 31, 2025

Scientists from NASA are conducting a series of research flights to advance the supersonic parachutes. The plan is to make these parachutes more reliable and safer with advanced sensors. These upgraded parachutes are aimed at delivering scientific instruments and payloads to Mars



[In the shadow of China, Taiwan is building a drone army to stop an invasion](#)

By Erin Hale, July 31, 2025

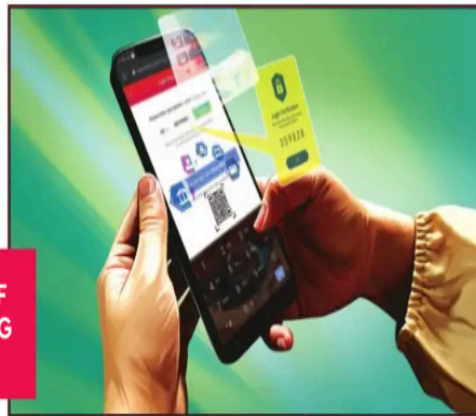
Taipei, Taiwan – On a bright morning last month, three sea drones skimmed across Su'ao Bay, off of Taiwan's rugged northeast coast. The tiny "stealth" Carbon Voyager 1, fast-moving Black Tide I, and explosives-carrying Sea Shark 800 were the highlight of an expo for companies vying to help Taiwan build up a maritime drone force.



News Articles

● What has DoT proposed?

THE DRAFT TELECOMMUNICATIONS (Telecom Cyber Security) Amendment Rules, 2025, introduced by the Department of Telecommunications (DoT) significantly broadens the scope to cover non-licensed entities that use telecom identifiers for user authentication. This includes what are now termed Telecommunication Identifier User Entities (TUEs)—digital platforms, OTT services, e-commerce websites, *et al*—that rely on OTP-based user verification and login mechanisms. All TUEs would have to validate users' mobile numbers through a centralised, government-managed platform—Mobile Number Validation platform—before delivering services. Government-authorized entities would be charged ₹1.50 per request, while other organisations would have to pay ₹3 per request. The draft rules also propose creation of a national International Mobile Equipment Identity (IMEI) database that will list tampered or blocked identifiers; second-hand mobile resellers will need to check this list before every sale, paying ₹10 per IMEI. IMEI numbers are unique serial numbers attached to phones and other personal electronics that use SIM cards.



COST OF CURBING FRAUDS

How draft telecom cyber rules can hurt the digital economy

Digital industry associations have slammed the proposed amendments to the telecom cyber security rules. The higher cost of compliance could impact the growth of consumer tech and allied sectors which rely on OTP-based user verification over the mobile phone, explains *Ojasvi Gupta*

THE PROPOSED MOBILE NUMBER VALIDATION SYSTEM IMPOSES ADDITIONAL COSTS ON STARTUPS AND MSMEs

₹1.5-3

PER VERIFICATION REQUEST PROPOSED AGAINST LESS THAN ₹0.1 IN OTP BASED SYSTEM CURRENTLY

● Increased cost of user verification

THE PROPOSED MOBILE Number Validation (MNV) system imposes additional costs that are likely to be untenable for startups and MSMEs. "The proposed fee of ₹1.5-3 per verification request via the MNV platform is nearly 30 to 60 times higher than the prevailing cost

of existing one-time password (OTP)-based verification, which is basically under ₹0.1 per request," IT body NASSCOM said in a letter to DoT. Platforms which handle millions of authentications each month may incorporate these expenses into their pricing models, subtly raising the cost of

access for users. For example, if 10% of Zomato's ~4.39 million daily users require validation, it can cost ₹24 crore each year. Further, since MNV doesn't top issues like SIM-swapping or spoofing, it adds cost without delivering proportionate security improvements.

● Fears of regulatory overreach

THE MOVE to bring in every kind of entity that uses mobile numbers for user identification under the ambit of the telecom cyber security rules has raised alarm. This classification is excessively wide and vague, say industry bodies, as it brings non-telecom digital entities under the ambit of telecom regulation for the first time. Many of them do not operate or manage telecom infrastructure and are already supervised by other sectoral regulators such as the Reserve Bank of India, Securities & Exchange Board of India, or the ministry of electronics and information technology. The Internet and Mobile Association

of India (IAMA) has said that the inclusion of digital businesses under the proposed amendments are in violation of the scope of the Telecom Act and amounts to regulatory overreach. Directing OTT platforms to suspend the use of specific telecom identifiers for user identification or service delivery without prior notice to the user could result in "arbitrary and unjustified user deactivation and service discontinuity, leading to business disruption, commercial loss and customer dissatisfaction," the body wrote its submission to the telecom department.

● IMEI controls may duplicate regulation

THE PROPOSED CREATION of a national IMEI database for tampered or restricted devices raises concerns of over-delegation without clear statutory backing. It shifts the regulatory approach from pre-sale checks to intensive post-market surveillance, placing significant compliance burdens on fragmented, small-scale sellers. Without proper legal

safeguards, this system risks duplicating regulation and becoming logistically unworkable. Similarly, IMEI-based controls may fall short in tackling fraud involving low-cost burner phones, designed for temporary use, which often carry valid, untampered identifiers. Since these devices don't trigger tampering alerts, they can easily bypass detection.

● How to ensure a safer digital economy

DESPITE THE CRITICISM, stakeholders agree that the intent behind the draft rules is legitimate—enhancing cyber security, reducing fraud, and improving user trust in digital platforms. If the rules are refined to reflect stakeholder feedback, they could play a constructive role in India's digital future. For instance, tiered compliance obligations based on the size and risk profile of TUEs could make the system more proportionate and fair. Sandbox or phased rollouts may also help mitigate disruption while

still testing security protocols. Alongside, by clarifying data protection safeguards and aligning with existing privacy laws, the government could balance its fraud-prevention goals with constitutional rights. There is merit in pursuing centralised mechanisms to flag compromised identifiers—if implemented with strong oversight. If recalibrated carefully, the rules could serve as a foundational framework for digital safety, helping India lead in secure and inclusive digital transformation.

Source: Financial Express Newspaper, 01-08-2025

Page No 11

Link: <https://epaper.financialexpress.com/4039885/Mumbai/AUGUST-01-2025#page/11/2>

Big Tech is spending more on AI, but investors love it

ADITYA SONI & DEBORAH MARY SOPHIA
July 31

BIG TECH IS spending more than ever on artificial intelligence (AI) - but the returns are rising too, and investors are buying in.

AI played a bigger role in driving demand across internet search, digital advertising and cloud computing in the April-June quarter, powering revenue growth at technology giants Microsoft, Meta, and Alphabet.

Betting that momentum will sustain, Microsoft and Alphabet decided to ramp up spending to ease capacity shortages that have limited their ability to meet soaring AI services demand, even after several quarters of multi-billion-dollar outlays.

The results offer the clear-sighted signet that AI is emerging as a primary growth engine, although the monetization journey is still in its early days, investors and analysts said.

The upbeat commentary also bodes well for Amazon.com, the largest US cloud provider, which will report earnings on Thursday after markets close, and underscores how surging demand for the new technology is shielding the tech giants from tariff-driven economic uncertainty hobbling other sectors.

"As companies like Alphabet and Meta race to deliver on the promise of AI, capital expenditures are shockingly high and will remain elevated for the foreseeable future," said Debra Aho Williamson, founder and chief analyst at Sonata Insights.

But if their core businesses remain strong, "it will buy them more time with investors and provide confidence that the billions being spent on infrastructure, talent and other tech-related expenses

RETURNS ARE RISING, TOO



- Microsoft boosts capex after Google's hike last week
- AI powering bumper results on cloud, advertising gains

■ Payoffs from AI justifying hefty capital spending, analysts say

■ Microsoft and Alphabet decided to ramp up spending to ease capacity shortages

■ AI is emerging as a primary growth engine for Big Tech, analysts said



will be worthwhile," she added.

Microsoft shares rose about 9% in premarket trading on Thursday, putting the Windows maker on track to cross \$4 trillion in market value - a milestone only chip giant Nvidia has reached so far.

Meta was up even more, rising 11.5% and on course to add nearly \$200 billion to its market value of \$1.75 trillion. Amazon gained over 3%.

All the companies have faced intense scrutiny from investors over their ballooning capital expenditures, which were expected to total \$330 billion this year before the latest earnings.

And until a few days ago, the Magnificent Seven stocks were also trailing the S&P 500 in year-to-date performance.

SILENCING DOUBTS

Microsoft said on Wednesday it would spend a record \$30 billion in the current quarter, after better-than-expected sales and an above-estimate forecast for its Azure cloud computing business showcased the growing returns on its massive AI bets.

The prediction puts Microsoft on track to potentially outspend its rivals over the next year. It came after Google-parent Alphabet beat revenue expectations and raised its spending forecast by \$10 billion to \$85 billion for the year.

Microsoft also disclosed for the first time the dollar figure for Azure sales and the number of users for its Copilot AI tools, whose adoption has long been a concern for investors.

It said Azure generated more than \$75 billion in sales in its last fiscal year, while Copilot tools had over 100 million users. Overall, around 800 million customers use AI tools peppered across Microsoft's sprawling software empire.

"It's the kind of result that quickly silences any doubts about cloud or AI demand," said Josh Gilbert, market analyst at eToro. "Microsoft is more than justifying its spending."

Other AI companies have also attracted a clutch of users.

Alphabet said last week its Gemini AI assistant app has more than 450 million

monthly active users. OpenAI's ChatGPT, the application credited with kicking off the generative AI frenzy, has around 500 million weekly active users.

Meta, meanwhile, raised the bottom end of its annual capital expenditure forecast by \$2 billion, to a range of between \$66 billion and \$72 billion. It also said that costs driven by its efforts to catch up in Silicon Valley's intensifying AI race would push 2026 expense growth rate above 2025's pace.

Better-than-expected sales growth in the April-June period and an above-estimate revenue forecast for the current quarter, however, assured investors that strength in the social media giant's core advertising business can support the massive outlays.

"The big boys are back," said Brian Mulberry, portfolio manager at Zacks Investment Management, which holds shares in all three major US cloud providers. "This simply proves the Magnificent Seven is still magnificent at this moment in time." —REUTERS

Source: Financial Express Newspaper, 01-08-2025

Page No 20

Link: <https://epaper.financialexpress.com/4039885/Mumbai/AUGUST-01-2025#page/20/2>

Tech to track foreign SIMs, AI defence tools & more

Devanshi Mehta & Khushi Bhuta

New Delhi: Among the many technologies demonstrated on the opening day of the International Police Expo and Drone International Expo 2025 on Thursday at Bharat Mandapam was the Rapid Illegal Immigrants Detection System — a portable, standalone device designed to identify foreign SIM cards and mobile devices within a 50-metre radius. The system is being pitched for use in tracking illegal Bangladeshi and Rohingya immigrants, particularly in border villages and densely populated slum clusters.

The device claims to operate independently of mobile network providers and enables real-time detection of IMEIs and IMSIs, which are unique numbers identifying mobile phones or subscribers, making it useful during cordon-and-search operations.

Drone, AI-powered defence systems, anti-drone guns, armoured ambulances, and mobile forensic tools were also showcased at the event, which drew over 4,000 police and defence personnel on Thursday.

At one stall, a forensic analyst demonstrated an India-specific open-source intelligence tool. By entering a deceased person's phone number, the system generated a flowchart mapping linked UPI accounts, social media handles, email IDs, even photos, sourced from across platforms and the deep web and dark web. The tool aims to streamline background checks for law enforcement.

Deepgaze AI was introduced as a defence against deepfakes, flag-

ging manipulated audio, video and image files with forensic precision. Meanwhile, drone data recovery and data sanitization tools were also on show. Mobile laboratories,

CCTV cameras and forensic scanners emphasised on holistically capturing evidence in the context of crash investigations, post-blast investigations, disaster recovery as

well as crime scene investigations. The expo is focused on developments in the fields of military equipment too, including both drones and anti-drone technology, arms,

gear and vehicles. From pistols with technology designed to fire in darkness to armoured mine-protected vehicles capable of withstanding landmine blasts, the expo aimed to ensure armed forces envision a more efficient future.

"I was especially looking forward to seeing the weapons and new systems," said Vaishali Mane, superintendent of police, Pune, as she tested the weight and grip of a pistol at one of the stalls. "We're here not just to browse, but to take stock, assess and provide as many suggestions as we can to ensure our own units stay updated with the best available options."

The attendees saw the technologies as a pathway to a future that is still being nurtured. CRPF personnel Bhopinder Singh said, "New technology is growing in all aspects: weapons, vehicles, gear. Some of these technologies we have heard of, but we are seeing them up close for the first time here."

However, the forces also approached the new technology with a grounded perspective. "These tools show promise, but field readiness will take time," said CISEF sub-inspector Ramashish Rama.

Delhi Traffic Police inspector Devi Lal called the technologies "a step toward modernising policing". With quick response vehicles built for efficient communication for the forces as well as mobile computers creating databases for logistical management in healthcare and govt, the expo underlined the importance of speed in policing and surveillance.



Source: The Times of India Newspaper, 01-08-2025

Page No 3

Link: https://drive.google.com/file/d/1TYKAQEh_6iFpXNQAnhHexCcEj7CZnINL/view



ATHARVA

ROBOTICS CENTER